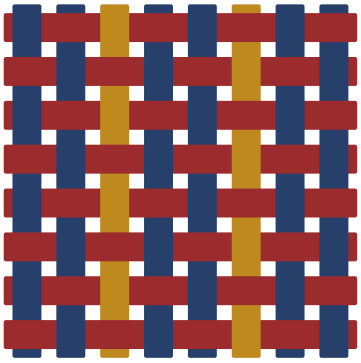


Tate cohomology and Galois cohomology

motivated by class field theory

Group cohomology seminar

Source readings, retypeset with integrated notes

dyed in indigo, madder & weld; ruled in iron-gall. woven on LOOM.

CONTENTS

1. Group and Galois Cohomology 3

1. Group cohomology . . . 3
- 1.1 Group rings . . . 3
- 1.2 Group cohomology via cochains . . . 4
- 1.3 Group cohomology via projective resolutions . . . 8
- 1.4 Homology of groups . . . 10
- 1.5 Induced modules . . . 12
- 1.6 Tate cohomology . . . 14
- 1.7 Dimension shifting . . . 18
- 1.8 Comparing cohomology groups . . . 19
- 1.9 Cup products . . . 26
- 1.10 Tate cohomology of cyclic groups . . . 32
- 1.11 Cohomological triviality . . . 36
- 1.12 Tate's theorem . . . 39

2. Galois cohomology . . . 42
- 2.1 Profinite groups . . . 42
- 2.2 Cohomology of profinite groups . . . 47
- 2.3 Galois theory of infinite extensions . . . 51
- 2.4 Galois cohomology . . . 53
- 2.5 Kummer theory . . . 55

2. Local Class Field Theory: Cohomology 59

- 1 The Cohomology of Unramified Extensions . . . 59
- 2 The Cohomology of Ramified Extensions . . . 64
- 3 The Local Artin Map . . . 67
- 4 The Hilbert symbol . . . 70
- 5 The Existence Theorem . . . 75

3. Brauer Groups 78

- 1 Simple Algebras; Semisimple Modules . . . 78
- 2 Definition of the Brauer Group . . . 83
- 3 The Brauer Group and Cohomology . . . 89
- 4 The Brauer Groups of Special Fields . . . 95
- 5 Complements . . . 98

4. Global Class Field Theory: Statements 102

- 1 Ray Class Groups . . . 102
- 2 L-series . . . 108
- 3 The Main Theorems in Terms of Ideals . . . 110
- 4 Idèles . . . 121
- 5 The Main Theorems in Terms of Idèles . . . 129

5. Global Class Field Theory: Proofs 135

- 1 Outline . . . 135
- 2 The Cohomology of the Idèles . . . 136
- 3 The Cohomology of the Units . . . 141
- 4 Cohomology of the Idèle Classes I: the First Inequality . . . 143
- 5 Cohomology of the Idèle Classes II: The Second Inequality . . . 145

6 The Algebraic Proof of the Second Inequality . . . 146
7 Application to the Brauer Group . . . 151
8 Completion of the Proof of the Reciprocity Law . . . 153
9 The Existence Theorem . . . 155
A Appendix: Kummer theory . . . 158

Supplement. An Introduction to Galois Cohomology and Its Applications 160
1 Introduction . . . 160
2 Cohomology sets . . . 163
3 Hilbert's 90th theorem . . . 166
4 Exact sequences in cohomology . . . 168
5 (The) matrix (case) reloaded . . . 172
6 Functors . . . 174
7 Functorial group actions . . . 175
8 Twisted forms . . . 176
9 The Galois descent condition . . . 177
10 Stabilizers . . . 177
11 Galois descent lemma . . . 178
12 The conjugacy problem again . . . 181
13 The case of infinite Galois extensions . . . 185

1. GROUP AND GALOIS COHOMOLOGY

Romyar Sharifi, Group and Galois Cohomology

In the discussion below H^i_T denotes Tate cohomology, written $\widehat{H}^i$ in Sharifi. We write H^i_{cont} for continuous cohomology.

1. GROUP COHOMOLOGY

1.1 Group rings

Let G be a group.

Definition 1.1.1. The *group ring* (or, more specifically, $\mathbb{Z}$-group ring) $\mathbb{Z}[G]$ of a group G consists of the set of finite formal sums of group elements with coefficients in $\mathbb{Z}$

$$\left\{ \sum_{g \in G} a_g g \mid a_g \in \mathbb{Z} \text{ for all } g \in G, \text{ almost all } a_g = 0 \right\}.$$

with addition given by addition of coefficients and multiplication induced by the group law on G and $\mathbb{Z}$-linearity. (Here, "almost all" means all but finitely many.)

In other words, the operations are

$$\sum_{g \in G}{}' a_g g + \sum_{g \in G}{}' b_g g = \sum_{g \in G}{}' (a_g + b_g) g$$

and

$$\left(\sum_{g \in G} a_g g \right) \left(\sum_{g \in G} b_g g \right) = \sum_{g \in G} \left(\sum_{k \in G} a_k b_{k^{-1}g} \right) g.$$

Remark 1.1.2. In the above, we may replace $\mathbb{Z}$ by any ring R, resulting in the R-group ring $R[G]$ of G. However, we shall need here only the case that $R = \mathbb{Z}$.

Definition 1.1.3.

i. The *augmentation map* is the homomorphism $\varepsilon : \mathbb{Z}[G] \to \mathbb{Z}$ given by

$$\varepsilon \left(\sum_{g \in G} a_g g \right) = \sum_{g \in G} a_g.$$

ii. The *augmentation ideal* I_G is the kernel of the augmentation map ε.

Lemma 1.1.4. *The augmentation ideal I_G is equal to the ideal of $\mathbb{Z}[G]$ generated by the set $\{g - 1 \mid g \in G\}$.*

Proof. Clearly $g - 1 \in \ker \varepsilon$ for all $g \in G$. On the other hand, if $\sum_{g \in G} a_g = 0$, then

$$\sum_{g \in G}{}' a_g g = \sum_{g \in G}{}' a_g (g - 1).$$

[

Definition 1.1.5. If G is a finite group, we then define the *norm element* of $\mathbb{Z}[G]$ by $N_G = \sum_{g \in G} g$.

Remark 1.1.6.

a. We may speak, of course, of modules over the group ring $\mathbb{Z}[G]$. We will refer here to such $\mathbb{Z}[G]$-modules more simply as *G-modules*. To give a G-module is equivalent to giving an abelian group A together with a G-action on A that is compatible with the structure of A as an abelian group, i.e., a map

$$G \times A \to A, \qquad (g, a) \mapsto g \cdot a$$

satisfying the following properties:

(i) $1 \cdot a = a$ for all $a \in A$,

(ii) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ for all $a \in A$ and $g_1, g_2 \in G$, and

(iii) $g \cdot (a_1 + a_2) = g \cdot a_1 + g \cdot a_2$ for all $a_1, a_2 \in A$ and $g \in G$.

b. A homomorphism $\kappa : A \to B$ of G-modules is just a homomorphism of abelian groups that satisfies $\kappa(ga) = g\kappa(a)$ for all $a \in A$ and $g \in G$. The group of such homomorphisms is denoted by $\mathrm{Hom}_{\mathbb{Z}[G]}(A, B)$.

Definition 1.1.7. We say that a G-module A is a *trivial* if $g \cdot a = a$ for all $g \in G$ and $a \in A$.

Definition 1.1.8. Let A be a G-module.

i. The group of *G-invariants* A^G of A is given by

$$A^G = \{a \in A \mid g \cdot a = a \text{ for all } g \in G, a \in A\},$$

which is to say the largest submodule of A fixed by G.

ii. The group of *G-coinvariants* A_G of A is given by

$$A_G = A/I_G A,$$

which is to say (noting Lemma 1.1.4) the largest quotient of A fixed by G.

Example 1.1.9.

a. If A is a trivial G-module, then $A^G = A$ and $A_G \cong A$.

b. One has $\mathbb{Z}[G]_G \cong \mathbb{Z}$. We have $\mathbb{Z}[G]^G = (N_G)$ if G is finite and $\mathbb{Z}[G]^G = (0)$ otherwise.

1.2 Group cohomology via cochains

The simplest way to define the ith cohomology group $H^i(G, A)$ of a group G with coefficients in a G-module A would be to let $H^i(G, A)$ be the ith derived functor on A of the functor of G-invariants. However, not wishing to assume homological algebra at this point, we take a different tack.

Definition 1.2.1. Let A be a G-module, and let $i \geq 0$.

i. The group of *i-cochains* of G with coefficients in A is the set of functions from G^i to A:

$$C^i(G, A) = \{f : G^i \to A\}.$$

ii. The ith *differential* $d^i = d^i_A : C^i(G, A) \to C^{i+1}(G, A)$ is the map

$$d^i(f)(g_0, g_1, \dots, g_i) = g_0 \cdot f(g_1, \dots g_i) + \sum_{j=1}^{i} (-1)^j f(g_0, \dots, g_{j-2}, g_{j-1} g_j, g_{j+1}, \dots, g_i) + (-1)^{i+1} f(g_0, \dots, g_{i-1}).$$

We will continue to let A denote a G-module throughout the section. We remark that $C^0(G, A)$ is taken simply to be A, as G^0 is a singleton set. The proof of the following is left to the reader.

Lemma 1.2.2. *For any $i \geq 0$, one has $d^{i+1} \circ d^i = 0$.*

Remark 1.2.3. Lemma 1.2.2 shows that $C^\cdot(G,A) = (C^i(G,A), d^i)$ is a cochain complex.

We consider the cohomology groups of $C^\cdot(G,A)$.

Definition 1.2.4. Let $i \geq 0$.

i. We set $Z^i(G,A) = \ker d^i$, the group of *i-cocycles* of G with coefficients in A.

ii. We set $B^0(G,A) = 0$ and $B^i(G,A) = \operatorname{im} d^{i-1}$ for $i \geq 1$. We refer to $B^i(G,A)$ as the group of *i-coboundaries* of G with coefficients in A.

We remark that, since $d^i \circ d^{i-1} = 0$ for all $i \geq 1$, we have $B^i(G,A) \subseteq Z^i(G,A)$ for all $i \geq 0$. Hence, we may make the following definition.

Definition 1.2.5. We define the *ith cohomology group* of G with coefficients in A to be

$$H^i(G,A) = Z^i(G,A)/B^i(G,A).$$

The cohomology groups measure how far the cochain complex $C^\cdot(G,A)$ is from being exact. We give some examples of cohomology groups in low degree.

Lemma 1.2.6.

a. The group $H^0(G,A)$ is equal to A^G, the group of G-invariants of A.

b. We have

$$Z^1(G,A) = \{f : G \to A \mid f(gh) = gf(h) + f(g) \text{ for all } g,h \in G\}$$

and $B^1(G,A)$ is the subgroup of $f : G \to A$ for which there exists $a \in A$ such that $f(g) = ga - a$ for all $g \in G$.

c. If A is a trivial G-module, then $H^1(G,A) = \operatorname{Hom}(G,A)$.

Proof. Let $a \in A$. Then $d^0(a)(g) = ga - a$ for $g \in G$, so $\ker d^0 = A^G$. That proves part a, and part b is simply a rewriting of the definitions. Part c follows immediately, as the definition of $Z^1(G,A)$ reduces to $\operatorname{Hom}(G,A)$, and $B^1(G,A)$ is clearly (0), in this case. ∎

We remark that, as A is abelian, we have $\operatorname{Hom}(G,A) = \operatorname{Hom}(G^{\mathrm{ab}},A)$, where G^{ab} is the maximal abelian quotient of G (i.e., its abelianization). We turn briefly to an even more interesting example.

Definition 1.2.7. A *group extension* of G by a G-module A is a short exact sequence of groups

$$0 \to A \xrightarrow{\iota} \mathscr{E} \xrightarrow{\pi} G \to 1$$

such that, choosing any section $s : G \to \mathscr{E}$ of π, one has

$$s(g)as(g)^{-1} = g \cdot a$$

for all $g \in G$, $a \in A$. Two such extensions $\mathscr{E} \to \mathscr{E}'$ are said to be equivalent if there is an isomorphism $\theta : \mathscr{E} \xrightarrow{\sim} \mathscr{E}'$ fitting into a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & \mathscr{E} & \longrightarrow & G & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle\theta} & & \| & & \\ 0 & \longrightarrow & A & \longrightarrow & \mathscr{E}' & \longrightarrow & G & \longrightarrow & 0, \end{array}$$

We denote the set of equivalence classes of such extensions by $\mathscr{E}(G,A)$.

We omit the proof of the following result, as it is not used in the remainder of these notes. We also leave it as an exercise to the reader to define the structure of an abelian group on $\mathscr{E}(G,A)$ which makes the following identification an isomorphism of groups.

Theorem 1.2.8. *The group $H^2(G,A)$ is in canonical bijection with $\mathscr{E}(G,A)$ via the map induced by that taking a 2-cocycle $f : G^2 \to A$ to the extension $\mathscr{E}_f = A \times G$ with multiplication given by*

$$(a,g)\cdot(b,h) = (a + gb + f(g,h), gh)$$

This identification takes the identity to the semi-direct product $A \ltimes G$ determined by the action of G on A.

One of the most important uses of cohomology is that it converts short exact sequences of Gmodules to long exact sequences of abelian groups. For this, in homological language, we need the fact that $C^i(G,A)$ provides an exact functor in the module A.

Lemma 1.2.9. *If $\alpha : A \to B$ is a G-module homomorphism, then for each $i \geq 0$, there is an induced homomorphism of groups*

$$\alpha^i : C^i(G,A) \to C^i(G,B)$$

taking f to $\alpha \circ f$ and compatible with the differentials in the sense that

$$d_B^i \circ \alpha^i = \alpha^{i+1} \circ d_A^i.$$

Proof. We need only check the compatibility. For this, note that

$$\begin{aligned} d^i(\alpha\circ f)(g_0,g_1,\dots,g_i) &= g_0\alpha\circ f(g_1,\dots g_i) \\ &+ \sum_{j=i}^{i}(-1)^j\alpha\circ f(g_0,\dots,g_{j-2},g_{j-1}g_j,g_{j+1},\dots,g_i) + (-1)^{i+1}\alpha\circ f(g_0,\dots,g_{i-1}) \\ &= \alpha(d^i(f)(g_0,g_1,\dots,g_i)), \end{aligned}$$

as α is a G-module homomorphism (the fact of which we use only to deal with the first term). ∎

In other words, α induces a morphism of complexes $\alpha^\cdot : C^\cdot(G,A) \to C^\cdot(G,B)$. As a consequence, one sees easily the following

Notation 1.2.10. If not helpful for clarity, we will omit the superscripts from the notation in the morphisms of cochain complexes. Similarly, we will consistently omit them in the resulting maps on cohomology, described below.

Corollary 1.2.11. *A G-module homomorphism $\alpha : A \to B$ induces maps*

$$\alpha^* : H^i(G,A) \to H^i(G,B)$$

on cohomology.

The key fact that we need about the morphism on cochain complexes is the following.

Lemma 1.2.12. *Suppose that*

$$0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0$$

is a short exact sequence of G-modules. Then the resulting sequence

$$0 \to C^i(G,A) \xrightarrow{\iota} C^i(G,B) \xrightarrow{\pi} C^i(G,C) \to 0$$

is exact.

Proof. Let $f \in C^i(G,A)$, and suppose $\iota \circ f = 0$. As ι is injective, this clearly implies that $f = 0$, so the map ι^i is injective. As $\pi \circ \iota = 0$, the same is true for the maps on cochains. Next, suppose

that $f' \in C^i(G,B)$ is such that $\pi \circ f' = 0$. Define $f \in C^i(G,A)$ by letting $f(g_1,\dots,g_i) \in A$ be the unique element such that

$$\iota(f(g_1,\dots,g_i)) = f'(g_1,\dots,g_i),$$

which we can do since $\operatorname{im}\iota = \ker\pi$. Thus, $\operatorname{im}\iota^i = \ker\pi^i$. Finally, let $f'' \in C^i(G,C)$. As π is surjective, we may define $f' \in C^i(G,B)$ by taking $f'(g_1,\dots,g_i)$ to be any element with

$$\pi(f'(g_1,\dots,g_i)) = f''(g_1,\dots,g_i).$$

We therefore have that π^i is surjective. ∎

We now prove the main theorem of the section.

Theorem 1.2.13. *Suppose that*

$$0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0$$

is a short exact sequence of G-modules. Then there is a long exact sequence of abelian groups

$$0 \to H^0(G,A) \xrightarrow{\iota^*} H^0(G,B) \xrightarrow{\pi^*} H^0(G,C) \xrightarrow{\delta^0} H^1(G,A) \to \cdots.$$

Moreover, this construction is natural in the short exact sequence in the sense that any morphism

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \xrightarrow{\iota} & B & \xrightarrow{\pi} & C & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\
0 & \longrightarrow & A' & \xrightarrow{\iota'} & B' & \xrightarrow{\pi'} & C' & \longrightarrow & 0,
\end{array}$$

gives rise to a morphism of long exact sequences, and in particular, a commutative diagram

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & H^i(G,A) & \xrightarrow{\iota^*} & H^i(G,B) & \xrightarrow{\pi^*} & H^i(G,C) & \xrightarrow{\delta^i} & H^{i+1}(G,A) & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle\alpha^*} & & \downarrow{\scriptstyle\beta^*} & & \downarrow{\scriptstyle\gamma^*} & & \downarrow{\scriptstyle\alpha^*} & & \\
\cdots & \longrightarrow & H^i(G,A') & \xrightarrow{(\iota')^*} & H^i(G,B') & \xrightarrow{(\pi')^*} & H^i(G,C') & \xrightarrow{\delta^i} & H^{i+1}(G,A') & \longrightarrow & \cdots.
\end{array}$$

Proof. First consider the diagrams

$$\begin{array}{ccccccccc}
0 & \longrightarrow & C^j(G,A) & \xrightarrow{\iota} & C^j(G,B) & \xrightarrow{\pi} & C^j(G,C) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d_A^j} & & \downarrow{\scriptstyle d_B^j} & & \downarrow{\scriptstyle d_C^j} & & \\
0 & \longrightarrow & C^{j+1}(G,A) & \xrightarrow{\iota} & C^{j+1}(G,B) & \xrightarrow{\pi} & C^{j+1}(G,C) & \longrightarrow & 0
\end{array}$$

for $j \geq 0$. Noting Lemma 1.2.12, the exact sequences of cokernels (for $j = i-1$) and kernels (for $j = i+1$) can be placed in a second diagram

$$\begin{array}{ccccccccc}
 & & \frac{C^i(G,A)}{B^i(G,A)} & \xrightarrow{\iota} & \frac{C^i(G,B)}{B^i(G,B)} & \xrightarrow{\pi} & \frac{C^i(G,C)}{B^i(G,C)} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d_A^i} & & \downarrow{\scriptstyle d_B^i} & & \downarrow{\scriptstyle d_C^i} & & \\
0 & \longrightarrow & Z^{i+1}(G,A) & \xrightarrow{\iota} & Z^{i+1}(G,B) & \xrightarrow{\pi} & Z^{i+1}(G,C) & &
\end{array}$$

(recalling that $B^0(G,A) = 0$ for the case $i = 0$), and the snake lemma now provides the exact sequence

$$H^i(G,A) \xrightarrow{\alpha^*} H^i(G,B) \xrightarrow{\beta^*} H^i(G,C) \xrightarrow{\delta^i} H^{i+1}(G,A) \xrightarrow{\alpha^*} H^{i+1}(G,B) \xrightarrow{\beta^*} H^{i+1}(G,C).$$

Splicing these together gives the long exact sequence in cohomology, exactness of

$$0 \to H^0(G,A) \to H^0(G,B)$$

being obvious. We leave naturality of the long exact sequence as an exercise. ∎

Remark 1.2.14. The maps $\delta^i : H^i(G,C) \to H^{i+1}(G,A)$ defined in the proof of theorem 1.2.13 are known as *connecting homomorphisms*. Again, we will often omit superscripts and simply refer to δ.

Remark 1.2.15. A sequence of functors that take short exact sequences to long exact sequences (i.e., which also give rise to connecting homomorphisms) and is natural in the sense that every morphism of short exact sequences gives rise to a morphism of long exact sequences is known as a δ-functor. Group cohomology forms a (cohomological) δ-functor that is universal in a sense we omit a discussion of here.

1.3 Group cohomology via projective resolutions

In this section, we assume a bit of homological algebra, and redefine the G-cohomology of A in terms of projective resolutions.

For $i \geq 0$, let G^{i+1} denote the direct product of $i+1$ copies of G. We view $\mathbb{Z}[G^{i+1}]$ as a G-module via the left action

$$g \cdot (g_0, g_1, \dots, g_i) = (gg_0, gg_1, \dots, gg_i).$$

We first introduce the standard resolution.

Definition 1.3.1. The *(augmented) standard resolution* of $\mathbb{Z}$ by G-modules is the sequence of Gmodule homomorphisms

$$\cdots \to \mathbb{Z}[G^{i+1}] \xrightarrow{d_i} \mathbb{Z}[G^i] \to \cdots \to \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z},$$

where

$$d_i(g_0, \dots, g_i) = \sum_{j=0}^{i} (-1)^j (g_0, \dots, g_{j-1}, g_{j+1}, \dots, g_i)$$

for each $i \geq 1$, and ε is the augmentation map.

At times, we may use $(g_0, \dots, \widehat{g_j}, \dots, g_i) \in G^i$ to denote the i-tuple excluding g_j. To see that this definition is actually reasonable, we need the following lemma.

Proposition 1.3.2. *The augmented standard resolution is exact.*

Proof. In this proof, take $d_0 = \varepsilon$. For each $i \geq 0$, compute

$$d_i \circ d_{i+1}(g_0, \dots, g_{i+1}) = \sum_{j=0}^{i+1} \sum_{\substack{k=0 \\ k \neq j}}^{i+1} (-1)^{j+k-s(j,k)} (g_0, \dots, \widehat{g_j}, \dots, \widehat{g_k}, \dots, g_{i+1}),$$

where $s(j,k)$ is 0 if $k < j$ and 1 if $k > j$. Each possible $(i-1)$-tuple appears twice in the sum, with opposite sign. Therefore, we have $d_i \circ d_{i+1} = 0$.

Next, define $\theta_i : \mathbb{Z}[G^i] \to \mathbb{Z}[G^{i+1}]$ by

$$\theta_i(g_1, \dots, g_i) = (1, g_1, \dots, g_i).$$

Then

$$\begin{aligned} d_i \circ \theta_i(g_0, \dots, g_i) &= (g_0, \dots, g_i) - \sum_{j=0}^{i} (-1)^j (1, g_0, \dots, \widehat{g_j}, \dots, g_i) \\ &= (g_0, \dots, g_i) - \theta_{i-1} \circ d_{i-1}(g_0, \dots, g_i), \end{aligned}$$

which is to say that

$$d_i \circ \theta_i + \theta_{i-1} \circ d_{i-1} = \mathrm{id}_{\mathbb{Z}[G^i]}.$$

If $\alpha \in \ker d_{i-1}$ for $i \geq 1$, it then follows that $d_i(\theta_i(\alpha)) = \alpha$, so $\alpha \in \operatorname{im} d_i$. ∎

For a G-module A, we wish to consider the following complex

$$0 \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) \to \cdots \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{i+1}], A) \xrightarrow{D^i} \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{i+2}], A) \to \cdots. \quad (1.3.1)$$

Here, we define $D^i = D^i_A$ by $D^i(\varphi) = \varphi \circ d_{i+1}$. We compare this with the complex of cochains for G.

Theorem 1.3.3. *The maps*

$$\psi^i \colon \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{i+1}], A) \to C^i(G, A)$$

defined by

$$\psi^i(\varphi)(g_1, \dots, g_i) = \varphi(1, g_1, g_1 g_2, \dots, g_1 g_2 \cdots g_i)$$

are isomorphisms for all $i \geq 0$. This provides isomorphisms of complexes in the sense that $\psi^{i+1} \circ D^i = d^i \circ \psi^i$ for all $i \geq 0$. Moreover, these isomorphisms are natural in the G-module A.

Proof. If $\psi^i(\varphi) = 0$, then $\varphi(1, g_1, g_1 g_2, \dots, g_1 g_2 \cdots g_i) = 0$ for all $g_1, \dots, g_i \in G$. Let $h_0, \dots, h_i \in G$, and define $g_j = h_{j-1}^{-1} h_j$ for all $1 \leq j \leq i$. We then have

$$\varphi(h_0, h_1, \dots, h_i) = h_0 \varphi(1, h_0^{-1} h_1, \dots, h_0^{-1} h_i) = h_0 \varphi(1, g_1, \dots, g_1 \cdots g_i) = 0.$$

Therefore, ψ^i is injective. On the other hand, if $f \in C^i(G, A)$, then defining

$$\varphi(h_0, h_1, \dots, h_i) = h_0 f(h_0^{-1} h_1, \dots, h_{i-1}^{-1} h_i),$$

we have

$$\varphi(gh_0, gh_1, \dots, gh_i) = gh_0 f((gh_0)^{-1} gh_1, \dots, (gh_{i-1})^{-1} gh_i) = g\varphi(h_0, h_1, \dots, h_i)$$

and $\psi^i(\varphi) = f$. Therefore, ψ^i is an isomorphism of groups.

That $\psi^\cdot$ forms a map of complexes is shown in the following computation:

$$\begin{aligned} \psi^{i+1}(D^i(\varphi))(g_1, \dots, g_{i+1}) &= D^i(\varphi)(1, g_1, \dots, g_1 \cdots g_{i+1}) \\ &= \varphi \circ d_{i+1}(1, g_1, \dots, g_1 \cdots g_{i+1}) \\ &= \sum_{j=0}^{i+1} (-1)^j \varphi(1, g_1, \dots, \widehat{g_1 \cdots g_j}, \dots, g_1 \cdots g_{i+1}). \end{aligned}$$

The latter term equals

$$g_1 \psi^i(\varphi)(g_2, \dots, g_{i+1}) + \sum_{j=1}^{i} (-1)^j \psi^i(\varphi)(g_1, \dots, g_{j-1}, g_j g_{j+1}, g_{j+2}, \dots, g_{i+1}) + (-1)^{i+1} \psi^i(\varphi)(g_1, \dots, g_i),$$

which is $d^i(\psi^i(\varphi))$.

In degree zero, a homogeneous cochain $F \colon G \to A$ has $F(g) = gF(1)$ by equivariance. The alternating deletion differential gives

$$(D^0 F)(g_0, g_1) = F(g_1) - F(g_0).$$

Putting $a = F(1)$ and evaluating at $(1, g)$ gives $(d^0 a)(g) = ga - a$.

Finally, suppose that $\alpha : A \to B$ is a G-module homomorphism. We then have

$$\alpha \circ \psi^i(\varphi)(g_1, \dots, g_i) = \alpha \circ \varphi(1, g_1, \dots, g_1 \cdots g_i) = \psi^i(\alpha \circ \varphi)(g_1, \dots, g_i),$$

hence the desired naturality. ∎

Corollary 1.3.4. *The ith cohomology group of the complex* $(\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{i+1}], A), D_A^i)$ *is naturally isomorphic to* $H^i(G, A)$.

In fact, the standard resolution is a projective resolution of $\mathbb{Z}$, as is a consequence of the following lemma and the fact that every free module is projective.

Lemma 1.3.5. *The G-module $\mathbb{Z}[G^{i+1}]$ is free.*

Proof. In fact, we have

$$\mathbb{Z}[G^{i+1}] \cong \bigoplus_{(g_1,\dots,g_i) \in G^i} \mathbb{Z}[G](1, g_1, \dots, g_i),$$

and the submodule generated by $(1, g_1, \dots, g_i)$ is clearly free. ∎

Remarks 1.3.6.

a. Lemma 1.3.5 implies that the standard resolution provides a projective resolution of $\mathbb{Z}$. It follows that

$$H^i(G, A) \cong \mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z}, A)$$

for any G-module A. Moreover, if $P_\cdot \to \mathbb{Z} \to 0$ is any projective resolution of $\mathbb{Z}$ by G-modules, we have that $H^i(G, A)$ is the ith cohomology group of the complex $\mathrm{Hom}_{\mathbb{Z}[G]}(P_\cdot, A)$.

b. By definition, $\mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z}, A)$ is the ith right derived functor of the functor that takes the value $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$ on A. Note that $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A) \cong A^G$, the module of G-invariants. Therefore, if $0 \to A \to I^\cdot$ is any injective $\mathbb{Z}[G]$-resolution of A, then $H^i(G, A)$ is the ith cohomology group in the sequence

$$0 \to (I^0)^G \to (I^1)^G \to (I^2)^G \to \cdots.$$

1.4 Homology of groups

In this section, we consider a close relative of group cohomology, known as group homology. Note first that $\mathbb{Z}[G^{i+1}]$ is also a right module over $\mathbb{Z}[G]$ by the diagonal right multiplication by an element of G. Up to isomorphism of G-modules, this is the same as taking the diagonal left multiplication of $\mathbb{Z}[G^{i+1}]$ by the inverse of an element of G.

Definition 1.4.1. Use the standard resolution as a right $\mathbb{Z}[G]$-resolution of the trivial mod $\mathbb{Z}$. For a left $\mathbb{Z}[G]$-mod A, the ith homology group is $H_i(G, A) = \ker(d_i)/\operatorname{im}(d_{i+1})$ in the complex

$$\cdots \to \mathbb{Z}[G^3] \otimes_{\mathbb{Z}[G]} A \xrightarrow{d_2} \mathbb{Z}[G^2] \otimes_{\mathbb{Z}[G]} A \xrightarrow{d_1} \mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} A \to 0.$$

The right action on the standard resolution is diagonal right multiplication. For a projective resolution originally written with a left action, $x \cdot g = g^{-1}x$ gives the right action used to form the tensor product.

We note that if $f : A \to B$ is a G-module homomorphism, then there are induced maps $f_* : H_i(G, A) \to H_i(G, B)$ for each $i \geq 0$.

Remark 1.4.2. It follows from Definition 1.4.1 that $H_i(G, A) \cong \mathrm{Tor}^i_{\mathbb{Z}[G]}(\mathbb{Z}, A)$ for every $i \geq 0$, and that $H_i(G, A)$ may be calculated by taking the homology of $P_\cdot \otimes_{\mathbb{Z}[G]} A$, where $P_\cdot$ is any

projective $\mathbb{Z}[G]$-resolution of $\mathbb{Z}$. Here, we view P_i as a right G-module via the action $x \cdot g = g^{-1}x$ for $g \in G$ and $x \in X$.

As a first example, we have

Lemma 1.4.3. *We have natural isomorphisms $H_0(G,A) \cong A_G$ for every G-module A.*

Proof. Identify $\mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} A$ with A. By the alternating deletion convention in Definition 1.3.1,

$$d_1\big((g_0,g_1)\otimes a\big) = (g_1 - g_0)a.$$

The image of d_1 is $I_G A$, so $H_0(G,A) = A/I_G A = A_G$. ∎

As $A_G \cong \mathbb{Z} \otimes_{\mathbb{Z}[G]} A$, we have in particular that $H_i(G,A)$ is the ith left derived functor of A_G. As with cohomology, we therefore have in particular that homology carries short exact sequences to long exact sequences, as we now spell out.

Theorem 1.4.4. *Suppose that*

$$0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0$$

is a short exact sequence of G-modules. Then there are connecting homomorphisms $\delta_* \colon H_i(G,C) \to H_{i-1}(G,A)$ and a long exact sequence of abelian groups

$$\cdots \to H_1(G,C) \xrightarrow{\delta} H_0(G,A) \xrightarrow{\iota_*} H_0(G,B) \xrightarrow{\pi_*} H_0(G,C) \to 0.$$

Moreover, this construction is natural in the short exact sequence in the sense that any morphism of short exact sequences gives rise to a morphism of long exact sequences.

The following result computes the homology group $H_1(G,\mathbb{Z})$, where $\mathbb{Z}$ has the trivial G-action.

Proposition 1.4.5. *There are canonical isomorphisms $H_1(G,\mathbb{Z}) \cong I_G/I_G^2 \cong G^{\mathrm{ab}}$, where G^{ab} denotes the abelianization of G, the latter taking the coset of $g-1$ to the coset of $g \in G$.*

Proof. Since $\mathbb{Z}[G]$ is $\mathbb{Z}[G]$-projective, we have $H_1(G,\mathbb{Z}[G]) = 0$, and hence our long exact sequence in homology has the form

$$0 \to H_1(G,\mathbb{Z}) \to H_0(G,I_G) \to H_0(G,\mathbb{Z}[G]) \to H_0(G,\mathbb{Z}) \to 0.$$

Note that $H_0(G,I_G) \cong I_G/I_G^2$ and $H_0(G,\mathbb{Z}[G]) \cong \mathbb{Z}[G]/I_G \cong \mathbb{Z}$ via the augmentation map. Since $H_0(G,\mathbb{Z}) \cong \mathbb{Z}$ and any surjective map $\mathbb{Z} \to \mathbb{Z}$ (in this case the identity) is an isomorphism, we obtain the first isomorphism of the proposition.

For the second isomorphism, let us define maps $\phi \colon G^{\mathrm{ab}} \to I_G/I_G^2$ and $\psi \colon I_G/I_G^2 \to G^{\mathrm{ab}}$. For $g \in G$, we set

$$\phi(g[G,G]) = (g-1) + I_G^2,$$

where $[G,G]$ denotes the commutator subgroup of G. To see that this is a homomorphism on G, hence on G^{ab}, note that

$$(gh-1) + I_G^2 = (g-1) + (h-1) + (g-1)(h-1) + I_G^2 = (g-1) + (h-1) + I_G^2$$

for $g,h \in G$.

Next, define ψ on $\alpha = \sum_{g\in G} a_g g \in I_G$ by

$$\psi(\alpha + I_G^2) = \prod_{g\in G} g^{a_g}[G,G].$$

The order of the product doesn't matter as G^{ab} is abelian, and ψ is then a homomorphism if welldefined. It suffices for the latter to check that the recipe defining ψ takes

the generators $(g-1)(h-1)$ of I_G^2 for $g,h \in G$ to the trivial coset, but this follows as $(g-1)(h-1) = gh - g - h + 1$, and for instance, we have

$$gh \cdot g^{-1} \cdot h^{-1} \in [G,G].$$

Finally, we check that the two homomorphisms are inverse to each other. We have

$$\phi(\psi(\alpha + I_G^2)) = \sum_{g \in G} a_g(g-1) + I_G^2 = \alpha + I_G^2$$

since $\alpha \in I_G$ implies $\sum_{g\in G} a_g = 0$, and

$$\psi(\phi(g[G,G])) = \phi((g-1) + I_G^2) = g[G,G].$$

[

1.5 Induced modules

Definition 1.5.1. Let H be a subgroup of G, and suppose that B is a $\mathbb{Z}[H]$-module. We set

$$\mathrm{Ind}_H^G(B) = \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} B \quad \text{and} \quad \mathrm{CoInd}_H^G(B) = \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], B).$$

We give these G-actions by

$$g \cdot (\alpha \otimes b) = (g\alpha) \otimes b \quad \text{and} \quad (g \cdot \varphi)(\alpha) = \varphi(\alpha \cdot g).$$

We say that the resulting modules are *induced* and *coinduced*, respectively, from H to G.

Remark 1.5.2. What we refer to as a "coinduced" module is often actually referred to as an "induced" module.

We may use these modules to interpret H-cohomology groups as G-cohomology groups.

Theorem 1.5.3 (Shapiro's Lemma)**.** *For each $i \geq 0$, we have canonical isomorphisms*

$$H_i(G, \mathrm{Ind}_H^G(B)) \cong H_i(H,B) \quad \text{and} \quad H^i(G, \mathrm{CoInd}_H^G(B)) \cong H^i(H,B)$$

that provide natural isomorphisms of δ-functors.

Proof. Let $P_\cdot$ be the standard resolution of $\mathbb{Z}$ by G-modules. Define

$$\psi_i \colon \mathrm{Hom}_{\mathbb{Z}[G]}(P_i, \mathrm{CoInd}_H^G(B)) \to \mathrm{Hom}_{\mathbb{Z}[H]}(P_i, B)$$

by $\psi_i(\theta)(x) = \theta(x)(1)$. If $\theta \in \ker \psi_i$, then

$$\theta(x)(g) = (g \cdot \theta(x))(1) = \theta(gx)(1) = 0.$$

for all $x \in P_i$ and $g \in G$, so $\theta = 0$. Conversely, if $\varphi \in \mathrm{Hom}_{\mathbb{Z}[H]}(P_i, B)$, then define θ by $\theta(x)(g) = \varphi(gx)$, and we have $\psi_i(\theta) = \varphi$.

As for the induced case, note that associativity of tensor products yields

$$P_i \otimes_{\mathbb{Z}[G]} (\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} B) \cong P_i \otimes_{\mathbb{Z}[H]} B,$$

and $P_i = \mathbb{Z}[G^{i+1}]$ is free as a left H-module, hence projective. (We leave it to the reader to check that usual $\otimes$-Hom adjunction can be similarly used to give a shorter proof of the result for cohomology.) ∎

In fact, if H is of finite index in G, the notions of induced and coinduced from H to G coincide.

Proposition 1.5.4. *Suppose that H is a subgroup of finite index in G and B is a H-module. Then we have a canonical isomorphism of G-modules*

$$\chi : \operatorname{CoInd}_H^G(B) \xrightarrow{\sim} \operatorname{Ind}_H^G(B), \qquad \chi(\varphi) = \sum_{\bar{g} \in H\backslash G} g^{-1} \otimes \varphi(g),$$

where for each $\bar{g} \in H\backslash G$, the element $g \in G$ is an arbitrary choice of representative of $\bar{g}$.

Proof. First, we note that χ is a well-defined map, as

$$(hg)^{-1} \otimes \varphi(hg) = g^{-1}h^{-1} \otimes h\varphi(g) = g \otimes \varphi(g)$$

for $\varphi \in \operatorname{CoInd}_H^G(B)$, $h \in H$, and $g \in G$. Next, we see that χ is a G-module homomorphism, as

$$\chi(g'\varphi) = \sum_{\bar{g} \in H\backslash G} g^{-1} \otimes \varphi(gg') = g' \sum_{\bar{g} \in H\backslash G} (gg')^{-1} \otimes \varphi(gg') = g'\chi(\varphi)$$

for $g' \in G$. As the coset representatives form a basis for $\mathbb{Z}[G]$ as a free $\mathbb{Z}[H]$-module, we may define an inverse to χ that maps

$$\sum_{\bar{g} \in H\backslash G} g^{-1} \otimes b_g \in \operatorname{Ind}_H^G(B)$$

to the unique $\mathbb{Z}[H]$-linear map φ that takes the value b_g on g for the chosen representative of $\bar{g} \in H\backslash G$. ∎

In the special case of the trivial subgroup, we make the following definition.

Definition 1.5.5. We say that G-modules of the form

$$\operatorname{Ind}^G(X) = \mathbb{Z}[G] \otimes_{\mathbb{Z}} X \quad \text{and} \quad \operatorname{CoInd}^G(X) = \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], X),$$

where X is an abelian group, are *induced* and *coinduced* G-modules, respectively.

Remark 1.5.6. Note that Proposition 1.5.4 implies that the notions of induced and coinduced modules coincide for finite groups G. On the other hand, for infinite groups, $\operatorname{CoInd}^G(X)$ will never be finitely generated over $\mathbb{Z}[G]$ for nontrivial X, while $\operatorname{Ind}^G(X)$ will be for any finitely generated abelian group X.

Theorem 1.5.7. *Suppose that A is an induced (resp., coinduced) G-module. Then we have $H_i(G, A) = 0$ (resp., $H^i(G, A) = 0$) for all $i \geq 1$.*

Proof. Let X be an abelian group. By Shapiro's Lemma, we have

$$H_i(G, \operatorname{Ind}^G(X)) = H_i(\{1\}, X)$$

for $i \geq 1$. Since $\mathbb{Z}$ has a projective $\mathbb{Z}$-resolution by itself, the latter groups are 0. The proof for cohomology is essentially identical. ∎

Definition 1.5.8. A G-module A such that $H^i(G, A) = 0$ for all $i \geq 1$ is called *G-acyclic*.

We show that we may construct induced and coinduced G-modules starting from abelian groups that are already equipped with a G-action.

Remark 1.5.9. Suppose that A and B are G-modules. We give $\operatorname{Hom}_{\mathbb{Z}}(A, B)$ and $A \otimes_{\mathbb{Z}} B$ the G-actions

$$(g \cdot \varphi)(a) = g\varphi(g^{-1}a), \qquad g \cdot (a \otimes b) = ga \otimes gb,$$

respectively.

Lemma 1.5.10. *Let A be a G-module, and let A° be its underlying abelian group. Then*

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A) \cong \mathrm{CoInd}^G(A^\circ) \quad \text{and} \quad \mathbb{Z}[G] \otimes_{\mathbb{Z}} A \cong \mathrm{Ind}^G(A^\circ).$$

Proof. We define

$$\kappa \colon \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A) \to \mathrm{CoInd}^G(A^\circ), \qquad \kappa(\varphi)(g) = g \cdot \varphi(g^{-1}).$$

For $g, k \in G$, we then have

$$(k \cdot \kappa(\varphi))(g) = \kappa(\varphi)(gk) = gk \cdot \varphi(k^{-1}g^{-1}) = g \cdot (k \cdot \varphi)(g^{-1}) = \kappa(k \cdot \varphi)(g),$$

so κ is a G-module homomorphism. Note that κ is also self-inverse on the underlying set of both groups, so is an isomorphism. In the induced case, we define

$$\nu \colon \mathbb{Z}[G] \otimes_{\mathbb{Z}} A \to \mathrm{Ind}^G(A^\circ), \qquad \nu(g \otimes a) = g \otimes g^{-1}a.$$

For $g, k \in G$, we now have

$$k \cdot \nu(g \otimes a) = (kg) \otimes g^{-1}a = \nu(kg \otimes ka) = \nu(k \cdot (g \otimes a)),$$

so ν is a G-module isomorphism with inverse $\nu^{-1}(g \otimes a) = g \otimes ga$. ∎

Remark 1.5.11. Noting the lemma, we will simply refer to $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A)$ as $\mathrm{CoInd}^G(A)$ and $\mathbb{Z}[G] \otimes_{\mathbb{Z}} A$ as $\mathrm{Ind}^G(A)$.

1.6 Tate cohomology

We suppose in this section that G is a finite group. In this case, recall that we have the norm element $N_G \in \mathbb{Z}[G]$, which defines by left multiplication a map $N_G \colon A \to A$ on any G-module A. Its image $N_G A$ is the *group of G-norms* of A.

Lemma 1.6.1. *The norm element induces a map $\bar{N}_G \colon A_G \to A^G$.*

Proof. We have $N_G((g-1)a) = 0$ for any $g \in G$ and $a \in A$, so the map factors through A_G, and clearly $\mathrm{im}\, N_G \subseteq A^G$. ∎

Definition 1.6.2. Write $H_T^0(G, A)$ and $H_T^{-1}(G, A)$ for the cokernel and kernel, respectively, of the norm map $\overline{N}_G : A_G \to A^G$ in Lemma 1.6.1. In other words,

$$H_T^0(G, A) = A^G / N_G A, \qquad H_T^{-1}(G, A) = \ker(N_G : A \to A)/I_G A.$$

Example 1.6.3. Take $A = \mathbb{Z}$ with trivial G-action. The norm $N_G : \mathbb{Z} \to \mathbb{Z}$ is multiplication by $|G|$, so $H_T^0(G, \mathbb{Z}) = \mathbb{Z}/|G|\mathbb{Z}$ and $H_T^{-1}(G, \mathbb{Z}) = 0$.

Remark 1.6.4. In general, when we take cohomology with coefficients in a group, like $\mathbb{Z}$ or $\mathbb{Q}$, with no specified action of the group G, the action is taken to be trivial.

The Tate cohomology groups are an amalgamation of the homology groups and cohomology groups of G, with the homology groups placed in negative degrees.

Definition 1.6.5. Let G be a finite group and A a G-mod. For each $i \in \mathbb{Z}$ the ith Tate cohomology group is

$$H_T^i(G, A) = \begin{cases} H^i(G, A), & i \geq 1, \\ \mathrm{coker}(\overline{N}_G), & i = 0, \\ \ker(\overline{N}_G), & i = -1, \\ H_{-i-1}(G, A), & i \leq -2. \end{cases}$$

We have modified the zeroth homology and cohomology groups in defining Tate cohomology so that we obtain long exact sequences from short exact sequences as before, but extending infinitely in both directions, as we shall now see.

Theorem 1.6.6 (Tate)**.** *Suppose that*

$$0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0$$

is a short exact sequence of G-modules. Then there is a long exact sequence of abelian groups

$$\cdots \to \hat{H}^i(G,A) \xrightarrow{\iota} \hat{H}^i(G,B) \xrightarrow{\pi} \hat{H}^i(G,C) \xrightarrow{\delta} \hat{H}^{i+1}(G,A) \to \cdots.$$

Moreover, this construction is natural in the short exact sequence in the sense that any morphism of short exact sequences gives rise to a morphism of long exact sequences.

Proof. The first part follows immediately from applying the snake lemma to the following diagram, which in particular defines the map δ on $H_T^{-1}(G,C)$:

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & H_1(G,C) & \xrightarrow{\delta} & H_0(G,A) & \xrightarrow{\iota_*} & H_0(G,B) & \xrightarrow{\pi_*} & H_0(G,C) & \longrightarrow & 0 \\
 & & & & \downarrow{\scriptstyle \bar{N}_G} & & \downarrow{\scriptstyle \bar{N}_G} & & \downarrow{\scriptstyle \bar{N}_G} & & \\
0 & \longrightarrow & H^0(G,A) & \xrightarrow{\iota_*} & H^0(G,B) & \xrightarrow{\pi_*} & H^0(G,C) & \xrightarrow{\delta} & H^1(G,A) & \longrightarrow & \cdots,
\end{array}$$

and the second part is easily checked. ∎

Tate cohomology groups have the interesting property that they vanish entirely on induced modules.

Proposition 1.6.7. *Suppose that A is an induced G-module. Then $H_T^i(G,A) = 0$ for all $i \in \mathbb{Z}$.*

Proof. By Theorem 1.5.7 and Proposition 1.5.4, it suffices to check this for $i = -1$ and $i = 0$. Let X be an abelian group. Since $\mathbb{Z}[G]^G = N_G\mathbb{Z}[G]$, we have

$$H^0(G, \mathrm{Ind}^G(X)) = N_G\mathbb{Z}[G] \otimes_{\mathbb{Z}} X,$$

so $\hat{H}^0(G, \mathrm{Ind}^G(X)) = 0$ by definition. We also have that

$$H_0(G, \mathrm{Ind}^G(X)) = (\mathbb{Z}[G] \otimes_{\mathbb{Z}} X)_G \cong \mathbb{Z} \otimes_{\mathbb{Z}} X \cong X. \tag{1.6.1}$$

Let $\alpha = \sum_{g\in G}(g \otimes x_g)$ be an element of $\mathrm{Ind}^G(X)$. Then

$$N_G\alpha = N_G \otimes \sum_{g\in G} x_g$$

is trivial if and only if $\sum_{g\in G} x_g = 0$, which by the identification in (1.6.1) is to say that α has trivial image in $H_0(G, \mathrm{Ind}^G(X))$. Hence $\hat{H}_0(G, \mathrm{Ind}^G(X)) = 0$ as well. ∎

The Tate cohomology groups can also be computed via a doubly infinite resolution of G-modules. The proof of this is rather involved and requires some preparation.

Lemma 1.6.8. *Let X be a G-module that is free of finite rank over $\mathbb{Z}$, and let A be any G-module. Then the map*

$$\nu : X \otimes_{\mathbb{Z}} A \to \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{Z}}(X,\mathbb{Z}),A), \qquad \nu(x\otimes a)(\varphi) = \varphi(x)a$$

is an isomorphism of G-modules.

Proof. We note that

$$\nu(g\cdot(x\otimes a))(\varphi) = \varphi(gx)ga,$$

while

$$(g \cdot \nu(x \otimes a))(\varphi) = g\nu(x \otimes a)(g^{-1}\varphi) = (g^{-1}\varphi)(x)ga = \varphi(gx)ga,$$

so ν is a homomorphism of G-modules.

Let $x_1, \dots, x_m$ be any $\mathbb{Z}$-basis of X, and let $x_1^*, \dots, x_m^*$ be the dual basis of $\mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z})$ such that $x_i^*(x_j) = \delta_{ij}$ for $1 \le i, j \le m$. We define

$$\omega \colon \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z}), A) \to X \otimes_{\mathbb{Z}} A, \qquad \omega(\psi) = \sum_{i=1}^{m} x_i \otimes \psi(x_i^*).$$

Then

$$(\nu \circ \omega)(\psi)(\varphi) = \nu\left(\sum_{i=1}^{m} x_i \otimes \psi(x_i^*)\right)(\varphi) = \sum_{i=1}^{m} \varphi(x_i)\psi(x_i^*) = \psi\left(\sum_{i=1}^{m} \varphi(x_i)x_i^*\right) = \psi(\varphi).$$

On the other hand,

$$(\omega \circ \nu)(x \otimes a) = \sum_{i=1}^{m} x_i \otimes x_i^*(x)a = \sum_{i=1}^{m} x_i^*(x)x_i \otimes a = x \otimes a.$$

Hence, ν is an isomorphism. ∎

Lemma 1.6.9. *Let X and A be G-modules, and endow X with a right G-action by $x \cdot g = g^{-1}x$. Then we have a canonical isomorphism*

$$X \otimes_{\mathbb{Z}[G]} A \xrightarrow{\sim} (X \otimes_{\mathbb{Z}} A)_G$$

induced by the identity on $X \otimes_{\mathbb{Z}} A$. Proof. First, note that $X \otimes_{\mathbb{Z}[G]} A$ is a quotient of the G-module $X \otimes_{\mathbb{Z}} A$, which is endowed the diagonal left G-action. By definition of the tensor product over $\mathbb{Z}[G]$, we have

$$g^{-1}x \otimes a = x \cdot g \otimes a = x \otimes ga,$$

so G acts trivially on $X \otimes_{\mathbb{Z}[G]} A$, and hence the latter group is a quotient of $(X \otimes_{\mathbb{Z}} A)_G$. On the other hand, the $\mathbb{Z}$-bilinear map

$$X \times A \to (X \otimes_{\mathbb{Z}} A)_G, \qquad (x, a) \mapsto x \otimes a$$

is $\mathbb{Z}[G]$-balanced, hence induces a map on the tensor product inverse to the above-described quotient map. ∎

We are now ready to prove the theorem.

Theorem 1.6.10. *Let $P_\cdot \xrightarrow{\alpha} \mathbb{Z}$ be a projective resolution by G-modules of finite $\mathbb{Z}$-rank, and consider the $\mathbb{Z}$-dual $\mathbb{Z} \xrightarrow{\hat{\alpha}} P_*^\cdot$, where $P_*^i = \mathrm{Hom}_{\mathbb{Z}}(P_i, \mathbb{Z})$ for $i \ge 0$ and G acts on P_*^i by $(g \cdot \varphi)(x) = \varphi(g^{-1}x)$. Let $Q_\cdot$ be the exact chain complex*

$$\cdots \to P_1 \to P_0 \xrightarrow{\hat{\alpha} \circ \alpha} P_*^0 \to P_*^1 \to \cdots,$$

where P_0 occurs in degree 0. (That is, we set $Q_i = P_i$ for $i \ge 0$ and $Q_i = P_*^{-1-i}$ for $i < 0$.) For any G-module A, the Tate cohomology group $H_T^i(G, A)$ is the ith cohomology group of the cochain complex $C^\cdot = \mathrm{Hom}_{\mathbb{Z}[G]}(Q_\cdot, A)$.

Proof. As P_i is projective over $\mathbb{Z}[G]$, it is in particular $\mathbb{Z}$-free, so the $\mathbb{Z}$-dual sequence $\mathbb{Z} \to P_*^\cdot$ is still exact. Let us denote the ith differential on P_i by d_i and its $\mathbb{Z}$-dual by $\hat{d}^i$. We check exactness at Q_0 and Q_{-1}. Let $\beta = \hat{\alpha} \circ \alpha$. By definition, $\mathrm{im}\, d_1 = \ker \alpha$, and as $\hat{\alpha}$ is injective, we have im

$d_1 = \ker \beta$. Similarly, we have $\ker \hat{d}^0 = \operatorname{im} \hat{\alpha}$, and as α is surjective, we have $\ker \hat{d}^0 = \operatorname{im} \beta$. Therefore, $Q_\cdot$ is exact.

That $\operatorname{Hom}_{\mathbb{Z}[G]}(Q_\cdot, A)$ computes the Tate cohomology groups $H^i_T(G, A)$ follows immediately from the definition for $i \geq 1$. By Lemma 1.6.9, we have an isomorphism

$$P_i \otimes_{\mathbb{Z}[G]} A \xrightarrow{\sim} (P_i \otimes_{\mathbb{Z}} A)_G.$$

By Proposition 1.6.7 and Lemma 1.5.10, we have that

$$(P_i \otimes_{\mathbb{Z}} A)_G \xrightarrow{\bar{N}_G} (P_i \otimes_{\mathbb{Z}} A)^G$$

is an isomorphism as well, and following this by the restriction

$$(P_i \otimes_{\mathbb{Z}} A)^G \to \operatorname{Hom}_{\mathbb{Z}}(P^i_*, A)^G = \operatorname{Hom}_{\mathbb{Z}[G]}(P^i_*, A)$$

of the map ν of Lemma 1.6.8, we obtain in summary an isomorphism

$$\chi_i \colon P_i \otimes_{\mathbb{Z}[G]} A \to \operatorname{Hom}_{\mathbb{Z}[G]}(P^i_*, A).$$

Next, we check that the maps ν of Lemma 1.6.8 commute with the differentials on the complexes $P_\cdot \otimes_{\mathbb{Z}} A$ and $\operatorname{Hom}_{\mathbb{Z}}(P^\cdot_*, A)$, the former of which are just the tensor products of the differentials d_i on the P_i with the identity (then also denoted d_i), and the latter of which are double duals $\tilde{d}_i$ of the d_i, i.e., which satisfy

$$\tilde{d}_i(\psi)(\varphi) = \psi(\varphi \circ d_i),$$

for $\psi \in \operatorname{Hom}_{\mathbb{Z}}(P^i_*, A)$ and $\varphi \in \operatorname{Hom}_{\mathbb{Z}}(P_{i-1}, \mathbb{Z})$. We have

$$(\nu \circ d_i)(x \otimes a)(\varphi) = \nu(d_i(x) \otimes a)(\varphi) = \varphi(d_i(x))a.$$

On the other hand, we have

$$(\tilde{d}_i \circ \nu)(x \otimes a)(\varphi) = \tilde{d}_i(\nu(x \otimes a))(\varphi) = \nu(x \otimes a)(\varphi \circ d_i) = \varphi(d_i(x))a,$$

as desired. Moreover, the d_i commute with $\bar{N}_G$ on $(P_i \otimes_{\mathbb{Z}} A)_G$, being that they are G-module maps. Hence, the maps χ_i for all i together provide an isomorphism of complexes. In particular, the ith cohomology group of $\operatorname{Hom}_{\mathbb{Z}[G]}(Q_\cdot, A)$ is $H^i_T(G, A)$ for all $i \leq -2$, and we already knew this for all $i \geq 1$.

It remains to consider the cases $i = 0, -1$. We need to compute the cohomology of

$$P_1 \otimes_{\mathbb{Z}[G]} A \to P_0 \otimes_{\mathbb{Z}[G]} A \xrightarrow{\tau} \operatorname{Hom}_{\mathbb{Z}[G]}(P_0, A) \to \operatorname{Hom}_{\mathbb{Z}[G]}(P_1, A) \tag{1.6.2}$$

in the middle two degrees, and

$$\tau(x \otimes a)(y) = (\chi_0(x \otimes a) \circ \hat{\alpha} \circ \alpha)(y) = \sum_{g \in G}{}' (\hat{\alpha} \circ \alpha)(y)(gx)ga = \sum_{g \in G}{}' \alpha(y)\alpha(x)ga,$$

noting that $\alpha(gx) = \alpha(x)$ for every $g \in G$ and $\hat{\alpha}(n)(x) = n\alpha(x)$ for every $n \in \mathbb{Z}$. On the other hand, viewing α and $\hat{\alpha}$ as inducing maps

$$\lambda \colon P_0 \otimes_{\mathbb{Z}[G]} A \to A_G \quad \text{and} \quad \hat{\lambda} \colon A^G \to \operatorname{Hom}_{\mathbb{Z}[G]}(P_0, A),$$

respectively, we have

$$\begin{aligned}(\hat{\lambda} \circ \bar{N}_G \circ \lambda)(x \otimes a)(y) = \hat{\lambda}(\bar{N}_G(\alpha(x)a))(y) = \hat{\lambda}\Big(\sum_{g \in G}{}' \alpha(x)ga\Big)(y) \\ = \sum_{g \in G}{}' \hat{\alpha}(\alpha(x))(y)ga = \sum_{g \in G}{}' \alpha(x)\alpha(y)ga.\end{aligned}$$

In other words, we have $\tau = \hat{\lambda} \circ \bar{N}_G \circ \lambda$. As the cokernel of the first map in (1.6.2) is $H_0(G,A) = A_G$ and the kernel of the last is $H^0(G,A) = A^G$, with these identifications given by the maps λ and $\hat{\lambda}$ respectively, we have that the complex given by $A_G \xrightarrow{\bar{N}_G} A^G$ in degrees -1 and 0 computes the cohomology groups in question, as desired. ∎

As what is in essence a corollary, we have the following version of Shapiro's lemma.

Theorem 1.6.11. *Let G be a finite group, let H be a subgroup, and let B be an H-module. Then for every $i \in \mathbb{Z}$, we have canonical isomorphisms*

$$\hat{H}^i(G, \mathrm{CoInd}_H^G(B)) \cong \hat{H}^i(H,B)$$

that together provide natural isomorphisms of δ-functors.

Proof. The proof is nearly identical to that of Shapiro's lemma for cohomology groups. That is, we may simply use the isomorphisms induced by

$$\psi_i \colon \mathrm{Hom}_{\mathbb{Z}[G]}(Q_i, \mathrm{CoInd}_H^G(B)) \to \mathrm{Hom}_{\mathbb{Z}[H]}(Q_i, B)$$

by $\psi_i(\theta)(x) = \theta(x)(1)$, for $Q_\cdot$ the doubly infinite resolution of $\mathbb{Z}$ for G of Theorem 1.6.10. ∎

1.7 Dimension shifting

One useful technique in group cohomology is that of dimension shifting. The key idea here is to use the acyclicity of coinduced modules to obtain isomorphisms among cohomology groups.

To describe this technique, note that we have a short exact sequence

$$0 \to A \xrightarrow{\iota} \mathrm{CoInd}^G(A) \to A^* \to 0, \tag{1.7.1}$$

where ι is defined by $\iota(a)(g) = a$ for $a \in A$ and $g \in G$, and A^* is defined to be the cokernel of ι. We also have a short exact sequence

$$0 \to A_* \to \mathrm{Ind}^G(A) \xrightarrow{\pi} A \to 0, \tag{1.7.2}$$

where π is defined by $\pi(g \otimes a) = a$ for $a \in A$ and $g \in G$, and A_* is defined to be the kernel of π.

Remark 1.7.1. If we view A as $\mathbb{Z} \otimes_{\mathbb{Z}} A$, we see by the freeness of $\mathbb{Z}$ as a $\mathbb{Z}$-module and the definition of $\mathrm{Ind}^G(A)$ that $A_* \cong I_G \otimes_{\mathbb{Z}} A$ with a diagonal action of G. Moreover, viewing A as $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A)$, we see that $A^* \cong \mathrm{Hom}_{\mathbb{Z}}(I_G, A)$.

Proposition 1.7.2. *With the notation as above, we have*

$$H^{i+1}(G,A) \cong H^i(G,A^*) \quad \text{and} \quad H_{i+1}(G,A) \cong H_i(G,A_*)$$

for all $i \geq 1$. Proof. By Lemma 1.5.10, we know that $\mathrm{CoInd}^G(A)$ (resp., $\mathrm{Ind}^G(A)$) is coinduced (resp., induced). The result then follows easily by Theorem 1.5.7 and the long exact sequences of Theorems 1.2.13 and 1.4.4. ∎

For Tate cohomology groups, we have an even cleaner result.

Theorem 1.7.3 (Dimension shifting)**.** *Suppose that G is finite. With the above notation, we have*

$$\hat{H}^{i+1}(G,A) \cong \hat{H}^i(G,A^*) \quad \text{and} \quad \hat{H}^{i-1}(G,A) \cong \hat{H}^i(G,A_*)$$

for all $i \in \mathbb{Z}$.

Proof. Again noting Lemma 1.5.10, it follows from Theorem 1.5.4 and Proposition 1.6.7 that the long exact sequences associated by Theorem 1.6.6 to the short exact sequences in (1.7.1) and (1.7.2) reduce to the isomorphisms in question. ∎

This result allows us to transfer questions about cohomology groups in a certain degree to analogous questions regarding cohomology groups in other degrees. Let us give a first application.

Proposition 1.7.4. *Suppose that G is a finite group and A is a G-module. Then the groups $H_T^i(G, A)$ have exponent dividing $|G|$ for every $i \in \mathbb{Z}$.*

Proof. By Theorem 1.7.3, the problem immediately reduces to proving the claim for $i = 0$ and every module A. But for any $a \in A^G$, we have $|G|a = N_G a$, so $H_T^0(G, A)$ has exponent dividing $|G|$. ∎

This has the following important corollary.

Corollary 1.7.5. *Suppose that G is a finite group and A is a G-module that is finitely generated as an abelian group. Then $H_T^i(G, A)$ is finite for every $i \in \mathbb{Z}$.*

Proof. We know that $H_T^i(G, A)$ is a subquotient of the finitely generated abelian group $Q_i \otimes_{\mathbb{Z}[G]} A$ of Theorem 1.6.10, hence is itself finitely generated. As it has finite exponent, it is therefore finite. ∎

We also have the following.

Corollary 1.7.6. *Suppose that G is finite. Suppose that A is a G-module on which multiplication by $|G|$ is an isomorphism. Then $H_T^i(G, A) = 0$ for $i \in \mathbb{Z}$.*

Proof. Multiplication by $|G|$ on A induces multiplication by $|G|$ on Tate cohomology, which is then an isomorphism. Since by Proposition 1.7.4, multiplication by $|G|$ is also the zero map on Tate cohomology, the Tate cohomology groups must be 0. ∎

1.8 Comparing cohomology groups

Definition 1.8.1. Let G and G' be groups, A a G-module and A' a G'-module. We say that a pair (ρ, λ) with $\rho : G' \to G$ and $\lambda : A \to A'$ group homomorphisms is *compatible* if

$$\lambda(\rho(g')a) = g'\lambda(a)$$

for all $g' \in G'$ and $a \in A$.

Compatible pairs are used to provide maps among cohomology groups.

Proposition 1.8.2. *Suppose that $\rho : G' \to G$ and $\lambda : A \to A'$ form a compatible pair. Then the maps*

$$C^i(G,A) \to C^i(G',A'), \qquad f \mapsto \lambda \circ f \circ (\rho \times \cdots \times \rho)$$

induce maps on cohomology $H^i(G,A) \to H^i(G',A')$ for all $i \geq 0$.

Proof. One need only check that this is compatible with differentials, but this is easily done using compatibility of the pair. That is, if f' is the image of f , then to show that

$$d^i f'(g'_0, \dots, g'_i) = \lambda(d^i f(\rho(g'_0), \dots, \rho(g'_i))),$$

immediately reduces to showing that the first terms on both sides arising from the expression for the definition of the differential are equal. Since the pair is compatible, we have

$$g'_0 f'(g'_1, \dots g'_i) = g'_0 \lambda(f(\rho(g'_1), \dots, \rho(g'_i))) = \lambda(\rho(g'_0) f(\rho(g'_1), \dots, \rho(g'_i))),$$

as desired. ∎

Remark 1.8.3. Using the standard resolution, we have a homomorphism

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{i+1}], A) \to \mathrm{Hom}_{\mathbb{Z}[G']}(\mathbb{Z}[(G')^{i+1}], A'), \qquad \psi \mapsto \lambda \circ \psi \circ (\rho \times \cdots \times \rho)$$

attached to a compatible pair (ρ, λ) that is compatible with the map on cochains.

Remark 1.8.4. Given a third group G'', a G''-module A'', and compatible pair (ρ', λ') with $\rho' : G'' \to G'$ and $\lambda' : A' \to A''$, we may speak of the composition $(\rho \circ \rho', \lambda' \circ \lambda)$, which will be a compatible pair that induces the morphism on complexes that is the composition of the morphisms arising from the pairs (ρ, λ) and (ρ', λ').

Example 1.8.5. In Shapiro's Lemma, the inclusion map $H \hookrightarrow G$ and the evaluation at 1 map $\mathrm{CoInd}_H^G(B) \to B$ form a compatible pair inducing the isomorphisms in its statement.

We consider two of the most important examples of compatible pairs, and the maps on cohomology arising from them.

Definition 1.8.6. Let H be a subgroup of G. Let A be a G-module.

a. Let $e : H \hookrightarrow G$ be the natural inclusion map. Then the maps

$$\mathrm{Res} : H^i(G, A) \to H^i(H, A)$$

induced by the compatible pair (e, id_A) on cohomology are known as *restriction maps*.

b. Suppose that H is normal in G. Let $q : G \to G/H$ be the quotient map, and let $\iota : A^H \to A$ be the inclusion map. Then the maps

$$\mathrm{Inf} : H^i(G/H, A^H) \to H^i(G, A)$$

induced by the compatible pair (q, ι) are known as *inflation maps*.

Remark 1.8.7. Restriction of an i-cocycle is just simply that, it is the restriction of the map $f : G^i \to A$ to a map $\mathrm{Res}(f) : H^i \to A$ given by $\mathrm{Res}(f)(h) = f(h)$ for $h \in H^i$. Inflation of an i-cocycle is just as simple: $\mathrm{Inf}(f)(g) = f(\bar{g})$, for $g \in G^i$ and $\bar{g}$ its image in $(G/H)^i$.

Example 1.8.8. In degree 0, the restriction map $\mathrm{Res} : A^G \to A^H$ is simply inclusion, and the inflation map $\mathrm{Inf} : (A^H)^{G/H} \to A^G$ is the identity.

Remarks 1.8.9.

a. Restriction provides a morphism of δ-functors. That is, it provides a sequence of natural transformations between the functors $H^i(G, \cdot)$ and $H^i(H, \cdot)$ on G-modules (which is to say that restriction commutes with G-module homomorphisms) such that for any short exact sequence of G-modules, the maps induced by the natural transformations commute with the connecting homomorphisms in the two resulting long exact sequences.

b. We could merely have defined restriction for $i = 0$ and used dimension shifting to define it for all $i \geq 1$, as follows from the previous remark.

Theorem 1.8.10 (Inflation-Restriction Sequence)**.** *Let G be a group and N a normal subgroup. Let A be a G-module. Then the sequence*

$$0 \to H^1(G/N, A^N) \xrightarrow{\mathrm{Inf}} H^1(G, A) \xrightarrow{\mathrm{Res}} H^1(N, A)$$

is exact. Proof. The injectivity of inflation on cocycles obvious from Remark 1.8.7. Let f be a cocycle in $Z^1(G/N, A^N)$. If $f(\bar{g}) = (g-1)a$ for some $a \in A$ and all $g \in G$, then $a \in A^N$ as $f(\bar{1}) = 0$, so Inf is injective. Also, note that $\mathrm{Res} \circ \mathrm{Inf}(f)(n) = f(\bar{n}) = 0$ for all $n \in N$.

Let $f' \in Z^1(G, A)$ and suppose $\mathrm{Res}(f') = 0$. Then there exists $a \in A$ such that $f'(n) = (n-1)a$ for all $n \in N$. Define $k \in Z^1(G, A)$ by $k(g) = f'(g) - (g-1)a$. Then $k(n) = 0$ for all $n \in N$. We then have

$$k(gn) = gk(n) + k(g) = k(g)$$

for all $g \in G$ and $n \in N$, so k factors through G/N. Also,

$$k(g) = k(g \cdot g^{-1}ng) = k(ng) = nk(g) + k(n) = nk(g),$$

so k has image in A^N. Therefore, k is the inflation of a cocycle in $Z^1(G/N, A^N)$, proving exactness. ∎

In fact, under certain conditions, we have an inflation-restriction sequence on the higher cohomology groups.

Proposition 1.8.11. *Let G be a group and N a normal subgroup. Let A be a G-module. Let $i \geq 1$, and suppose that $H^j(N, A) = 0$ for all $1 \leq j \leq i-1$. Then the sequence*

$$0 \to H^i(G/N, A^N) \xrightarrow{\text{Inf}} H^i(G, A) \xrightarrow{\text{Res}} H^i(N, A)$$

is exact.

Proof. Let A_* be as in (1.7.1). By Theorem 1.8.10 we may assume $i \geq 2$. Since $H^1(N, A) = 0$, taking N-invariants gives the exact sequence

$$0 \to A^N \to \text{CoInd}^G(A)^N \to (A_*)^N \to 0. \tag{1.8.1}$$

By Lemma 1.5.10, $\text{CoInd}^G(A)^N$ is isomorphic to

$$\text{Hom}_{\mathbb{Z}[N]}(\mathbb{Z}[G], A^\circ) \cong \text{Hom}_{\mathbb{Z}}(\mathbb{Z}[G/N], A^\circ) \cong \text{CoInd}^{G/N}(A^\circ),$$

where A° is the underlying abelian group with trivial action. In particular the middle term of (1.8.1) is cohomologically acyclic as a G/N-mod. The connecting map

$$\delta^{i-1} : H^{i-1}(G/N, (A_*)^N) \xrightarrow{\sim} H^i(G/N, A^N)$$

is an isomorphism for $i \geq 2$.

Consider the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^{i-1}(G/N, (A^*)^N) & \xrightarrow{\text{Inf}} & H^{i-1}(G, A^*) & \xrightarrow{\text{Res}} & H^{i-1}(N, A^*) \\ & & \downarrow{\scriptstyle \delta^{i-1}} & & \downarrow{\scriptstyle \delta^{i-1}} & & \downarrow{\scriptstyle \delta^{i-1}} \\ 0 & \longrightarrow & H^i(G/N, A^N) & \xrightarrow{\text{Inf}} & H^i(G, A) & \xrightarrow{\text{Res}} & H^i(N, A). \end{array} \tag{1.8.2}$$

We have already seen that the leftmost vertical map in (1.8.2) is an isomorphism, and since $\text{CoInd}^G(A)$ is an coinduced G-module, the central vertical map in (1.8.2) is an isomorphism. Moreover, as a coinduced G-module, $\text{CoInd}^G(A)$ is also coinduced as an N-module, and therefore the rightmost vertical map in (1.8.2) is also an isomorphism. Therefore, the lower row of (1.8.2) will be exact if the top row is. But the top row is exact by Theorem 1.8.10 if $i = 2$, and by induction if $i > 2$, noting that

$$H^{j-1}(N, A^*) \cong H^j(N, A) = 0$$

for all $2 \leq j < i$. ∎

We consider one other sort of compatible pair, which is conjugation.

Proposition 1.8.12. *Let A be a G-module.*

a. Let H be a subgroup of G. Let $g \in G$, and define $\rho_g : gHg^{-1} \to H$ by $\rho_g(k) = g^{-1}kg$ for $k \in gHg^{-1}$. Define $\lambda_g : A \to A$ by $\lambda_g(a) = ga$. Then (ρ_g, λ_g) forms a compatible pair, and we denote by g^* the resulting map

$$g^* : H^i(H, A) \to H^i(gHg^{-1}, A).$$

We have $g_1^* \circ g_2^* = (g_1 \circ g_2)^*$ for all $g_1, g_2 \in G$.

b. Suppose that N is normal in G. Then $H^i(N,A)$ is a G-module, where $g \in G$ acts as g^*. We refer to the above action as the conjugation action of G. The conjugation action factors through the quotient G/N and turns N-cohomology into a δ-functor from the category of G-modules to the category of (G/N)-modules.

c. The action of conjugation commutes with restriction maps among subgroups of G, which is to say that if $K \leq H \leq G$ and $g \in G$, then the diagram

$$\begin{array}{ccc} H^i(H,A) & \xrightarrow{\text{Res}} & H^i(K,A) \\ \downarrow{\scriptstyle g^*} & & \downarrow{\scriptstyle g^*} \\ H^i(gHg^{-1},A) & \xrightarrow{\text{Res}} & H^i(gKg^{-1},A) \end{array}$$

commutes.

Proof.

a. First, we need check compatibility:

$$\lambda_g(\rho_g(h)a) = g \cdot g^{-1}hga = hga = h\lambda_g(a).$$

Next, we have

$$\lambda_{g_1g_2} = \lambda_{g_1} \circ \lambda_{g_2} \quad \text{and} \quad \rho_{g_1g_2} = \rho_{g_2} \circ \rho_{g_1},$$

so by Remark 1.8.4, composition is as stated.

b. Suppose that $\kappa : A \to B$ is a G-module homomorphism. If $\alpha \in H^i(N,A)$ is the class of $f \in Z^i(N,A)$, then $\kappa^* \circ g^*(\alpha)$ is the class of

$$(n_1, \dots, n_i) \mapsto \kappa(gf(g^{-1}n_1g, \dots, g^{-1}n_ig)) = g\kappa(f(g^{-1}n_1g, \dots, g^{-1}n_ig)),$$

and so has class $g^* \circ \kappa^*(\alpha)$. Moreover, if

$$0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0$$

is an exact sequence of G-modules, then let

$$\delta : H^i(N,C) \to H^{i+1}(N,A)$$

Let $\gamma \in H^i(N,C)$. We must show that $\delta \circ g^*(\gamma) = g^* \circ \delta(\gamma)$. Since ι and π are G-module maps, by what we showed above, we need only show that the differential on $C^i(N,B)$ commutes with the map $g^{\cdot}$ induced by g on cochains. Let $z \in C^i(N,B)$. Then

$$\begin{aligned} g^{\cdot} \circ d^i(z)(n_0, \dots, n_i) &= gd^i(z)(g^{-1}n_0g, \dots, g^{-1}n_ig) \\ &= n_0gz(g^{-1}n_0g, \dots, g^{-1}n_ig) + \sum_{j=1}^{i}(-1)^j f(g^{-1}n_0g, \dots, g^{-1}n_{j-1}n_jg, \dots, g^{-1}n_ig) \\ &\quad + (-1)^{i+1}f(g^{-1}n_0g, \dots, g^{-1}n_{i-1}g) = d^i(g^*(z))(n_0, \dots, n_i). \end{aligned}$$

It only remains to show that the restriction of the action of G on Tate cohomology to N is trivial. This is easily computed on H^0: for $a \in A^N$ and $n \in N$, we have $n^*(a) = na = a$. In general, let A^* be as in (1.7.1) for the group G. The diagram

$$\begin{array}{ccc} H^i(N,A^*) & \xrightarrow{\delta} & H^{i+1}(N,A) \\ \downarrow{\scriptstyle n^*} & & \downarrow{\scriptstyle n^*} \\ H^i(N,A^*) & \xrightarrow{\delta} & H^{i+1}(N,A), \end{array}$$

which commutes what we have already shown. Assuming that n^* is the identity on $H^i(N,B)$ for every G-module B by induction (and in particular for $B = A^*$), we then have that n^* is the identity on $H^{i+1}(N,A)$ as well.

c. Noting Remark 1.8.4, it suffices to check that the compositions of the compatible pairs in question are equal, which is immediate from the definitions. ∎

We note the following corollary.

Corollary 1.8.13. *The conjugation action of G on $H^i(G,A)$ is trivial for all i: that is,*

$$g^*\colon H^i(G,A) \to H^i(G,A)$$

is just the identity for all $g \in G$ and $i \geq 0$.

On homology, the analogous notion of a compatible pair is a pair (ρ, λ) where $\rho\colon G \to G'$ and $\lambda : A \to A'$ are group homomorphisms satisfying

$$\lambda(ga) = \rho(g)\lambda(a) \tag{1.8.3}$$

for all $g \in G$ and $a \in A$. These then provide morphisms

$$\tilde{\rho} \otimes \lambda\colon \mathbb{Z}[G^{i+1}] \otimes_{\mathbb{Z}[G]} A \to \mathbb{Z}[(G')^{i+1}] \otimes_{\mathbb{Z}[G']} A',$$

where $\tilde{\rho}$ is the induced map $\mathbb{Z}[G^{i+1}] \to \mathbb{Z}[(G')^{i+1}]$. By the homological compatibility of (1.8.3), these are seen to be compatible with the differentials, providing maps

$$H_i(G,A) \to H_i(G',A')$$

for all $i \geq 0$. As a consequence, we may make the following definition.

Definition 1.8.14. For $i \geq 0$ and a subgroup H of G, the *corestriction maps*

$$\mathrm{Cor}\colon H_i(H,A) \to H_i(G,A)$$

are defined to be the maps induced by the compatible pair (e, id_A), where $e\colon H \to G$ is the natural inclusion map.

Example 1.8.15. In degree 0, corestriction $\mathrm{Cor}\colon A_H \to A_G$ is just the quotient map.

Definition 1.8.16. For $i \geq 0$ and a normal subgroup H of G, the *coinflation maps*

$$\mathrm{CoInf}\colon H_i(G,A) \to H_i(G/H, A_H)$$

are defined to be the maps induces by the compatible pair (q, π), where $q\colon G \to G/H$ and $\pi : A \to A_H$ are the quotient maps.

Remark 1.8.17. For a G-module A and any normal subgroup H of G, the sequence

$$H_1(H,A) \xrightarrow{\mathrm{Cor}} H_1(G,A) \xrightarrow{\mathrm{CoInf}} H_1(G/H, A_H) \to 0.$$

is exact.

Remark 1.8.18. For a subgroup H of G, the pair (ρ_g^{-1}, λ_g) is a compatible pair for H-homology, inducing conjugation maps

$$g_*\colon H_i(H,A) \to H_i(gHg^{-1}, A).$$

If H is a normal subgroup, then these again provide a (G/H)-action on $H_i(H,A)$ and turn H-homology into a δ-functor. Conjugation commutes with corestriction on subgroups of G.

If H is of finite index in G, then we may define restriction maps on homology and corestriction maps on cohomology as well. If G is finite, then we obtain restriction and corestriction maps on

all Tate cohomology groups as well. Let us first explain this latter case, as it is a bit simpler. Take, for instance, restriction. We have

$$\mathrm{Res}\colon H^i(G,A) \to H^i(H,A)$$

for all $i \geq 0$, so maps on Tate cohomology groups for $i \geq 1$. By Proposition 1.7.3, we have

$$\hat{H}^{i-1}(G,A) \cong \hat{H}^i(G,A_*),$$

and the same holds for H-cohomology, as $\mathrm{Ind}^G(A)$ is also an induced H-module. We define

$$\mathrm{Res}\colon \hat{H}^{i-1}(G,A) \to \hat{H}^{i-1}(H,A)$$

to make the diagram

$$\begin{array}{ccc} \hat{H}^{i-1}(G,A) & \xrightarrow{\sim} & \hat{H}^i(G,A_*) \\ \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} \\ \hat{H}^{i-1}(H,A) & \xrightarrow{\sim} & \hat{H}^i(H,A_*) \end{array}$$

commute.

If we wish to define restriction on homology groups when G is not finite, we need to provide first a definition of restriction on $H_0(G,A)$, so that we can use dimension shifting to define it for $H_i(G,A)$ with $i \geq 1$. Similarly, we need a description of corestriction on $H^0(G,A)$.

Definition 1.8.19. Suppose that H is a finite index subgroup of a group G and A is a G-module.

i. Define

$$\mathrm{Res}\colon H_0(G,A) \to H_0(H,A), \qquad x \mapsto \sum_{\bar{g}\in H\backslash G}{}' g\cdot\tilde{x},$$

where $x \in A_G$ and $\tilde{x} \in A_H$ is any lift of it, and where g denotes any coset representative of $\bar{g} \in H\backslash G$.

ii. Define

$$\mathrm{Cor}\colon H^0(H,A) \to H^0(G,A), \qquad a \mapsto \sum_{\bar{g}\in G/H} g\cdot a$$

where $a \in A^H$ and g is as above.

Proposition 1.8.20. *Let G be a group and H a subgroup of finite index. Then there are maps*

$$\mathrm{Res}\colon H_i(G,A) \to H_i(H,A) \quad \textit{and} \quad \mathrm{Cor}\colon H^i(H,A) \to H^i(G,A)$$

for all $i \geq 0$ that coincide with the maps of Definition 1.8.19 for $i = 0$ and that provide morphisms of δ-functors.

Proof. Again, we consider the case of restriction, that of corestriction being analogous. We have a commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 \longrightarrow & H_1(G,A) & \longrightarrow & H_0(G,A_*) & \longrightarrow & H_0(G,\mathrm{Ind}^G(A)) \\ & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} \\ 0 \longrightarrow & H_1(H,A) & \longrightarrow & H_0(H,A_*) & \longrightarrow & H_0(H,\mathrm{Ind}^G(A)), \end{array}$$

which allows us to define restriction as the induced maps on kernels. For any $i \geq 2$, we proceed as described above in the case of Tate cohomology to define restriction maps on the ith homology groups.

That Res gives of morphism of δ-functors can be proven by induction using dimension shifting and a straightforward diagram chase and is left to the reader. ∎

Remark 1.8.21. Corestriction commutes with conjugation on the cohomology groups of subgroups of G with coefficients in G-modules. In the same vein, restriction commutes with conjugation on the homology of subgroups of G with G-module coefficients.

Corollary 1.8.22. *Let G be finite and H a subgroup. The maps* Res *and* Cor *defined on both homology and cohomology above induce maps*

$$\mathrm{Res}\colon \hat{H}^i(G,A) \to \hat{H}^i(H,A) \quad \textit{and} \quad \mathrm{Cor}\colon \hat{H}^i(H,A) \to \hat{H}^i(G,A)$$

for all $i \in \mathbb{Z}$, and these provide morphisms of δ-functors.

Proof. The reader may check that Res and Cor defined in homological and cohomological degree 0, respectively, induce morphisms on the corresponding Tate cohomology groups. We then have left only to check the commutativity of one diagram in each case.

Suppose that

$$0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0$$

is an exact sequence of G-modules. For restriction, we want to check that

$$\begin{array}{ccc} \hat{H}^{-1}(G,C) & \xrightarrow{\delta} & \hat{H}^0(G,A) \\ \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} \\ \hat{H}^{-1}(H,C) & \xrightarrow{\delta} & \hat{H}^0(H,A) \end{array}$$

commutes. Let c be in the kernel of N_G on C, and denote its image in $H_T^{-1}(G,C)$ by c. Choose $b \in B$ with $\pi(b) = c$ and considering $N_G b \in B^G$, which is $\iota(a)$ for some $a \in A^G$. Then $\delta(c)$ is the image of a in $H_T^0(G,A)$. Then $\mathrm{Res}(\delta(\bar{c}))$ is just the image of a in $H_T^0(H,A)$. On the other hand,

$$\mathrm{Res}(\bar{c}) = \sum_{\bar{g} \in H\backslash G}{}' g\tilde{c},$$

where $\tilde{c}$ is the image of c in $H_T^{-1}(H,C)$. We may lift the latter element to $\sum_{\bar{g}} gc$ in the kernel of N_H on C and then to $\sum_{\bar{g}} gb \in B$. Taking N_H of this element gives us $N_G b$, which is $\iota(a)$, and so $\delta(\mathrm{Res}(\bar{c}))$

is once again the image of a in $H_T^0(H,A)$.

The case of corestriction is very similar, and hence omitted. ∎

The following describes an important relationship between restriction and corestriction.

Proposition 1.8.23. *Let G be a group and H a subgroup of finite index. Then the maps* Cor $\circ$ Res *on homology, cohomology, and, when G is finite, Tate cohomology, are just the multiplication by $[G:H]$ maps.*

Proof. It suffices to prove this on the zeroth homology and cohomology groups. The result then follows by dimension shifting. On cohomology we have the composite map

$$A^G \xrightarrow{\mathrm{Res}} A^H \xrightarrow{\mathrm{Cor}} A^G,$$

where Res is the natural inclusion and Cor the map of Definition 1.8.19. For $a \in A^G$, we have

$$\sum_{g \in G/H}{}' ga = [G:H]a,$$

as desired.

On homology, we have maps

$$A_G \xrightarrow{\text{Res}} A_H \xrightarrow{\text{Cor}} A_G,$$

where Res is as in Definition 1.8.19 and Cor is the natural quotient map. For $x \in A_G$ and $\tilde{x} \in A_H$ lifting it, the element

$$\sum_{g \in H\backslash G} g\tilde{x}$$

has image $[G : H]x$ in A_G, again as desired. ∎

Here is a useful corollary.

Corollary 1.8.24. *Let G_p be a Sylow p-subgroup of a finite group G, for a prime p. Then the kernel of*

$$\text{Res}\colon \hat{H}^i(G,A) \to \hat{H}^i(G_p,A)$$

has no elements of order p. Proof. Let $\alpha \in H^i_T(G,A)$ with $p^n\alpha = 0$ for some $n \geq 0$. Then $\text{Cor}(\text{Res}(\alpha)) = [G : G_p]\alpha$, but $[G : G_p]$ is prime to p, hence $\text{Cor}(\text{Res}(\alpha))$ is nonzero if $\alpha \neq 0$, and therefore $\text{Res}(\alpha)$ cannot be 0 unless $\alpha = 0$. ∎

We then obtain the following.

Corollary 1.8.25. *Let G be a finite group. For each prime p, fix a Sylow p-subgroup G_p of G. Fix $i \in \mathbb{Z}$, and suppose that*

$$\text{Res}\colon \hat{H}^i(G,A) \to \hat{H}^i(G_p,A)$$

is trivial for all primes p. Then $H^i_T(G,A) = 0$.

Proof. The intersection of the kernels of the restriction maps over all p contains no elements of p-power order for any p by Corollary 1.8.24. So, if all of the restriction maps are trivial, the group $H^i_T(G,A)$ must be trivial. ∎

Finally, we remark that we have conjugation Tate cohomology, as in the cases of homology and cohomology.

Remark 1.8.26. Suppose G is finite and $H \leq G$. The conjugation maps on $H^0(H,A)$ and $H_0(H,A)$ induce the conjugation maps in Tate degrees 0 and -1, respectively. In other degrees use the maps on ordinary homology or cohomology. In every degree they give isomorphisms

$$g_*\colon H^i_T(H,A) \xrightarrow{\sim} H^i_T(gHg^{-1},A).$$

For normal H this gives a G/H-action and makes Tate cohomology a δ-functor. Conjugation commutes with restriction and corestriction.

1.9 Cup products

We consider the following maps on the standard complex $P_\cdot$:

$$\kappa_{i,j}\colon P_{i+j} \to P_i \otimes_{\mathbb{Z}} P_j, \qquad \kappa_{i,j}(g_0,\dots,g_{i+j}) = (g_0,\dots,g_i) \otimes (g_i,\dots,g_{i+j}).$$

That is, there is a natural map

$$\text{Hom}_{\mathbb{Z}[G]}(P_i,A) \otimes_{\mathbb{Z}} \text{Hom}_{\mathbb{Z}[G]}(P_j,B) \to \text{Hom}_{\mathbb{Z}[G]}(P_i \otimes_{\mathbb{Z}} P_j, A \otimes_{\mathbb{Z}} B)$$

defined by

$$\varphi \otimes \varphi' \mapsto (\alpha \otimes \beta \mapsto \varphi(\alpha) \otimes \varphi'(\beta)).$$

Composing this with the map induced by precomposition with $\kappa_{i,j}$ gives rise to a map

$$\mathrm{Hom}_{\mathbb{Z}[G]}(P_i, A) \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}[G]}(P_j, B) \xrightarrow{\cup} \mathrm{Hom}_{\mathbb{Z}[G]}(P_{i+j}, A \otimes_{\mathbb{Z}} B),$$

and we denote the image of $\varphi \otimes \varphi'$ under this map by $\varphi \cup \varphi'$. Let us summarize this.

Definition 1.9.1. Let $\varphi \in \mathrm{Hom}_{\mathbb{Z}[G]}(P_i, A)$ and $\varphi' \in \mathrm{Hom}_{\mathbb{Z}[G]}(P_j, B)$. The *cup product* $\varphi \cup \varphi' \in \mathrm{Hom}_{\mathbb{Z}[G]}(P_{i+j}, A \otimes_{\mathbb{Z}} B)$ is defined by

$$(\varphi \cup \varphi')(g_0, \dots, g_{i+j}) = \varphi(g_0, \dots, g_i) \otimes \varphi'(g_i, \dots, g_{i+j}).$$

Lemma 1.9.2. *Let $\varphi \in \mathrm{Hom}_{\mathbb{Z}[G]}(P_i, A)$ and $\varphi' \in \mathrm{Hom}_{\mathbb{Z}[G]}(P_j, B)$. Then*

$$D^{i+j}_{A\otimes B}(\varphi \cup \varphi') = D^i_A(\varphi) \cup \varphi' + (-1)^i \varphi \cup D^j_B(\varphi'),$$

where the differentials D^i are as in (1.3.1).

Proof. We compute the terms. We have

$$\begin{aligned} D^{i+j}_{A\otimes B}(\varphi \cup \varphi')(g_0, \dots, g_{i+j+1}) = &\sum_{k=0}^{i} (-1)^k \varphi(g_0, \dots, \widehat{g_k}, \dots, g_{i+1}) \otimes \varphi'(g_{i+1}, \dots, g_{i+j+1}) \\ &+ \sum_{k=i+1}^{i+j+1} (-1)^k \varphi(g_0, \dots, g_i) \otimes \varphi'(g_i, \dots, \widehat{g_k}, \dots, g_{i+j+1}), \end{aligned}$$

while

$$(D^i_A(\varphi) \cup \varphi')(g_0, \dots, g_{i+j+1}) = \sum_{k=0}^{i+1} (-1)^k \varphi(g_0, \dots, \widehat{g_k}, \dots, g_{i+1}) \otimes \varphi'(g_{i+1}, \dots, g_{i+j+1}) \tag{1.9.1}$$

and

$$(\varphi \cup D^j_B(\varphi'))(g_0, \dots, g_{i+j+1}) = \sum_{k=i}^{j+i+1} (-1)^{k-i} \varphi(g_0, \dots, g_i) \otimes \varphi'(g_i, \dots, \widehat{g_j}, \dots, g_{i+j+1}). \tag{1.9.2}$$

As $(-1)^{i+1} + (-1)^i = 0$, the last term in (1.9.1) cancels with the $(-1)^i$ times the first term in (1.9.2). The equality of the two sides follows. ∎

Remark 1.9.3. On cochains, we can define cup products

$$C^i(G, A) \otimes_{\mathbb{Z}} C^j(G, B) \xrightarrow{\cup} C^{i+j}(G, A \otimes_{\mathbb{Z}} B)$$

of $f \in C^i(G, A)$ and $f' \in C^j(G, B)$ by

$$(f \cup f')(g_1, g_2, \dots g_{i+j}) = f(g_1, \dots, g_i) \otimes g_1 g_2 \cdots g_i f'(g_{i+1}, \dots, g_{i+j}).$$

To see that these match up with the previous definition, note that if we define φ and φ' by

$$\varphi(1, g_1, \dots, g_1 \cdots g_i) = f(g_1, \dots, g_i) \quad \text{and} \quad \varphi'(1, g_1, \dots, g_1 \cdots g_j) = f'(g_1, \dots, g_j),$$

then

$$\begin{aligned} (f \cup f')(g_1, \dots, g_{i+j}) &= \varphi(1, g_1, \dots, g_1 \cdots g_i) \cup g_1 g_2 \cdots g_i \varphi(1, g_{i+1}, \dots, g_{i+1} \cdots g_{i+j+1}) \\ &= \varphi(1, g_1, \dots, g_1 \cdots g_i) \cup \varphi(g_1 \cdots g_i, g_1 \cdots g_{i+1}, \dots, g_1 \cdots g_{i+j+1}) \\ &= (\varphi \cup \varphi')(1, g_1, \dots, g_1 \cdots g_{i+j+1}), \end{aligned}$$

so the definitions agree under the identifications of Theorem 1.3.3. As a consequence of Lemma 1.9.2, the cup products on cochains satisfy

$$d^{i+j}_{A\otimes B}(f \cup f') = d^i_A(f) \cup f' + (-1)^i f \cup d^j_B(f'). \tag{1.9.3}$$

Lemma 1.9.4. *The sequences*

$$0 \to A \otimes_{\mathbb{Z}} B \to \mathrm{CoInd}^G(A) \otimes_{\mathbb{Z}} B \to A^* \otimes_{\mathbb{Z}} B \to 0 \tag{1.9.4}$$

$$0 \to A_* \otimes_{\mathbb{Z}} B \to \mathrm{Ind}^G(A) \otimes_{\mathbb{Z}} B \to A \otimes_{\mathbb{Z}} B \to 0 \tag{1.9.5}$$

are exact for any G-modules A and B.

Proof. Since the augmentation map ε is split over $\mathbb{Z}$, it follows using Remark 1.7.1 that the sequences (1.7.1) and (1.7.2) are split as well. It follows that the sequences in the lemma are exact. ∎

Theorem 1.9.5. *The cup products of Definition 1.9.1 induce maps, also called cup products,*

$$H^i(G,A) \otimes_{\mathbb{Z}} H^j(G,B) \xrightarrow{\cup} H^{i+j}(G, A \otimes_{\mathbb{Z}} B)$$

that are natural in A and B and satisfy the following properties:

(i) For $i = j = 0$, one has that the cup product

$$A^G \otimes_{\mathbb{Z}} B^G \to (A \otimes_{\mathbb{Z}} B)^G$$

is induced by the identity on $A \otimes_{\mathbb{Z}} B$.

(ii) If

$$0 \to A_1 \to A \to A_2 \to 0$$

is an exact sequence of G-modules such that

$$0 \to A_1 \otimes_{\mathbb{Z}} B \to A \otimes_{\mathbb{Z}} B \to A_2 \otimes_{\mathbb{Z}} B \to 0$$

is exact as well, then

$$\delta(\alpha_2 \cup \beta) = (\delta\alpha_2) \cup \beta \in H^{i+j+1}(G, A_1 \otimes_{\mathbb{Z}} B)$$

for all $\alpha_2 \in H^i(G,A_2)$ and $\beta \in H^j(G,B)$. (In other words, cup product on the right with a cohomology class provides a morphism of δ-functors.)

(iii) If

$$0 \to B_1 \to B \to B_2 \to 0$$

is an exact sequence of G-modules such that

$$0 \to A \otimes_{\mathbb{Z}} B_1 \to A \otimes_{\mathbb{Z}} B \to A \otimes_{\mathbb{Z}} B_2 \to 0$$

is exact as well, then

$$\delta(\alpha \cup \beta_2) = (-1)^i \alpha \cup (\delta\beta_2) \in H^{i+j+1}(G, A \otimes_{\mathbb{Z}} B_1)$$

for all $\alpha \in H^i(G,A)$ and $\beta_2 \in H^j(G,B_2)$.

Moreover, the cup products on cohomology are the unique collection of such maps natural in A and B and satisfying properties (i), (ii), and (iii).

Proof. Let $f \in C^i(G,A)$ and $f' \in C^j(G,B)$. By (1.9.3), it is easy to see that the cup product of two cocycles is a cocycle and that the cup product of a cocycle and a coboundary is a coboundary. Thus, the cup product on cochains induces cup products on cohomology. The naturality in A and B follows directly from the definition. Property (i) is immediate from the definition as well. Property (ii) can be seen by tracing through the definition of the connecting homomorphism. Let f_2 represent α_2. Then $\delta(\alpha_2)$ is obtained by lifting f_2 to a cochain $f \in C^i(G,A)$, taking its boundary $df \in C^{i+1}(G,A)$, and then noting that df is the image of some cocycle $z_1 \in Z^{i+1}(G,A_1)$. Let

$f' \in Z^j(G,B)$ represent β. By (1.9.3), we have $df \cup f' = d(f \cup f')$. Note that $z_1 \cup f'$ has class $\delta(\alpha_2) \cup \beta$ and image $df \cup f'$ in $C^{i+j+1}(G, A \otimes_{\mathbb{Z}} B)$. On the other hand, $d(f \cup f')$ is the image of a cocycle representing $\delta(\alpha_2 \cup \beta)$, as $f \cup f'$ is a cocycle lifting $f_2 \cup f'$. Since the map

$$C^{i+j+1}(G, A_1 \otimes_{\mathbb{Z}} B) \to C^{i+j+1}(G, A \otimes_{\mathbb{Z}} B)$$

is injective, we have (ii). Property (iii) follows similarly, the sign appearing in the computation arising from (1.9.3).

The uniqueness of the maps with these properties follows from the fact that given a collection of such maps, property (i) specifies them uniquely for $i = j = 0$, while properties (ii) and (iii) specify them uniquely for all other $i, j \geq 0$ by dimension shifting. For instance, by (ii) and Lemma 1.9.4, we have a commutative square

$$\begin{array}{ccc} H^i(G,A^*) \otimes_{\mathbb{Z}} H^j(G,B) & \xrightarrow{\cup} & H^{i+j}(G, A^* \otimes_{\mathbb{Z}} B) \\ \downarrow & & \downarrow \\ H^{i+1}(G,A) \otimes_{\mathbb{Z}} H^j(G,B) & \xrightarrow{\cup} & H^{i+j+1}(G, A \otimes_{\mathbb{Z}} B) \end{array}$$

in which the lefthand vertical arrow is a surjection for all i (and an isomorphism for $i \geq 1$). Thus, the cup products in degrees (i,j) for $i \geq 1$ and $j \geq 0$ specify by the cup products in degrees $(i+1, j)$. Similarly, using (iii), we see that the cup products in degrees (i,j) specify the cup products in degrees $(i, j+1)$. ∎

Remark 1.9.6. Associativity of tensor products and Lemma 1.5.10 tell us that

$$\mathrm{Ind}^G(A \otimes_{\mathbb{Z}} B) \cong \mathrm{Ind}^G(A) \otimes_{\mathbb{Z}} B,$$

so in particular the latter modules is induced. This also implies that we have isomorphisms

$$(A \otimes_{\mathbb{Z}} B)_* \cong A_* \otimes_{\mathbb{Z}} B.$$

If G is finite, Proposition 1.5.4 tells us that we have

$$\mathrm{CoInd}^G(A \otimes_{\mathbb{Z}} B) \cong \mathrm{CoInd}^G(A) \otimes_{\mathbb{Z}} B \quad \text{and} \quad (A \otimes_{\mathbb{Z}} B)^* \cong A^* \otimes_{\mathbb{Z}} B$$

as well.

Corollary 1.9.7. *Consider the natural isomorphism*

$$s_{AB} \colon A \otimes_{\mathbb{Z}} B \to B \otimes_{\mathbb{Z}} A$$

given by $a \otimes b \mapsto b \otimes a$, and the maps that it induces on cohomology. For all $\alpha \in H^i(G,A)$ and $\beta \in H^j(G,B)$, one has that

$$s_{AB}^*(\alpha \cup \beta) = (-1)^{ij}(\beta \cup \alpha).$$

Proof. We first verify the result in the case $i = j = 0$. For $a \in A^G$ and $b \in B^G$, we have

$$s_{AB}^*(a \cup b) = s_{AB}(a \otimes b) = b \otimes a = b \cup a.$$

Suppose that we know the result for a given pair $(i-1, j)$. Let $\alpha \in H^i(G,A)$ and $\beta \in H^j(G,B)$. Recall that the maps $H^{i-1}(G,A^*) \to H^i(G,A)$ are surjective for all $i \geq 1$ (and isomorphisms for $i \geq 2$), and write $\alpha = \delta(\alpha^*)$ for some $\alpha^* \in H^{i-1}(G,A^*)$. Since (1.9.4) is exact, we have by Theorem 1.9.5 that

$$\begin{aligned} s_{AB}^*(\alpha \cup \beta) = s_{AB}^*(\delta(\alpha^*) \cup \beta) = s_{AB}^*(\delta(\alpha^* \cup \beta)) = \delta(s_{AB}^*(\alpha^* \cup \beta)) \\ = (-1)^{(i-1)j}\delta(\beta \cup \alpha^*) = (-1)^{(i-1)j}(-1)^j \beta \cup \delta(\alpha^*) = (-1)^{ij}\beta \cup \alpha. \end{aligned}$$

Suppose next that we know the result for a given pair $(i, j-1)$. Let $\alpha \in H^i(G,A)$ and $\beta \in H^{j-1}(G,B)$, and write $\beta = \delta(\beta^*)$ for some $\beta^* \in H^j(G,B^*)$. Since (1.9.4) is exact, we have by Theorem 1.9.5 that

$$\begin{aligned} s^*_{AB}(\alpha \cup \beta) = s^*_{AB}(\alpha \cup \delta(\beta^*)) &= (-1)^i s^*_{AB}(\delta(\alpha \cup \beta^*)) = \delta(s^*_{AB}(\alpha \cup \beta^*)) \\ &= (-1)^i(-1)^{i(j-1)}\delta(\beta^* \cup \alpha) = (-1)^{ij}\delta(\beta^*) \cup \alpha = (-1)^{ij}\beta \cup \alpha. \end{aligned}$$

The result now follows by induction on i and j. ∎

Cup products also have an associative property, which can be checked directly on cochains.

Proposition 1.9.8. *Let A, B, and C be G-modules, and let $\alpha \in H^i(G,A)$, $\beta \in H^j(G,B)$, and $\gamma \in H^k(G,C)$. Then*

$$(\alpha \cup \beta) \cup \gamma = \alpha \cup (\beta \cup \gamma) \in H^{i+j+k}(G, A \otimes_{\mathbb{Z}} B \otimes_{\mathbb{Z}} C).$$

Often, when we speak of cup products, we apply an auxiliary map from the tensor product of A and B to a third module before taking the result. For instance, if $A = B = \mathbb{Z}$, then one will typically make the identification $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Z}$. We codify this in the following definition.

Definition 1.9.9. Suppose that A, B, and C are G-modules and $\theta : A \otimes_{\mathbb{Z}} B \to C$ is a G-module homomorphism. Then the maps

$$H^i(G,A) \otimes_{\mathbb{Z}} H^j(G,B) \to H^{i+j}(G,C), \qquad \alpha \otimes \beta \mapsto \theta(\alpha \cup \beta)$$

are also referred to as cup products. When θ is understood, we denote $\theta(\alpha \cup \beta)$ more simply by $\alpha \cup \beta$.

Cup products behave nicely with respect to restriction, corestriction, and inflation.

Proposition 1.9.10. *Let A and B be G-modules. We then have the following compatibilities.*

a. Let H be a subgroup of G. For $\alpha \in H^i(G,A)$ and $\beta \in H^j(G,B)$, one has

$$\mathrm{Res}(\alpha \cup \beta) = \mathrm{Res}(\alpha) \cup \mathrm{Res}(\beta) \in H^{i+j}(H, A \otimes_{\mathbb{Z}} B),$$

where Res *denotes restriction from G to H.*

b. Let N be a normal subgroup of G. For $\alpha \in H^i(G/N, A^N)$ and $\beta \in H^j(G/N, B^N)$, one has

$$\mathrm{Inf}(\alpha \cup \beta) = \mathrm{Inf}(\alpha) \cup \mathrm{Inf}(\beta) \in H^{i+j}(G, A \otimes_{\mathbb{Z}} B),$$

where Inf *denotes inflation from G/N to G. (Here, we implicitly use the canonical map $A^N \otimes_{\mathbb{Z}} B^N \to (A \otimes_{\mathbb{Z}} B)^N$ prior to taking inflation on the left.)*

c. Let H be a subgroup of finite index in G. For $\alpha \in H^i(H,A)$ and $\beta \in H^j(G,B)$, one has

$$\mathrm{Cor}(\alpha) \cup \beta = \mathrm{Cor}(\alpha \cup \mathrm{Res}(\beta)) \in H^{i+j}(G, A \otimes_{\mathbb{Z}} B),$$

where Res *denotes restriction from G to H and* Cor *denotes corestriction from H to G.*

Proof. For part a, let $f \in Z^i(G,A)$, $f' \in Z^j(G,B)$, and $h_1, \dots, h_{i+j} \in H$. The restriction of $f \smile f'$ at these inputs is

$$f(h_1, \dots, h_i) \otimes (h_1 \cdots h_i) f'(h_{i+1}, \dots, h_{i+j}).$$

This is the value of $\mathrm{Res}(f) \smile \mathrm{Res}(f')$ on the same inputs, so passing to cohomology proves part a.

Part b is similarly computed.

We now prove part c. In degree $i = j = 0$, take $a \in A^H$ and $b \in B^G$. The definition of corestriction gives

$$\mathrm{Cor}(a) \smile b = \sum_{gH \in G/H} (ga) \otimes b = \sum_{gH \in G/H} g(a \otimes b) = \mathrm{Cor}(a \smile \mathrm{Res}(b)).$$

Restriction and corestriction commute with connecting maps, and cup products satisfy the connecting-map formulas of Theorem 1.9.5. Suppose the result is known in degrees $(i-1, j)$ and $i > 0$. The exact sequence (1.7.1) for A remains acyclic in its middle term after restriction to H. Choose $\alpha_* \in H^{i-1}(H, A_*)$ with $\delta(\alpha_*) = \alpha$. Then

$$\begin{aligned}\mathrm{Cor}(\alpha) \smile \beta &= \delta\big(\mathrm{Cor}(\alpha_*) \smile \beta\big) \\ &= \delta\big(\mathrm{Cor}(\alpha_* \smile \mathrm{Res}(\beta))\big) \\ &= \mathrm{Cor}\big(\delta(\alpha_* \smile \mathrm{Res}(\beta))\big) = \mathrm{Cor}(\alpha \smile \mathrm{Res}(\beta)).\end{aligned}$$

Similarly, if the result is known in degrees $(i, j-1)$, choose $\beta_* \in H^{j-1}(G, B_*)$ with $\delta(\beta_*) = \beta$. Then

$$\begin{aligned}\mathrm{Cor}(\alpha) \smile \beta &= (-1)^i \delta\big(\mathrm{Cor}(\alpha) \smile \beta_*\big) \\ &= (-1)^i \delta\big(\mathrm{Cor}(\alpha \smile \mathrm{Res}(\beta_*))\big) \\ &= \mathrm{Cor}\big(\alpha \smile \delta(\mathrm{Res}(\beta_*))\big) = \mathrm{Cor}(\alpha \smile \mathrm{Res}(\beta)).\end{aligned}$$

These identities prove the projection formula in $H^{i+j}(G, A \otimes_{\mathbb{Z}} B)$. ∎

Notation 1.9.11. We may express the statement of Proposition 1.9.10a as saying that the diagram

$$\begin{array}{ccc} H^i(G,A) \otimes_{\mathbb{Z}} H^j(G,B) & \xrightarrow{\cup} & H^i(G, A \otimes_{\mathbb{Z}} B) \\ \downarrow{\scriptstyle \mathrm{Res}} \quad \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} \\ H^i(H,A) \otimes_{\mathbb{Z}} H^j(H,B) & \xrightarrow{\cup} & H^i(H, A \otimes_{\mathbb{Z}} B) \end{array}$$

commutes (with a similar diagram for part b) and the statement of Proposition 1.9.10c as saying that the diagram

$$\begin{array}{ccc} H^i(G,A) \otimes_{\mathbb{Z}} H^j(G,B) & \xrightarrow{\cup} & H^i(G, A \otimes_{\mathbb{Z}} B) \\ \uparrow{\scriptstyle \mathrm{Cor}} \quad \downarrow{\scriptstyle \mathrm{Res}} & & \uparrow{\scriptstyle \mathrm{Cor}} \\ H^i(H,A) \otimes_{\mathbb{Z}} H^j(H,B) & \xrightarrow{\cup} & H^i(H, A \otimes_{\mathbb{Z}} B) \end{array}$$

commutes.

For finite groups, we have cup products on Tate cohomology as well.

Theorem 1.9.12. *Let G be finite. There exists a unique family of maps*

$$\hat{H}^i(G,A) \otimes_{\mathbb{Z}} \hat{H}^j(G,B) \xrightarrow{\cup} \hat{H}^{i+j}(G, A \otimes_{\mathbb{Z}} B)$$

with $i, j \in \mathbb{Z}$ that are natural in the G-modules A and B and which satisfy the following properties:

(i) The diagram

$$\begin{array}{ccc} H^0(G,A) \otimes_{\mathbb{Z}} H^0(G,B) & \xrightarrow{\cup} & H^0(G, A \otimes_{\mathbb{Z}} B) \\ \downarrow & & \downarrow \\ \hat{H}^0(G,A) \otimes_{\mathbb{Z}} \hat{H}^0(G,B) & \xrightarrow{\cup} & \hat{H}^0(G, A \otimes_{\mathbb{Z}} B) \end{array}$$

commutes.

(ii) If

$$0 \to A_1 \to A \to A_2 \to 0$$

is an exact sequence of G-modules such that

$$0 \to A_1 \otimes_{\mathbb{Z}} B \to A \otimes_{\mathbb{Z}} B \to A_2 \otimes_{\mathbb{Z}} B \to 0$$

is exact as well, then

$$\delta(\alpha_2 \cup \beta) = (\delta\alpha_2) \cup \beta \in \hat{H}^{i+j+1}(G, A_1 \otimes_{\mathbb{Z}} B)$$

for all $\alpha_2 \in \hat{H}^i(G, A_2)$ and $\beta \in H_T^j(G, B)$.

(iii) If

$$0 \to B_1 \to B \to B_2 \to 0$$

is an exact sequence of G-modules such that

$$0 \to A \otimes_{\mathbb{Z}} B_1 \to A \otimes_{\mathbb{Z}} B \to A \otimes_{\mathbb{Z}} B_2 \to 0$$

is exact as well, then

$$\delta(\alpha \cup \beta_2) = (-1)^i \alpha \cup (\delta\beta_2) \in \hat{H}^{i+j+1}(G, A \otimes_{\mathbb{Z}} B_1)$$

for all $\alpha \in H_T^i(G, A)$ and $\beta_2 \in \hat{H}^j(G, B_2)$.

Proof. Consider the complex $Q_\cdot$ of Theorem 1.6.10, obtained from the standard resolution $P_\cdot$. The proof goes through as in Theorem 1.9.5 once we define maps $Q_{i+j} \to Q_i \otimes_{\mathbb{Z}} Q_j$ satisfying the formula of Lemma 1.9.2. There are six cases to consider (the case $i, j \geq 0$ being as before), and these are omitted. ∎

Remark 1.9.13. Corollary 1.9.7, Proposition 1.9.8, and the restriction and projection formulas of Proposition 1.9.10 extend to Tate cup products. The ordinary inflation formula is used in positive input degrees. Ordinary inflation does not descend unchanged in degree zero: for $G = C_4$, $N = C_2$, and trivial coefficients $\mathbb{Z}$, the identity on invariants does not induce $\mathbb{Z}/2 \to \mathbb{Z}/4$. In the homological range ordinary co-inflation instead goes from $H_i(G, A)$ to $H_i(G/N, A_N)$. We may also compose cup products with equivariant maps out of the tensor product and denote the composite by the same symbol.

1.10 Tate cohomology of cyclic groups

In this section, let G be a cyclic group of finite order. We prove that the Tate cohomology groups with coefficients in a module A are periodic in the degree of period 2, up to isomorphisms determined by a choice of generator g of G.

The first thing that we will observe is that for such a group G, there is an even nicer projective resolution of $\mathbb{Z}$ than the standard one: i.e., consider the sequence

$$\cdots \to \mathbb{Z}[G] \xrightarrow{N_G} \mathbb{Z}[G] \xrightarrow{g-1} \mathbb{Z}[G] \xrightarrow{N_G} \mathbb{Z}[G] \xrightarrow{g-1} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \to 0, \tag{1.10.1}$$

where the boundary maps are multiplication N_G in even degree and by $g - 1$ in odd degree. We can splice this together with its dual as in Theorem 1.6.10.

Proposition 1.10.1. *The G-cohomology groups of A are the cohomology groups of the complex*

$$\cdots \to A \xrightarrow{g-1} A \xrightarrow{N_G} A \xrightarrow{g-1} A \to \cdots,$$

with a map $g-1$ following the term in degree 0. Proof. Note first that for $i \in \{-1, 0\}$, the group $H_T^i(G, A)$ is by definition isomorphic to the ith cohomology group of the complex in question. Let $C_\cdot$ denote the projective resolution of $\mathbb{Z}$ given by (1.10.1). The complex $C_\cdot \otimes_{\mathbb{Z}[G]} A$ that ends

$$\cdots \to A \xrightarrow{g-1} A \xrightarrow{N_G} A \xrightarrow{g-1} A \to 0$$

computes $H_i(G, A)$, yielding the result for $i \leq -2$.

Multiplication by g induces the endomorphism

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A), \qquad \varphi \mapsto (x \mapsto \varphi(gx) = g\varphi(x)).$$

Via the isomorphism of G-modules $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) \xrightarrow{\sim} A$ given by evaluation at 1, the latter endomorphism is identified with multiplication by g on A. The complex $\mathrm{Hom}_{\mathbb{Z}[G]}(C_\cdot, A)$ that computes $H^i(G, A)$ is therefore isomorphic to

$$0 \to A \xrightarrow{g-1} A \xrightarrow{N_G} A \xrightarrow{g-1} A \to \cdots,$$

providing the result for $i \geq 1$. ∎

Corollary 1.10.2. *For any $i \in \mathbb{Z}$, we have*

$$\hat{H}^i(G, A) \cong \begin{cases} \hat{H}^0(G, A) & i \text{ even} \\ \hat{H}^{-1}(G, A) & i \text{ odd.} \end{cases}$$

We show that, in fact, these isomorphisms can be realized by means of a cup product. As usual, consider $\mathbb{Z}$ as having a trivial G-action. We remark that

$$\hat{H}^{-2}(G, \mathbb{Z}) \cong H_1(G, \mathbb{Z}) \cong G^{\mathrm{ab}} \cong G$$

by Proposition 1.4.5. Any choice of generator g of G is now a generator u_g of this Tate cohomology group. Note that $\mathbb{Z} \otimes_{\mathbb{Z}} A \cong A$ for any G-module A via multiplication. Here then is the result.

Proposition 1.10.3. *Let G be cyclic with generator g, and let A be a G-module. Then the map*

$$\hat{H}^i(G, A) \to \hat{H}^{i-2}(G, A), \qquad c \mapsto u_g \cup c$$

is an isomorphism for any $i \in \mathbb{Z}$.

Proof. Consider the two exact sequences of G-modules:

$$0 \to I_G \to \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \to 0 \quad \text{and} \quad 0 \to \mathbb{Z} \xrightarrow{N_G} \mathbb{Z}[G] \xrightarrow{g-1} I_G \to 0.$$

As $\hat{H}^i(G, \mathbb{Z}[G]) = 0$ for all $i \in \mathbb{Z}$, we then have two isomorphisms

$$\hat{H}^{-2}(G, \mathbb{Z}) \xrightarrow{\delta} \hat{H}^{-1}(G, I_G) \xrightarrow{\delta} \hat{H}^0(G, \mathbb{Z}).$$

(In fact, tracing it through, one sees that the image of u_g under this composition is 1 modulo $|G|$. This is not needed for the proof.)

Since we have

$$\delta(\delta(u_g)) \cup c = \delta(\delta(u_g \cup c))$$

by property (ii) of Theorem 1.9.12, it suffices to show that cup product with the image of 1 in $H^0_T(G,\mathbb{Z})$ is an isomorphism. For this, using property (iii) of Theorem 1.9.12 to dimension shift, the problem reduces to the case that $i = 0$. In this case, we know that the cup product is induced on $\hat{H}^0$ by the multiplication map on H^0's:

$$\mathbb{Z} \otimes_{\mathbb{Z}} A^G \to A^G, \qquad m \otimes a \mapsto ma.$$

However, $1 \cdot a = a$, so the map $\hat{H}^0(G,A) \to \hat{H}^0(G,A)$ induced by taking cup product with the image of 1 is an isomorphism. ∎

Given the 2-periodicity of the Tate cohomology groups of a finite cyclic group, we can make the following definition.

Definition 1.10.4. Let G be a finite cyclic group and A a G-module. Set $h_0(A) = |\hat{H}^0(G,A)|$ and $h_1(A) = |\hat{H}^1(G,A)|$, taking them to be infinite when the orders of the Tate cohomology groups are infinite. If both $h_0(A)$ and $h_1(A)$ are finite, we then define the *Herbrand quotient* $h(A)$ by

$$h(A) = \frac{h_0(A)}{h_1(A)}.$$

Clearly, if A is finitely generated, then $h(A)$ will be defined. The following explains how Herbrand quotients behave with respect to modules in short exact sequences.

Theorem 1.10.5. *Let*

$$0 \to A \to B \to C \to 0$$

be an exact sequence of G-modules. Suppose that any two of $h(A)$, $h(B)$, and $h(C)$ are defined. Then the third is as well, and

$$h(B) = h(A) \cdot h(C).$$

Proof. It follows immediately from Proposition 1.10.3 that we have an exact hexagon

$$\begin{array}{ccccc} & & \hat{H}^0(G,A) & \longrightarrow & \hat{H}^0(G,B) & & \\ & \nearrow & & & & \searrow & \\ \hat{H}^1(G,C) & & & & & & \hat{H}^0(G,C) \\ & \nwarrow & & & & \swarrow & \\ & & \hat{H}^1(G,B) & \longleftarrow & \hat{H}^1(G,A) & & \end{array}.$$

Note that the order of any group in the hexagon is the product of the orders of the image of the map from the previous group and the order of the image of the map to the next group. Therefore, that any two of $h(A)$, $h(B)$, and $h(C)$ are finite implies the third is. When all three are finite, an Euler characteristic argument then tells us that

$$\frac{h_0(A) \cdot h_0(C) \cdot h_1(B)}{h_0(B) \cdot h_1(A) \cdot h_1(C)} = 1, \tag{1.10.2}$$

hence the result. More specifically, the order of each cohomology group is the product of the orders of the images of two adjacent maps in the hexagon, and the order of the image of each such map then appears once in each of the numerator and denominator of the left-hand side of (1.10.2). ∎

As an immediate consequence of Theorem 1.10.5, we have the following.

Corollary 1.10.6. Suppose $0 \to A_1 \to \cdots \to A_n \to 0$ is an exact sequence of G-mods, and the Herbrand quotient is defined for all terms except possibly one. Then it is defined for every term and

$$\prod_{k=1}^{n} h_G(A_k)^{(-1)^k} = 1.$$

Split the long exact sequence at its images and apply multiplicativity in short exact sequences from both ends. Finiteness on alternating terms alone is insufficient. For $G = C_2$, take $M = \bigoplus_{j\geq 1} \mathbb{F}_2$ with trivial action and $P = \bigoplus_{j\geq 1} \mathbb{F}_2[G]$. The augmentation sequences give $0 \to 0 \to M \to P \to M \to 0$. The first and third terms have defined quotients, whereas the second and fourth do not.

Next, we show that the Herbrand quotients of finite modules are trivial.

Proposition 1.10.7. *Suppose that A is a finite G-module. Then $h(A) = 1$.*

Proof. Let g be a generator of G, and note that the sequence

$$0 \to A^G \to A \xrightarrow{g-1} A \to A_G \to 0$$

is exact. As A is finite and any alternating product of orders of finite groups in exact sequences of finite length is 1, we therefore have $|A^G| = |A_G|$. On the other hand, we have the exact sequence

$$0 \to \hat{H}^{-1}(G,A) \to A_G \xrightarrow{\tilde{N}_G} A^G \to \hat{H}^0(G,A) \to 0$$

defining $H_T^i(G,A)$ for $i = 0, -1$. As $h_1(A) = |\hat{H}^{-1}(G,A)|$, we therefore have $h(A) = 1$. ∎

We therefore have the following.

Proposition 1.10.8. *Let $f : A \to B$ be a G-module homomorphism with finite kernel and cokernel. Then $h(A) = h(B)$ if either one is defined.*

Proof. This follows immediately from the exact sequence

$$0 \to \ker f \to A \to B \to \operatorname{coker} f \to 0,$$

Corollary 1.10.6, and Proposition 1.10.7. ∎

Arithmetic applications of the Herbrand quotient

For a cyclic extension L/K of nonarchimedean local fields of degree n, use the valuation exact sequence $1 \to \mathcal{O}_L^\times \to L^\times \to \mathbb{Z} \to 0$. The unit computation in Chapter 2, §2 gives $h_G(\mathcal{O}_L^\times) = 1$. Since $h_G(\mathbb{Z}) = n$ and Hilbert 90 gives $H_T^1(G, L^\times) = 0$, multiplicativity yields

$$[K^\times : N_{L/K}(L^\times)] = h_G(L^\times) = n.$$

For a cyclic extension of number fields, choose S containing the infinite and ramified places, and enlarge it so that the S-idèles surject onto C_L. Shapiro and the local quotients give $h_G(I_{L,S}) = \prod_{v\in S}[L_w : K_v]$. The S-unit theorem compares the unit lattice with the augmentation kernel of the permutation lattice on the places over S, giving $h_G(U_{L,S}) = n^{-1}\prod_{v\in S}[L_w : K_v]$. Taking the quotient gives $h_G(C_L) = n$, and hence

$$[C_K : N_{L/K}C_L] = n\,|H_T^1(G, C_L)| \geq n.$$

This is the first inequality in Chapter 5, §4.

1.11 Cohomological triviality

In this section, we suppose that G is a finite group.

Definition 1.11.1. A G-module A is *cohomologically trivial* if $H_T^i(H, A) = 0$ for all subgroups $H \leq G$ and all $i \in \mathbb{Z}$.

Proposition 1.11.8. Let G be a finite group and choose a Sylow p-subgroup G_p of G for each prime p dividing $|G|$. A G-module A is cohomologically trivial if and only if A is cohomologically trivial as a G_p-module for each p.

Proof. If A is cohomologically trivial over G, its restriction to each G_p is cohomologically trivial by Definition 1.11.1. Conversely, suppose A is cohomologically trivial over each G_p and let $H \leq G$. A Sylow p-subgroup H_p of H lies in some conjugate gG_pg^{-1}. Hence

$$H_T^i(g^{-1}H_pg, A) = 0.$$

The conjugation isomorphism g_* from Remark 1.8.26 gives $H_T^i(H_p, A) = 0$. Thus the restriction $\mathrm{Res}: H_T^i(H, A) \to H_T^i(H_p, A)$ is zero for each p. By Corollary 1.8.25, $H_T^i(H, A) = 0$ for every $i \in \mathbb{Z}$. ∎

Proposition 1.11.8 reduces the study of cohomologically trivial modules over finite groups to the case of finite p-groups. We now turn to criteria for cohomological triviality.

Remark 1.11.2. Every free G-module is also a free H-module for every subgroup H of G and any group G, not necessarily finite. In particular, $\mathbb{Z}[G]$ is free over $\mathbb{Z}[H]$ on any set of cosets representatives of $H\backslash G$.

We remark that it follows from this that induced G-modules are induced H-modules, as direct sums commute with tensor products. We then have the following examples of cohomologically trivial modules.

Examples 1.11.3.

a. Induced G-modules are cohomologically trivial by Proposition 1.6.7.

b. Projective G-modules are cohomologically trivial. To see this, suppose that P and Q are projective G-modules with $P \oplus Q$ free over $\mathbb{Z}[G]$, hence over $\mathbb{Z}[H]$. Then

$$\hat{H}^i(H, P) \hookrightarrow \hat{H}^i(H, P) \oplus \hat{H}^i(H, Q) \cong \hat{H}^i(H, P \oplus Q) = 0$$

for all $i \in \mathbb{Z}$.

We need some preliminary lemmas. Fix a prime p.

Lemma 1.11.4. *Suppose that G is a p-group and that A is a G-module of exponent dividing p. Then $A = 0$ if and only if $A_G = 0$ and if and only if $A^G = 0$.* *Proof.* Suppose $A^G = 0$, and let $a \in A$. The submodule B of A generated by a is finite, and $B^G = 0$. The latter fact implies that the G-orbits in B are either $\{0\}$ or have order a multiple of p. Since B has p-power order, this forces the order to be 1, so $B = 0$. Since a was arbitrary, $A = 0$. On the other hand, if $A_G = 0$, then $X = \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{F}_p)$ satisfies $pX = 0$ and

$$X^G = \mathrm{Hom}_{\mathbb{Z}[G]}(A, \mathbb{F}_p) = \mathrm{Hom}_{\mathbb{Z}[G]}(A_G, \mathbb{F}_p) = 0.$$

By the invariants case just proven, we know $X = 0$, so $A = 0$. ∎

Lemma 1.11.5. Suppose G is a finite p-group and $pA = 0$. If $H_1(G, A) = 0$, then A is free as an $\mathbb{F}_p[G]$-mod.

Proof. Lift an $\mathbb{F}_p$-basis of A_G to a subset Σ of A. If B is the submod generated by Σ, then $(A/B)_G = 0$. Lemma 1.11.4 gives $A/B = 0$. Let F be the free $\mathbb{F}_p[G]$-mod on Σ, let $\pi : F \to A$ be the induced surjection, and put $R = \ker \pi$. The homology sequence and $H_1(G, A) = 0$ give

$$0 \to R_G \to F_G \xrightarrow{\bar{\pi}} A_G \to 0.$$

By construction $\bar{\pi}$ is an isomorphism, so $R_G = 0$. As $pR = 0$, Lemma 1.11.4 gives $R = 0$ and π is an isomorphism. ∎

We are now ready to give a module-theoretic characterization of cohomologically trivial modules that are killed by p.

Proposition 1.11.6. *Suppose that G is a p-group and that A is a G-module of exponent dividing p. The following are equivalent:*

(i) A is cohomologically trivial

(ii) A is a free $\mathbb{F}_p[G]$-module.

(iii) There exists $i \in \mathbb{Z}$ such that $H^i_T(G, A) = 0$.

Proof.

(i) ⇒ (iii) Immediate.

(i) ⇒ (ii) This is a special case of Lemma 1.11.5, since $H_1(G,A) \cong \hat{H}^{-2}(G,A)$. (ii) ⇒ (i) Suppose A is free over $\mathbb{F}_p[G]$ on a generating set I. Then

$$A \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}} \bigoplus_{i \in I} \mathbb{F}_p,$$

so A is induced, hence cohomologically trivial.

(iii) ⇒ (ii) We note that the modules A_* and A^* that we use to dimension shift, as in (1.7.2) and (1.7.1) are killed by p since A is. In particular, it follows by dimension shifting that there exists a G-module B such that $pB = 0$ and

$$\hat{H}^{j-2}(H,B) \cong \hat{H}^{j+i}(H,A)$$

for all $H \leq G$ and $j \in \mathbb{Z}$. In particular, $H_1(G,B) = \hat{H}^{-2}(G,B)$ is trivial. By Lemma 1.11.5, B is $\mathbb{F}_p[G]$-free. However, we have just shown that this implies that B is cohomologically trivial, and therefore so is A. ∎

We next consider the case that A has no elements of order p.

Proposition 1.11.7. *Suppose that G is a p-group and A is a G-module with no elements of order p. The following are equivalent:*

(i) A is cohomologically trivial.

(ii) There exists $i \in \mathbb{Z}$ such that $\hat{H}^i(G,A) = \hat{H}^{i+1}(G,A) = 0$.

(iii) A/pA is free over $\mathbb{F}_p[G]$.

Proof.

(i) ⇒ (ii) Immediate.

(ii) ⇒ (iii) Since A has no p-torsion,

$$0 \to A \xrightarrow{p} A \to A/pA \to 0$$

is exact. By (ii) and the long exact sequence in Tate cohomology, we have $\hat{H}^i(G, A/pA) = 0$. By Proposition 1.11.6, we have therefore that A/pA is free over $\mathbb{F}_p[G]$.

(iii) ⇒ (i) By Proposition 1.11.6, we have that A/pA is cohomologically trivial, and therefore multiplication by p is an isomorphism on each $H^i_T(H, A)$ for each subgroup H of G and every $i \in \mathbb{Z}$. However, the latter cohomology groups are annihilated by the order of H, so must be trivial since H is a p-group. ∎

In order to give a characterization of cohomologically trivial modules in terms of projective modules, we require the following lemma.

Lemma 1.11.9. *Suppose that G is a p-group and A is a G-module that is free as an abelian group and cohomologically trivial. For any G-module B which is p-torsion free, we have that $\mathrm{Hom}_{\mathbb{Z}}(A, B)$ is cohomologically trivial.*

Proof. Since B has no p-torsion and A is free over $\mathbb{Z}$, we have that

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(A, B) \xrightarrow{p} \mathrm{Hom}_{\mathbb{Z}}(A, B) \to \mathrm{Hom}_{\mathbb{Z}}(A, B/pB) \to 0$$

is exact. In particular, $\mathrm{Hom}_{\mathbb{Z}}(A, B)$ has no p-torsion, and

$$\mathrm{Hom}_{\mathbb{Z}}(A/pA, B/pB) \cong \mathrm{Hom}_{\mathbb{Z}}(A, B/pB) \cong \mathrm{Hom}_{\mathbb{Z}}(A, B)/p\,\mathrm{Hom}_{\mathbb{Z}}(A, B).$$

Since A/pA is free over $\mathbb{F}_p[G]$ with some indexing set that we shall call I, we have

$$\mathrm{Hom}_{\mathbb{Z}}(A/pA, B/pB) \cong \prod_{i \in I} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{F}_p[G], B/pB) \cong \mathrm{Hom}_{\mathbb{Z}}\Big(\mathbb{Z}[G], \prod_{i \in I} B/pB\Big),$$

so $\mathrm{Hom}_{\mathbb{Z}}(A, B/pB)$ is coinduced, and therefore $\mathbb{F}_p[G]$-free. By Proposition 1.11.7, we have that $\mathrm{Hom}_{\mathbb{Z}}(A, B)$ is cohomologically trivial. ∎

Proposition 1.11.10. *Let G be a finite group and A a G-module that is free as an abelian group. Then A is cohomologically trivial if and only if A is a projective G-module.*

Proof. The projective direction has already been proved. Suppose A is cohomologically trivial. Since A is free over $\mathbb{Z}$, $\mathrm{Ind}^G(A)$ is a free G-mod, and the kernel A_* of the natural surjection $\mathrm{Ind}^G(A) \to A$ is free over $\mathbb{Z}$. Applying $\mathrm{Hom}_{\mathbb{Z}}(A, -)$ gives the exact sequence (1.11.1)

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(A, A_*) \to \mathrm{Hom}_{\mathbb{Z}}(A, \mathrm{Ind}^G(A)) \to \mathrm{Hom}_{\mathbb{Z}}(A, A) \to 0.$$

Apply Lemma 1.11.9 after restriction to each Sylow p-subgroup. Proposition 1.11.8 gives cohomological triviality of $\mathrm{Hom}_{\mathbb{Z}}(A, A_*)$ over G. The exact sequence in ordinary cohomology then gives a surjection from $\mathrm{Hom}_{\mathbb{Z}[G]}(A, \mathrm{Ind}^G(A))$ to $\mathrm{Hom}_{\mathbb{Z}[G]}(A, A)$. A lift of id_A splits $\mathrm{Ind}^G(A) \to A$. Hence A is projective.

Finally, we consider the general case.

Theorem 1.11.11. *Let G be a finite group and A a G-module. The following are equivalent.*

(i) A is cohomologically trivial.

(ii) For each prime p, there exists some $i \in \mathbb{Z}$ such that $\hat{H}^i(G_p, A) = \hat{H}^{i+1}(G_p, A) = 0$.

(iii) There is an exact sequence of G-modules

$$0 \to P_1 \to P_0 \to A \to 0$$

in which P_0 and P_1 are projective.

Proof.

(i) ⇒ (ii) This follows from the definition of cohomologically trivial.

(ii) ⇒ (iii) Let F be a free G-module that surjects onto A, and let R be the kernel. As F is cohomologically trivial, we have $\hat{H}^{j-1}(G_p, A) \cong \hat{H}^j(G_p, R)$ for every $j \in \mathbb{Z}$. It follows that $\hat{H}^j(G_p, R)$ vanishes for two consecutive values of j. Since R is $\mathbb{Z}$-free, being a subgroup of F, we have by

Propositions 1.11.7, 1.11.8, and 1.11.10 that R is projective.

(iii) ⇒ (i) This follows from the fact that projective modules are cohomologically trivial and the long

exact sequence in Tate cohomology. ∎

1.12 Tate's theorem

We continue to assume that G is a finite group, and we choose a Sylow p-subgroup G_p of G for each prime p. We begin with a consequence of our characterization of cohomologically trivial modules to maps on cohomology.

Proposition 1.12.1. *Let $\kappa : A \to B$ be a G-module homomorphism. Viewed as a G_p-module homomorphism, let us denote it by κ_p. Suppose that, for each prime p, there exists a $j \in \mathbb{Z}$ such that*

$$\kappa_p^* : \hat{H}^i(G_p, A) \to \hat{H}^i(G_p, B)$$

is surjective for $i = j - 1$, an isomorphism for $i = j$, and injective for $i = j + 1$. Then

$$\kappa^* : \hat{H}^i(H, A) \to \hat{H}^i(H, B)$$

is an isomorphism for all $i \in \mathbb{Z}$ and subgroups H of G.

Proof. Consider the canonical injection of G-modules

$$\kappa \oplus \imath : A \to B \oplus \mathrm{CoInd}^G(A),$$

and let C be its cokernel. As $\mathrm{CoInd}^G(A)$ is H-cohomologically trivial for all $H \leq G$, we have

$$\hat{H}^i(H, B \oplus \mathrm{CoInd}^G(A)) \cong \hat{H}^i(H, B)$$

for all $i \in \mathbb{Z}$. The long exact sequence in G_p-cohomology then reads

$$\cdots \to \hat{H}^i(G_p, A) \xrightarrow{\kappa_p^*} \hat{H}^i(G_p, B) \to \hat{H}^i(G_p, C) \xrightarrow{\delta} \hat{H}^{i+1}(G_p, A) \xrightarrow{\kappa_p^*} \hat{H}^{i+1}(G_p, B) \to \cdots.$$

Consider the case $i = j - 1$. The map κ_p^* being surjective on $\hat{H}^{j-1}$ and injective on $\hat{H}^j$ implies that $\hat{H}^{j-1}(G_p, C) = 0$. Similarly, for $i = j$, the map κ_p^* being surjective on $\hat{H}^j$ and injective on $\hat{H}^{j+1}$ implies that $\hat{H}^j(G_p, C) = 0$. Therefore, C is cohomologically trivial by Theorem 1.11.11, and so each map $\kappa^* : \hat{H}^i(H, A) \to \hat{H}^i(H, B)$ in question must be an isomorphism by the long exact sequence in Tate cohomology. ∎

We now prove the main theorem of Tate and Nakayama.

Theorem 1.12.2. *Suppose that A, B, and C are G-modules and*

$$\theta : A \otimes_{\mathbb{Z}} B \to C$$

is a G-module map. Let $k \in \mathbb{Z}$ and $\alpha \in H_T^k(G, A)$. For each subgroup H of G, define

$$\Theta^i_{H,\alpha} : \hat{H}^i(H, B) \to \hat{H}^{i+k}(H, C), \qquad \Theta^i_{H,\alpha}(\beta) = \theta^*(\mathrm{Res}(\alpha) \cup \beta).$$

For each prime p, suppose that there exists $j \in \mathbb{Z}$ such that the map $\Theta^i_{G_p,\alpha}$ is surjective for $i = j - 1$, an isomorphism for $i = j$, and injective for $i = j + 1$. Then for every subgroup H of G and $i \in \mathbb{Z}$, one has that $\Theta^i_{H,\alpha}$ is an isomorphism.

Proof. First consider the case that $k = 0$. Then the map $\psi : B \to C$ given by $\psi(b) = \theta(a \otimes b)$, where $a \in A^G$ represents α, is a map of G-modules, since

$$\psi(gb) = \theta(a \otimes gb) = \theta(ga \otimes gb) = g\theta(a \otimes b) = g\psi(b).$$

We claim that the induced maps on cohomology

$$\psi^* : \hat{H}^i(H, B) \to \hat{H}^i(H, C)$$

agree with the maps given by left cup product with $\mathrm{Res}(\alpha)$. Given this, we have by Proposition 1.12.1 that the latter maps are all isomorphisms in the case $k = 0$.

To see the claim, consider first the case that $i = 0$, in which the map ψ^* is induced by $\psi : B^H \to C^H$. For $b \in B^H$, we have $\psi(b) = \theta(a \otimes b)$, and the class of the latter term is $\theta^*(\mathrm{Res}(a) \cup b)$ by (i) of

Theorem 1.9.12. For the case of arbitrary i, we consider the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (A \otimes_{\mathbb{Z}} B)_* & \longrightarrow & \mathrm{Ind}^G(A \otimes_{\mathbb{Z}} B) & \longrightarrow & A \otimes_{\mathbb{Z}} B & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \tilde{\theta}} & & \downarrow{\scriptstyle \mathrm{Ind}^G(\theta)} & & \downarrow{\scriptstyle \theta} & & \\ 0 & \longrightarrow & C_* & \longrightarrow & \mathrm{Ind}^G(C) & \longrightarrow & C & \longrightarrow & 0, \end{array} \tag{1.12.1}$$

where $\mathrm{Ind}^G(\theta) = \mathrm{id}_{\mathbb{Z}[G]} \otimes \theta$, and where $\tilde{\theta}$ is both the map making the diagram commute and $\mathrm{id}_{I_G} \otimes \theta$, noting Remark 1.7.1. In fact, by Remark 1.9.6, we have an exact sequence isomorphic to the top row of (1.12.1), given by

$$0 \to A \otimes_{\mathbb{Z}} B_* \to A \otimes_{\mathbb{Z}} \mathrm{Ind}^G(B) \to A \otimes_{\mathbb{Z}} B \to 0$$

and then a map $\tilde{\psi} : B_* \to C_*$ given by $\tilde{\psi}(b') = \tilde{\theta}(a \otimes b')$ for $b' \in B_*$. We then have two commutative diagrams

$$\begin{array}{ccc} \hat{H}^{i-1}(H, B) & \xrightarrow[\sim]{\delta} & \hat{H}^i(H, B_*) \\ \downarrow & & \downarrow \\ \hat{H}^{i-1}(H, C) & \xrightarrow[\sim]{\delta} & \hat{H}^i(H, C_*). \end{array}$$

In the first, the left vertical arrow is $\Theta^{i-1}_{H,\alpha}$ and the right vertical arrow is the map $\tilde{\Theta}^i_{H,\alpha}$ given on $\beta' \in \hat{H}^i(H, B_*)$ by

$$\tilde{\Theta}^i_{H,\alpha}(\beta') = \tilde{\theta}^*(\mathrm{Res}(\alpha) \cup \beta').$$

In the second, the left vertical arrow is ψ^* and the right is $\tilde{\psi}^*$. Supposing our claim for i, we have $\tilde{\psi}^* = \tilde{\Theta}^i_{H,\alpha}$. As the connecting homomorphisms in the diagrams are isomorphisms, we then have that $\psi^* = \Theta^i_{H,\alpha}$. I.e., if the claim holds for i, it holds for $i - 1$. The analogous argument using coinduced modules allows us to shift from i to $i + 1$, proving the claim for all $i \in \mathbb{Z}$, hence the theorem for $k = 0$.

For any $k \in \mathbb{Z}$, the result is again proven by dimension shifting, this time for A. Fix $\alpha \in H^{k-1}_T(H, A)$, and let $\alpha' = \delta(\alpha) \in \hat{H}^k(H, A_*)$. We note that the top row of (1.12.1) is also isomorphic to

$$0 \to A_* \otimes_{\mathbb{Z}} B \to \mathrm{Ind}^G(A) \otimes_{\mathbb{Z}} B \to A \otimes_{\mathbb{Z}} B \to 0.$$

Much as before, define $\Theta^i_{H,\alpha'}\colon \hat{H}^i(H,B) \to \hat{H}^{i+k}(H,C_*)$ by $\Theta^i_{H,\alpha'}(\beta) = \tilde{\theta}^*(\mathrm{Res}(\alpha') \cup \beta)$, where $\tilde{\theta}\colon A_* \otimes_{\mathbb{Z}} B \to C_*$ is the map determined by θ. The diagram

$$\begin{array}{ccc} \hat{H}^i(H,B) & = & \hat{H}^i(H,B) \\ \downarrow{\scriptstyle \Theta^i_{H,\alpha}} & & \downarrow{\scriptstyle \Theta^i_{H,\alpha'}} \\ \hat{H}^{i+k-1}(H,C) & \xrightarrow[\sim]{\delta} & \hat{H}^{i+k}(H,C_*) \end{array}$$

then commutes as

$$\delta \circ \Theta^i_{H,\alpha}(\beta) = \delta \circ \theta^*(\mathrm{Res}(\alpha) \cup \beta) = \tilde{\theta}^*\delta(\mathrm{Res}(\alpha) \cup \beta) = \tilde{\theta}^*(\mathrm{Res}(\alpha') \cup \beta) = \Theta^i_{H,\alpha'}(\beta).$$

There exists by assumption $j \in \mathbb{Z}$ such that the map $\Theta^i_{G_p,\alpha}$ is surjective for $i = j-1$, an isomorphism for $i = j$, and injective for $i = j+1$. By the commutativity of the diagram, the same holds for $\Theta^i_{G_p,\alpha'}$. Assuming the theorem for k, we then have that all of the maps $\Theta^i_{H,\alpha'}$ are isomorphisms, and therefore again by commutativity that so are the maps $\Theta^i_{H,\alpha}$. Thus, the theorem for a given k implies the theorem for $k-1$. By the analogous argument using coinduced modules, the theorem for k implies the theorem for $k+1$ as well. ∎

The following special case was first due to Tate.

Theorem 1.12.3 (Tate). Let G be finite, let A be a G-mod, and let $\alpha \in H^2(G,A)$. For every prime $p \mid |G|$, let P be a Sylow p-subgroup. Suppose that $H^1(P,A) = 0$ and $H^2(P,A)$ is cyclic of order $|P|$, generated by $\mathrm{Res}^G_P \alpha$. Then, for every $H \leq G$ and $r \in \mathbb{Z}$, the map

$$H^r_T(H,\mathbb{Z}) \longrightarrow H^{r+2}_T(H,A), \qquad \beta \longmapsto \mathrm{Res}^G_H(\alpha) \smile \beta$$

is an isomorphism.

Proof. For $H = G_p$, the maps in question are surjective for $i = -1$, as $H^1(G_p,A) = 0$, and injective for $i = 1$, as

$$H^1(G_p,\mathbb{Z}) = \mathrm{Hom}(G_p,\mathbb{Z}) = 0.$$

For $i = 0$, we have

$$\hat{H}^0(G_p,\mathbb{Z}) \cong \mathbb{Z}/|G_p|\mathbb{Z},$$

and the map takes the image of $n \in \mathbb{Z}$ to $n\,\mathrm{Res}(\alpha)$ (which is straightforward enough to see by dimension shifting, starting with the known case of cup products of degree zero classes), hence is an isomorphism by the assumption on $H^2(G_p,A)$. ∎

Application to the local norm quotient

Let L/K be finite Galois over a nonarchimedean local field and put $G = \mathrm{Gal}(L/K)$. For each $H \leq G$, let $E = L^H$. Hilbert's Theorem 90 gives $H^1(H,L^\times) = 0$. By the local Brauer invariant,

$$H^2(H,L^\times) \cong \ker(\mathrm{Br}(E) \to \mathrm{Br}(L)) \cong \tfrac{1}{|H|}\mathbb{Z}/\mathbb{Z} \cong \mathbb{Z}/|H|\mathbb{Z}.$$

The fundamental class $u_{L/K}$ of invariant $1/[L:K]$ restricts to the class of invariant $[E:K]/[L:K] = 1/|H|$, so it generates every such relative group. Tate's theorem applies. In degree $r = -2$, it gives

$$G^{\mathrm{ab}} = H_1(G,\mathbb{Z}) = H^{-2}_T(G,\mathbb{Z}) \xrightarrow[\sim]{u_{L/K} \smile -} H^0_T(G,L^\times) = K^\times/N_{L/K}(L^\times).$$

For abelian L/K, the group on the left is $\mathrm{Gal}(L/K)$. With arithmetic Frobenius normalization, the inverse is the finite-level local Artin map on the norm quotient.

2. GALOIS COHOMOLOGY

2.1 Profinite groups

Definition 2.1.1. A *topological group* G is a group endowed with a topology with respect to which both the multiplication map $G \times G \to G$ and the inversion map $G \to G$ that takes an element to its inverse are continuous.

Examples 2.1.2.

a. The groups $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}^\times$, and $\mathbb{C}^\times$ are continuous with respect to the topologies defined by their absolute values.

b. Any group can be made a topological group by endowing it with the discrete topology.

Remark 2.1.3. We may consider the category of topological groups, in which the maps are continuous homomorphisms between topological groups.

Definition 2.1.4. A homomorphism $\phi : G \to G'$ between topological groups G and G' is a *topological isomorphism* if it is both an isomorphism and a homeomorphism.

The following lemma is almost immediate, since elements of a group are invertible.

Lemma 2.1.5. *Let G be a topological group and $g \in G$. Then the map $m_g : G \to G$ with $m_g(a) = ga$ for all $a \in G$ is a homeomorphism.*

We also have the following.

Lemma 2.1.6. *A group homomorphism $\phi : G \to G'$ between topological groups is continuous if and only if, for each open neighborhood U of 1 in G' with $1 \in U$, the set $\phi^{-1}(U)$ contains an open neighborhood of 1.* *Proof.* We consider the non-obvious direction. Let V be an open set in G', and suppose that $g \in G$ is such that $h = \phi(g) \in V$. Then $h^{-1}V$ is open in G' as well, by Lemma 2.1.5. By assumption, there exists an open neighborhood W of 1 in G contained in $\phi^{-1}(h^{-1}V)$, and so gW is an open neighborhood of g in G such that $\phi(gW) \subseteq V$. Hence, ϕ is continuous. ∎

Lemma 2.1.7. *Let G be a topological group.*

a. Any open subgroup of G is closed.

b. Any closed subgroup of finite index in G is open.

Proof. If H is an open (resp., closed) subgroup of G, then its cosets are open (resp., closed) as well. Moreover, $G - H$ is the union of the nontrivial cosets of H. Therefore, $G - H$ is open if G is open and closed if G is closed of finite index, so that there are only finitely many cosets of H. ∎

Lemma 2.1.8. *Every open subgroup of a compact group G is of finite index in G.*

Proof. Let H be a open subgroup of G. Note that G is the union of its distinct H-cosets, which are open and disjoint. Since G is compact, there can therefore only be finitely many cosets, which is to say that H is of finite index in G. ∎

We leave it to the reader to verify the following.

Lemma 2.1.9.

a. A subgroup of a topological group is a topological group with respect to the subspace topology.

b. The quotient of a topological group G by a normal subgroup N is a topological group with respect to the quotient topology, and it is Hausdorff if N is closed.

c. A direct product of topological groups is a topological group with respect to the product topology.

Recall the definitions of a directed set, inverse system, and the inverse limit.

Definition 2.1.10. A *directed set* $I = (I, \geq)$ is a partially ordered set such that for every $i, j \in I$, there exists $k \in I$ with $k \geq i$ and $k \geq j$.

Definition 2.1.11. Let I be a directed set. An *inverse system* $(G_i, \phi_{i,j})$ of groups over the indexing set I is a set

$$\{G_i \mid i \in I\}$$

of groups and a set

$$\{\phi_{i,j} \colon G_i \to G_j \mid i, j \in I, i \geq j\}$$

of group homomrphisms.

Definition 2.1.12. An *inverse limit* $G = \varprojlim_{i \in I} G_i$ of an inverse system $(G_i, \phi_{i,j})$ over a directed set I consists of a group G and homomorphisms $\pi_i : G \to G_i$ with $\phi_{i,j} \circ \pi_i = \pi_j$ for all $i \geq j$. They have the following universal property. Given a group G' and maps $\pi_i' : G' \to G_i$ with $\phi_{i,j} \circ \pi_i' = \pi_j'$ for all $i \geq j$, there is a unique map $\psi : G' \to G$ such that $\pi_i' = \pi_i \circ \psi$ for every $i \in I$.

By the universal property, any two inverse limits of an inverse system of groups are canonically isomorphic by compatible maps.

Remark 2.1.13. We may make the latter definition more generally with any category C replacing the category of groups. The groups are replaced with objects in C and the group homomorphisms with morphisms in C. Moreover, we may view the system of groups as a covariant functor to the category C from the category that has the elements of I as its objects and morphisms $i \to j$ for each $i, j \in I$ with $i \geq j$.

We may give a direct construction of an inverse limit of an inverse system of groups as follows. The proof is left to the reader.

Proposition 2.1.14. *Let $(G_i, \phi_{i,j})$ be an inverse system of groups over an indexing set I. Then the an inverse limit of the system is given explicitly by the group*

$$G = \left\{ (g_i)_i \in \prod_{i \in I} G_i \mid \phi_{i,j}(g_i) = g_j \right\}$$

and the maps $\pi_i \colon G \to G_i$ for $i \in I$ that are the compositions of the $G \to \prod_{i \in I} G_i \to G_i$ of inclusion followed by projection.

We may endow an inverse limit of groups with a topology as follows.

Definition 2.1.15. Let $(G_i, \phi_{i,j})$ be an inverse system of topological groups over an indexing set I, with continuous maps. Then the *inverse limit topology* on the inverse limit G of Proposition 2.1.14 is the subspace topology for the product topology on $\prod_{i \in I} G_i$.

Lemma 2.1.16. *The inverse limit of an inverse system $(G_i, \phi_{i,j})$ of topological groups (over a directed indexing set I) is a topological group under the inverse limit topology.*

Proof. The maps

$$\prod_{i \in I} G_i \times \prod_{i \in I} G_i \to \prod_{i \in I} G_i \quad \text{and} \quad \prod_{i \in I} G_i \to \prod_{i \in I} G_i$$

given by componentwise multiplication and inversion are clearly continuous, and this continuity is preserved under the subspace topology on the inverse limit. ∎

Remark 2.1.17. In fact, the inverse limit of an inverse system of topological groups and continuous maps, when endowed with the product topology, is an inverse limit in the category of topological groups.

When we wish to view it as a topological group, we typically endow a finite group with the discrete topology.

Definition 2.1.18. A *profinite group* is an inverse limit of a system of finite groups, endowed with the inverse limit topology for the discrete topology on the finite groups.

Recall the following definition.

Definition 2.1.19. A topological space is *totally disconnected* if and only if every point is a connected component.

We leave the following as difficult exercises.

Proposition 2.1.20. *A compact Hausdorff space is totally disconnected if and only if it has a basis of open neighborhoods that are also closed.*

Proposition 2.1.21. *A compact Hausdorff group that is totally disconnected has a basis of neighbor- hoods of* 1 *consisting of open normal subgroups (of finite index).*

We may now give a topological characterization of profinite groups.

Theorem 2.1.22. *A profinite topological group G is compact, Hausdorff, and totally disconnected.*

Proof. First, suppose that G is profinite, equal to an inverse limit of a system $(G_i, \phi_{i,j})$ of finite groups over an indexing set I. The direct product $\prod_{i\in I} G_i$ of finite (discrete) groups G_i is compact Hausdorff (compactness being Tychonoff's theorem). As a subset of the direct product, G is Hausdorff, and to see it is compact, we show that G is closed. Suppose that

$$(g_i)_i \in \coprod_{i\in I} G_i$$

with $(g_i)_i \notin G$, and choose $i, j \in I$ with $i > j$ and $\phi_{i,j}(g_i) \neq g_j$. The open subset

$$\left\{(h_k)_k \in \prod_{k\in I} G_k \mid h_i = g_i, h_j = g_j\right\}$$

of the direct product contains $(g_i)_i$ and has trivial intersection with G. In that the complement of G is open, G itself is closed. Finally, note that any open set $\prod_{i\in I} U_i$ with each U_i open in G_i (i.e., an arbitrary subset) and $U_i = G_i$ for all but finitely many i is also closed. That is, its complement is the intersection

$$\bigcap_{j\in I}\left((G_j - U_j) \times \prod_{i\in I-\{j\}} U_i\right)$$

of open sets, which is actually equal to the finite intersection over $j \in I$ with $U_i \neq G_i$. It is therefore open, and by Proposition 2.1.20, the group G is totally disconnected. ∎

Remark 2.1.23. We leave it to the reader to check that the converse to Theorem 2.1.22 also holds. They key is found in the proof of part a of the following proposition.

Proposition 2.1.24. *Let G be a profinite group, and let U be the set of all open normal subgroups of G. Then the following canonical homomorphisms are homeomorphisms:*

a. $G \to \varprojlim_{N\in\mathcal{U}} G/N$,

b. $H \to \varprojlim_{N\in\mathcal{U}} H/(H \cap N)$, *for H a closed subgroup of G, and*

c. $G/K \to \varprojlim_{N\in\mathcal{U}} G/NK$, *for K a closed normal subgroup of G.*

Proof. We prove part *a.* The continuous map ϕ from G to the inverse limit Q of its quotients has closed image, and ϕ is injective since U is a basis of 1 in G as in Proposition 2.1.21. Suppose that $(g_N N)_{N\in\mathcal{U}}$ is not in the image of ϕ, which is exactly to say that the intersection of the closed sets $g_N N$ is empty. Since G is compact this implies that some finite subset of the $\{g_N N \mid N \in \mathcal{U}\}$

is empty, and letting M be the intersection of the N in this subset, we see that $g_M M = \emptyset$, which is a contradiction. In other words, ϕ is surjective. ∎

The following is a consequence of Proposition 2.1.24a. We leave the proof to the reader.

Corollary 2.1.25. *Let G be a profinite group and V a set of open normal subgroups of G that forms a basis of open neighborhoods of 1. Then the homomorphism*

$$G \to \varprojlim_{N \in \mathcal{V}} G/N$$

is a homeomorphism.

The following lemma will be useful later.

Lemma 2.1.26. *The closed subgroups of a profinite group are exactly those that may be written as intersections of open subgroups. Proof.* In a topological group, an open subgroup is also closed, an arbitrary intersection of closed sets is closed, and an arbitrary intersection of subgroups is a subgroup, so an intersection of open subgroups is a closed subgroup. Let U denote the set of open subgroups of a profinite group G. Let H be a closed subgroup of G. It follows from Proposition 2.1.24b and the second isomorphism theorem that the set of subgroups of the form NH with N open normal in G has intersection H. Note that each NH is open as a union of open subgroups, so it is open. ∎

We may also speak of pro-p groups.

Definition 2.1.27. A *pro-p group*, for a prime p, is an inverse limit of a system of finite p-groups.

We may also speak of profinite and pro-p completions of groups.

Definition 2.1.28. Let G be a group.

a. The *profinite completion* $\hat{G}$ of G is the inverse limit of its finite quotients G/N, for N a normal subgroup of finite index in G, together with the natural quotient maps $G/N \to G/N'$ for $N \leq N'$.

b. The *pro-p completion* $G^{(p)}$ of G, for a prime p, is the inverse limit of the finite quotients of G of p-power order, i.e., of the G/N for $N \trianglelefteq G$ with $[G : N]$ a power of p, together with the natural quotient maps.

Remark 2.1.29. A group G is endowed with a canonical homomorphism to its profinite completion $\hat{G}$ by the universal property of the inverse limit.

Remark 2.1.30. We may also speak of topological rings and fields, where multiplication, addition, and the additive inverse map are continuous, and in the case of a topological field, the multiplicative inverse map on the multiplicative group is continuous as well. We may speak of profinite rings as inverse limits by quotients by two-sided ideals of finite index (or for pro-p rings, of p-power index).

The next proposition shows that $\mathbb{Z}_p$ is the pro-p completion of $\mathbb{Z}$.

Proposition 2.1.31. *Let p be a prime. We have an isomorphism of rings*

$$\psi : \mathbb{Z}_p \xrightarrow{\sim} \varprojlim_{k \geq 1} \mathbb{Z}/p^k\mathbb{Z}, \qquad \sum_{i=0}^{\infty} a_i p^i \mapsto \left(\sum_{i=0}^{k-1} a_i p^i \right)_k,$$

where the maps $\mathbb{Z}/p^{k+1}\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ in the system are the natural quotient maps. Moreover, ψ is a homeomorphism. Proof. The canonical quotient map $\psi_k : \mathbb{Z}_p \to \mathbb{Z}/p^k\mathbb{Z}$ is the kth coordinate of ψ, which is then a ring homomorphism by the universal property of the inverse limit. The kernel ψ is the intersection of the kernels of the maps ψ_k, which is exactly

$$\bigcap_k p^k \mathbb{Z}_p = 0.$$

Moreover, any sequence of partial sums modulo increasing powers of p has a limit in $\mathbb{Z}_p$, which maps to the sequence under ψ. The open neighborhood $p^n\mathbb{Z}_p$ of 0 in the p-adic topology is sent to the intersection

$$\left(\prod_{k=1}^{n}\{0\} \times \prod_{k=n+1}^{\infty} \mathbb{Z}_p/p^k\mathbb{Z}_p\right) \cap \left(\varprojlim_{k\geq 1} \mathbb{Z}/p^k\mathbb{Z}\right),$$

which is open in the product topology. On the other hand, the inverse image of a basis open neighborhood

$$\left(\prod_{k=1}^{n} U_k \times \prod_{k=n+1}^{\infty} \mathbb{Z}_p/p^k\mathbb{Z}_p\right) \cap \left(\varprojlim_{k\geq 1} \mathbb{Z}/p^k\mathbb{Z}\right)$$

with $0 \in U_k$ for all $1 \leq k \leq n$ under ψ clearly contains $p^n\mathbb{Z}_p$. It then follows from Lemma 2.1.6 that ψ is a homeomorphism. ∎

Definition 2.1.32. The *Prüfer ring* $\hat{\mathbb{Z}}$ is the profinite completion of $\mathbb{Z}$. That is, we have

$$\hat{\mathbb{Z}} \cong \varprojlim_{n\geq 1} \mathbb{Z}/n\mathbb{Z}$$

with respect to the quotient maps $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ for $m \mid n$.

Since $\mathbb{Z}/n\mathbb{Z}$ may be written as a direct product of the $\mathbb{Z}/p^k\mathbb{Z}$ for primes p with p^k exactly dividing n, we have the following.

Lemma 2.1.33. *We have an isomorphism of topological rings*

$$\hat{\mathbb{Z}} \cong \coprod_{p \text{ prime}} \mathbb{Z}_p.$$

Example 2.1.34. The free profinite (or pro-p) group on a generating set S is the profinite (resp., pro-p) completion of the free group on S.

Remark 2.1.35. Closed subgroups of free pro-p groups are free pro-p. A closed subgroup of a free profinite group need not be free profinite. The rank-one free profinite group is $\widehat{\mathbb{Z}} \cong \prod_\ell \mathbb{Z}_\ell$, so it contains $\mathbb{Z}_p$ as a closed subgroup. The group $\mathbb{Z}_p$ has no continuous quotient C_ℓ for $\ell \neq p$, whereas any nontrivial free profinite group has such a quotient.

Definition 2.1.36. A subset S of a topological group G is said to be a *topological generating set* of G if G is the closure of the subgroup generated by S.

Definition 2.1.37. We say that a topological group is *(topologically) finitely generated* if it has a finite set of topological generators.

Remark 2.1.38. The set S topologically generates the free profinite or pro-p group on S.

We leave a proof of the following to the reader.

Lemma 2.1.39. Let G be a topological group and let H be a subgroup. Its closure $\overline{H}$ is a subgroup of G. If H is normal, then $\overline{H}$ is normal in G.

Definition 2.1.40. The Frattini subgroup $\Phi(G)$ of a pro-p group G, where p is a prime, is smallest closed normal subgroup containing the commutator subgroup $[G, G]$ and the pth powers in G.

The following lemma is a consequence of the well-known case of finite p-groups.

Lemma 2.1.41. Let G be a pro-p group. The Frattini subgroup $\Phi(G)$ is closed and normal. A subset $S \subseteq G$ topologically generates G if and only if its image topologically generates $G/\Phi(G)$.

Remark 2.1.42. In the case that G is an abelian pro-p group, the Frattini subgroup $\Phi(G)$ in Lemma 2.1.41 is G^p.

Finally, we state without proof the structure theorem for (topologically) finitely generated abelian pro-p groups. In fact, this is an immediate consequence of the structure theorem for finitely generated modules over a PID.

Theorem 2.1.43. *Let A be a topologically finitely generated abelian pro-p group. Then there exist $r, k \geq 0$ and $n_1 \geq n_2 \geq \cdots \geq n_k \geq 1$ such that we have an isomorphism*

$$A \cong \mathbb{Z}_p^r \oplus \mathbb{Z}/p^{n_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{n_k}\mathbb{Z}$$

of topological groups.

Neighborhoods, compatible systems, and completion

In a profinite group, each basic neighborhood at 1 contains the intersection of finitely many kernels of the finite coordinate projections. Thus all open normal subgroups form a local basis. For any $H \leq G$ its closure is $\bigcap_N HN$, where N runs over the open normal subgroups. This gives $H \cong \varprojlim H/(H \cap N)$ for closed H and $G/H \cong \varprojlim G/HN$ for closed normal H. A finite profinite group is discrete, since it is Hausdorff.

Levelwise isomorphisms induce an inverse-limit isomorphism when they commute with the transition maps. A tower of copies of C_2 with identity transitions has limit C_2, and the same groups with trivial transitions have trivial limit. The entrywise maps give $M_k(\mathbb{Z}_p) \cong \varprojlim_n M_k(\mathbb{Z}/p^n\mathbb{Z})$. Invertible compatible components have compatible inverses by uniqueness, proving the same statement for GL_k.

The profinite completion uses every finite quotient and the canonical map has dense image, with kernel the intersection of the finite-index normal subgroups. For $\mathbb{Z}$, this completion is $\widehat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$. Using only the quotients $\mathbb{Z}/p^n\mathbb{Z}$ gives the (p)-adic completion $\mathbb{Z}_p$. A continuous map out of a completion is determined by its values on the dense subgroup.

For a pro-p group, $\Phi(G) = \overline{G^p[G,G]}$, where G^p denotes the subgroup generated by the pth powers. Thus $G/\Phi(G)$ is a profinite elementary abelian group. With trivial action on $\mathbb{F}_p$, every continuous homomorphism $G \to \mathbb{F}_p$ factors uniquely through it, so $H^1_{\mathrm{cont}}(G, \mathbb{F}_p)$ is its continuous dual. If G is topologically finitely generated, the quotient is finite and its dimension is the minimum number of topological generators.

2.2 Cohomology of profinite groups

Why the finite-quotient formula uses inflation

Use H^i_{cont} for continuous cohomology. A discrete coefficient mod must have a continuous action, which is equivalent to every element having an open stabilizer. A continuous cochain on G^i has finite image and factors through $(G/N)^i$ for a sufficiently small open normal N. Shrinking N further fixes all of its finitely many values. Thus

$$H^i_{\mathrm{cont}}(G, A) = \varinjlim_{N \trianglelefteq_o G} H^i(G/N, A^N).$$

The group is reconstructed by inverse limit, whereas cochains and cohomology use inflation and a direct limit. Restriction is available for closed subgroups and corestriction by finite coset sums for open subgroups. For finite profinite G the topology is discrete and the ordinary and continuous complexes agree.

In this section, G will denote a topological group.

Definition 2.2.1. A *topological G-module* A is an abelian topological group such that the map $G \times A \to A$ defining the action of G on A is continuous.

Definition 2.2.2. A G-module A is *discrete* if it is a topological G-module for the discrete topology on A.

Proposition 2.2.3. *Let G be a profinite group, and let A be a G-module. The following are equivalent:*

i. A is discrete,

ii. $A = \bigcup_{N \in \mathcal{U}} A^N$, where U is the set of open normal subgroups of G, and

iii. the stabilizer of each $a \in A$ is open in G.

Proof. Let $\pi : G \times A \to A$ be the map defining the G-action on A. For $a \in A$, let G_a denote the stabilizer of a. If A is discrete, then $\pi^{-1}(a) \cap (G \times \{a\})$ is open and equal to $G_a \times \{a\}$, so G_a is open as well. Thus, (i) implies (iii). Conversely, suppose that (iii) holds. To see (i), it suffices to check that for any $a, b \in A$, then set $X_{a,b} = \{g \in G | ga = b\}$ is open. If $X_{a,b}$ is nonempty, then for any $g \in X_{a,b}$, we clearly have $X_{a,b} = G_b g$, which is open by the continuity of the multiplication on G. Thus, (iii) implies (i).

If G_a is open for a given $a \in A$, then as U is a base of open neighborhoods of 1 in G, there exists $N \in \mathcal{U}$ with $N \subseteq G_a$. In other words, $a \in A^N$. Thus (iii) implies (ii). Conversely, suppose that (ii) holds. Take $a \in A$ and let $N \in \mathcal{U}$ be such that $a \in A^N$. Since N has finite index in G, the stabilizer G_a is a finite union of N-cosets, so G_a is open as well. Thus (ii) implies (iii). ∎

Remark 2.2.4. Note that our notion of a discrete G-module A says only that the G-action on A is continuous with respect to the discrete topology, so A can be thought of as a topological module when endowed with said topology. It is possible that the discrete topology is not the unique topology that makes A a topological G-module. For instance, $\mathbb{Z}/2\mathbb{Z}$ acts on $\mathbb{R}$ by $x \mapsto -x$, and this is continuous with respect to both the discrete and the usual topology on $\mathbb{R}$.

Examples 2.2.5.

a. Every trivial G-module is a discrete G-module.

b. If G is finite (with the discrete topology), then every G-module is discrete.

c. If G is profinite, then every finite G-module is necessarily discrete. d. The action of $\mathbb{C}^\times$ on $\mathbb{C}$ by left multiplication gives $\mathbb{C}$ the structure of a $\mathbb{C}^\times$-module that is not discrete.

e. The action of $\hat{\mathbb{Z}}^\times$ on the group of roots of unity in $\mathbb{C}$ by $u \cdot \zeta = \zeta^u$, for $u \in \hat{\mathbb{Z}}^\times$ and ζ a root of unity, is discrete. Here, ζ^u is ζ raised to the power of any integer that is congruent to u modulo the order of ζ.

Definition 2.2.6. We say that a topological G-module A is *discrete* if its topology is the discrete topology.

Definition 2.2.7. For a topological G-module A and $i \in \mathbb{Z}$, the group of continuous i-cochains of G with A-coefficients is

$$C^i_{\text{cts}}(G, A) = \{f : G^i \to A \mid f \text{ continuous}\}.$$

Lemma 2.2.8. *Let A be a topological G-module. The usual differential d^i_A on $C^i(G, A)$ restricts to a map $d^i_A : C^i_{\text{cts}}(G, A) \to C^{i+1}_{\text{cts}}(G, A)$. Thus, $(C^\cdot_{\text{cts}}(G, A), d^\cdot_A)$ is a cochain complex.*

Proof. Set $X = G^{i+1}$. Since $f \in C^i_{\text{cts}}(G, A)$ and the multiplication maps $G \times G \to G$ and $G \times A \to A$ are continuous, so are the $i + 2$ maps $X \to A$ taking $(g_1, \dots, g_{i+1})$ to $g_1 f(g_2, \dots, g_{i+1})$, to $f(g_1, \dots, g_j g_{j+1}, \dots, g_i)$ for some $1 \leq j \leq i$, and to $f(g_1, \dots, g_i)$. The alternating sum defining $d^i_A(f)$ from these $i+2$ maps is the composition of the diagonal map $X \to X^{i+2}$, the direct product $X^{i+2} \to A^{i+2}$ of the maps in question, and the alternating sum map $A^{i+2} \to A$. Since all of these maps are continuous, so is $d^i_A(f)$. ∎

Remark 2.2.9. In general, $C^{\cdot}(G, \cdot)$ is a left exact functor from the category of topological G-modules with continuous G-module homomorphisms to the category of abelian groups. However, it need not be exact.

Proposition 2.2.10. *Let G be a topological group. If*

$$0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0$$

is an exact sequence of discrete G-modules, then endowing A, B, and C with the discrete topology, the sequence

$$0 \to C^i_{\mathrm{cts}}(G,A) \xrightarrow{\iota'} C^i_{\mathrm{cts}}(G,B) \xrightarrow{\pi'} C^i_{\mathrm{cts}}(G,C) \to 0$$

is exact for each i.

Proof. We need only show right-exactness. Choose a set-theoretic splitting of $s\colon C \to B$ of π. In that B and C are discrete, s is necessarily continuous. For any continuous $f\colon G^i \to C$, the map $s \circ f\colon G^i \to B$ is therefore continuous, and $\pi^i(s \circ f) = f$. ∎

Definition 2.2.11. Let G be a profinite group and A a discrete G-mod. Its continuous cohomology with coefficients in A is

$$H^i_{\mathrm{cont}}(G, A) = H^i\big(C^{\bullet}_{\mathrm{cont}}(G, A)\big),$$

where A is endowed with the discrete topology.

Notation 2.2.12. If $f\colon A \to B$ is a G-module homomorphism between discrete G-modules A and B, where G is profinite, then the induced maps on cohomology are denoted $f^*\colon H^i(G,A) \to H^i(G,B)$.

As a corollary of Proposition 2.2.10, any short exact sequence of discrete G-modules gives rise to a long exact sequence of profinite cohomology groups.

Theorem 2.2.13. *Suppose that*

$$0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0$$

is a short exact sequence of discrete G-modules. Then there is a long exact sequence of abelian groups

$$0 \to H^0(G,A) \xrightarrow{\iota^*} H^0(G,B) \xrightarrow{\pi^*} H^0(G,C) \xrightarrow{\delta^0} H^1(G,A) \to \cdots.$$

Moreover, this construction is natural in the short exact sequence in the sense of Theorem 1.2.13.

Remark 2.2.14. For profinite G and discrete A, the continuous group $H^i_{\mathrm{cont}}(G, A)$ can differ from the ordinary group $H^i(G, A)$ of the underlying abstract group. If G is finite, its topology is discrete, all cochains are continuous, and the two complexes coincide.

Example 2.2.15. For a pro-p group G, $H^1_{\mathrm{cont}}(G, \mathbb{F}_p)$ with trivial coefficients consists of the continuous homomorphisms $G \to \mathbb{F}_p$. They factor uniquely through $G/\Phi(G)$, so $H^1_{\mathrm{cont}}(G, \mathbb{F}_p)$ is the continuous $\mathbb{F}_p$-dual of that quotient. The dimension equals the minimum cardinality of a topological generating set by Lemma 2.1.41. For a topologically finitely generated group the quotient is finite and this is the usual finite-dimensional duality.

The following proposition shows that profinite cohomology groups are direct limits of usual cohomology groups of finite groups under inflation maps.

Proposition 2.2.16. For a profinite group G and a discrete G-mod A, there is a natural isomorphism

$$H^i_{\text{cont}}(G, A) \cong \varinjlim_{N \triangleleft_o G} H^i(G/N, A^N),$$

with transition maps given by inflation over the open normal subgroups.

Proof. It suffices to check that we have natural isomorphisms

$$C^i_{\text{cts}}(G, A) \cong \varinjlim_{N \in \mathcal{U}} C^i(G/N, A^N)$$

commuting with connecting homomorphisms. We verify the isomorphism, which then clearly has the other properties. Let $f : G^i \to A$ be continuous. Since G is compact and A is discrete, the image of f is finite. For each $a \in \operatorname{im} f$, let $M_a \in \mathcal{U}$ be such that $a \in A^{M_a}$. Then $M = \bigcap_{a \in \operatorname{im} f} M_a \in \mathcal{U}$, and $\operatorname{im} f \subset A^M$.

We next check that f factors through $(G/H)^i$ for an open subgroup $H \in \mathcal{U}$. For this, note that the continuity of f forces it to be constant on an open neighborhood of any $x \in G^i$, and inside such a neighborhood is a neighborhood of the form $x \prod_{j=1}^i H_j(x)$ with H_j an open normal subgroup of G. Take $H(x) = \bigcap_{j=1}^i H_j(x)$, which again is an open normal subgroup, so f is constant on $xH(x)^i$. Now G^i is covered by the $xH(x)^i$ for $x \in G^i$. Compactness of G^i tells us that is a finite subcover corresponding to some $x_1, \dots, x_n \in G^i$. The intersection $H = \bigcap_{k=1}^n H(x_k)$ is then such that f factors through $(G/H)^i$, since for any $y \in G^i$, we have $y \in x_k H(x_k)^i$ for some k, and therefore f is constant on $yH \subseteq x_i H(x_i)^i$. Thus f factors through $(G/H)^i$.

We have shown that f is the inflation of a map $(G/H)^i \to A^M$. If we take $N = H \cap M$, then f factors through a map $(G/N)^i \to A^N$, proving the result. ∎

The notion of a compatible pair passes to profinite group cohomology if we merely suppose that our map of profinite groups is continuous.

Definition 2.2.17. Let G and G' be profinite groups, A a discrete G-module and A' a G'-module. We say that a pair (ρ, λ) with $\rho : G' \to G$ a continuous group homomorphism and $\lambda : A \to A'$ a group homomorphism is *compatible* if

$$\lambda(\rho(g')a) = g'\lambda(a)$$

for all $a \in A$ and $g' \in G'$.

Consequently, we have inflation, restriction, and conjugation maps as in Definition 1.8.6 and Proposition 1.8.12 so long as the subgroup is taken to be closed, which ensures that it is a profinite group. By Proposition 2.2.16 and exactness of the direct limit, it is easy to see that these maps are just direct limits of the analogous maps for usual group cohomology under inflation, as holds for any map on profinite cohomology induced by a compatible pair. In fact, we also have corestriction, defined simply as the direct limit of corestriction maps at finite level. Moreover, the inflation-restriction sequence is still exact, and this works for any closed normal subgroup. We state the higher degree version of this result for later use.

Proposition 2.2.18. Let G be profinite, N a closed normal subgroup, and A a discrete G-mod. Let $i \geq 1$ and suppose $H^j_{\text{cont}}(N, A) = 0$ for $1 \leq j < i$. Then the following sequence is exact:

$$0 \to H^i_{\text{cont}}(G/N, A^N) \xrightarrow{\text{Inf}} H^i_{\text{cont}}(G, A) \xrightarrow{\text{Res}} H^i_{\text{cont}}(N, A).$$

2.3 Galois theory of infinite extensions

Krull topology and the direction of restriction

If E/K is a finite Galois intermediate extension, every K-automorphism preserves E by normality. Restriction $\mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K)$ is onto by extension of embeddings and has kernel $\mathrm{Gal}(L/E)$. These kernels are the open normal neighborhoods defining the Krull topology. A compatible family of restrictions defines an automorphism on the union of the finite Galois subextensions. In particular, $G_K^{\mathrm{ab}} = G_K/\overline{[G_K, G_K]} \cong \mathrm{Gal}(K^{\mathrm{ab}}/K)$ as profinite groups. The closure accounts for the fact that the quotient is Hausdorff.

Recall that an algebraic extension of fields L/K is Galois if it is normal, so that every polynomial in $K[x]$ that has a root in L splits completely, and separable, so that no irreducible polynomial in $K[x]$ has a double root in L. The Galois group $\mathrm{Gal}(L/K)$ of such an extension is the group of automorphisms of L that fix K.

In the setting of finite Galois extensions L/K, the subfields E of L containing K are in one-to-one correspondence with the subgroups H of $\mathrm{Gal}(L/K)$. In fact, the maps $E \mapsto \mathrm{Gal}(L/E)$ and $H \mapsto L^H$ give inverse bijections between these sets. This is not so in the setting of infinite Galois extensions, where there are rather more subgroups than there are subfields. To fix this issue, we place a topology on $\mathrm{Gal}(L/K)$ and consider only the closed subgroups under this topology. The above-described correspondences then work exactly as before.

Proposition 2.3.1. *Let L/K be a Galois extension of fields. Let E denote the set of finite Galois extensions of K contained in L, ordered by inclusion. This is a directed set. Let ρ be the map*

$$\rho : \mathrm{Gal}(L/K) \to \varprojlim_{E \in \mathscr{E}} \mathrm{Gal}(E/K)$$

defined by the universal property of the inverse limit, with the maps $\mathrm{Gal}(E'/K) \to \mathrm{Gal}(E/K)$ for $E, E' \in \mathscr{E}$ with $E \subseteq E'$ and the maps $\mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K)$ for $E \in \mathscr{E}$ being restriction maps. Then ρ is an isomorphism.

Proof. Let $\sigma \in \mathrm{Gal}(L/K)$. If $\sigma|_E = 1$ for all $E \in \mathscr{E}$, then since

$$L = \bigcup_{E \in \mathscr{E}} E,$$

we have that $\sigma = 1$. On the other hand, if elements $\sigma_E \in \mathrm{Gal}(E/K)$ for each $E \in \mathscr{E}$ are compatible under restriction, then define $\sigma \in \mathrm{Gal}(L/K)$ by $\sigma(\alpha) = \sigma_E(\alpha)$ if $\alpha \in E$. Then, if $\alpha \in E'$ for some $E' \in \mathscr{E}$ as well, then

$$\sigma_{E'}(\alpha) = \sigma_{E \cap E'}(\alpha) = \sigma_E(\alpha),$$

noting that $E \cap E' \in \mathscr{E}$. Therefore, σ is well-defined, and so ρ is bijective. ∎

Proposition 2.3.1 gives us an obvious topology to place on the Galois group of a Galois extension.

Definition 2.3.2. Let L/K be a Galois extension of fields. The *Krull topology* on $\mathrm{Gal}(L/K)$ is the unique topology under which the set of $\mathrm{Gal}(L/E)$ for E/K finite Galois with $E \subseteq L$ forms a basis of open neighborhoods of 1.

Remark 2.3.3. The Krull topology agrees with the inverse limit topology induced by the isomorphism of Proposition 2.3.1, since

$$1 \to \mathrm{Gal}(L/E) \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K) \to 1$$

is exact. Therefore, if L/K is Galois, then $\mathrm{Gal}(L/K)$ is a topological group under the Krull topology.

Lemma 2.3.4. *Let L/K be a Galois extension of fields. The open subgroups in $\mathrm{Gal}(L/K)$ are exactly those subgroups of the form $\mathrm{Gal}(L/E)$ with E an intermediate field in L/K of finite degree over K.*

Proof. First, let E be an intermediate field in L/K of finite degree. Let E' be the Galois closure of E in L, which is of finite degree over K. Then $\mathrm{Gal}(L/E')$ is an open normal subgroup under the Krull topology, contained in $\mathrm{Gal}(L/E)$. Since $\mathrm{Gal}(L/E)$ is then a union of left $\mathrm{Gal}(L/E')$-cosets, which are open, we have that $\mathrm{Gal}(L/E)$ is open.

Conversely, let H be an open subgroup in $\mathrm{Gal}(L/K)$. Then H contains $\mathrm{Gal}(L/E)$ for some finite Galois extension E/K in L. Any $\alpha \in L^H$, where L^H is the fixed field of H in L, is contained in $M^{\mathrm{Gal}(L/E)}$, where M is the Galois closure of $E(\alpha)$. Since the restriction map $\mathrm{Gal}(L/E) \to \mathrm{Gal}(M/E)$ is surjective, we then have $\alpha \in M^{\mathrm{Gal}(M/E)}$. But M/K is finite, so $M^{\mathrm{Gal}(M/E)} = E$ by the fundamental theorem of Galois theory. Thus $L^H \subseteq E$.

Let $\bar{H}$ be the image of H under the restriction map $\pi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K)$. As $\mathrm{Gal}(L/E) \leq H$, we have that $\pi^{-1}(\bar{H}) = H$. We remark that $\bar{H} = \mathrm{Gal}(E/L^H)$, since $\bar{H} = \mathrm{Gal}(E/E^{\bar{H}})$ by the fundamental theorem of Galois theory for finite extensions and $L^H = E^H = E^{\bar{H}}$. But $\pi^{-1}(\bar{H})$ is then $\mathrm{Gal}(L/L^H)$ as well. ∎

From this, we may derive the following.

Lemma 2.3.5. *Let L/K be a Galois extension of fields. The closed subgroups of $\mathrm{Gal}(L/K)$ are exactly those of the form $\mathrm{Gal}(L/E)$ for some intermediate field E in the extension L/K.*

Proof. Under the Krull topology on $\mathrm{Gal}(L/K)$, the open subgroups are those of the form $\mathrm{Gal}(L/E)$ with E/K finite. By Lemma 2.1.26, we have therefore that the closed subgroups are those that are intersections of $\mathrm{Gal}(L/E)$ over a set S of finite degree over K intermediate fields E. Any such intersection necessarily fixes the compositum $E' = \prod_{E \in S} E$, while if an element of $\mathrm{Gal}(L/K)$ fixes E', then it fixes every $E \in S$, so lies in the intersection. That is, any closed subgroup has the form

$$\mathrm{Gal}(L/E') = \bigcap_{E \in S} \mathrm{Gal}(L/E).$$

[

Theorem 2.3.6 (Fundamental theorem of Galois theory)**.** *Let L/K be a Galois extension. Then there are inverse one-to-one, inclusion reversing correspondences*

$$\{\text{intermediate extensions in } L/K\} \underset{\theta}{\overset{\psi}{\rightleftarrows}} \{\text{closed subgroups of } \mathrm{Gal}(L/K)\}$$

given by $\psi(E) = \mathrm{Gal}(L/E)$ for any intermediate extension E in L/K and $\theta(H) = L^H$ for any closed subgroup H of $\mathrm{Gal}(L/K)$. These correspondences restrict to bijections between the normal extensions of K in L and the closed normal subgroups of $\mathrm{Gal}(L/K)$, as well as to bijections between the finite degree (normal) extensions of K in L and the open (normal) subgroups of $\mathrm{Gal}(L/K)$. Moreover, if E is normal over K (resp., $H \trianglelefteq \mathrm{Gal}(L/K)$ is closed), then restriction induces a topological isomorphism

$$\mathrm{Gal}(L/K)/\mathrm{Gal}(L/E) \xrightarrow{\sim} \mathrm{Gal}(E/K)$$

(resp., $\mathrm{Gal}(L/K)/H \xrightarrow{\sim} \mathrm{Gal}(L^H/K)$*).*

Proof. We will derive this from the fundamental theorem of Galois theory for finite Galois extensions. Let E be an intermediate extension in L/K. Then $E \subseteq L^{\mathrm{Gal}(L/E)}$ by definition. Let $x \in L^{\mathrm{Gal}(L/E)}$. The Galois closure M of $E(x)$ in L is of finite degree over E. But every element of $\mathrm{Gal}(M/E)$ extends to an element of $\mathrm{Gal}(L/E)$, which fixes x. So $x \in M^{\mathrm{Gal}(M/E)}$, which equals E by fundamental theorem of Galois theory for finite Galois extensions. Since x was arbitrary, we have $E = L^{\mathrm{Gal}(L/E)}$. In other words, $\theta(\psi(E)) = E$.

Let H be a closed subgroup of $\mathrm{Gal}(L/K)$. In Lemma 2.3.5, we saw that $H = \mathrm{Gal}(L/E)$ for some intermediate E in L/K. Since $E = L^{\mathrm{Gal}(L/E)} = L^H$ from what we have shown, we have that $H = \mathrm{Gal}(L/L^H)$. Therefore, $\psi(\theta(H)) = H$. It follows that we have the desired inclusion-reversing one-to-one correspondences. The other claims are then easily checked and are left to the reader. ∎

Definition 2.3.7. Fix an algebraic closure of L. Its subfield of elements separable over L is a separable closure of L. Equivalently, it is the subfield generated over L by the roots of separable polynomials in $L[x]$.

Notation 2.3.8. We typically denote a separable closure of L by L^{sep}.

Remark 2.3.9. If one fixes an algebraically closed field Ω containing L, then there is a unique separable closure of L in Ω, being the subfield generated by the roots of all separable polynomials in $L[x]$.

Definition 2.3.10. The *absolute Galois group* of a field K is the Galois group

$$G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K),$$

sep where K is a separable closure of K.

Remark 2.3.11. An L-isomorphism between two separable closures of L induces an isomorphism of their absolute Galois groups by conjugation. Changing the chosen field isomorphism changes the resulting group isomorphism by an inner automorphism.

Example 2.3.12. Let q be a power of a prime number. Then there is a unique topological isomorphism $G_{\mathbb{F}_q} \xrightarrow{\sim} \hat{\mathbb{Z}}$ sending the Frobenius automorphism $\varphi_q \colon x \mapsto x^q$ to 1. To see this, note that $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \to \mathbb{Z}/n\mathbb{Z}$ given by sending φ_q to 1 is an isomorphism, and these give rise to compatible isomorphisms in the inverse limit

$$G_{\mathbb{F}_q} \xrightarrow{\sim} \varprojlim_n \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \xrightarrow{\sim} \varprojlim_n \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \hat{\mathbb{Z}}.$$

Example 2.3.13. Let $\mathbb{Q}(\mu_{p^\infty})$ denote the field given by adjoining all p-power roots of unity to $\mathbb{Q}$. Then

$$\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \cong \varprojlim_n \mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}) \cong \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}_p^\times$$

the middle isomorphisms arising from the p^nth cyclotomic characters.

Terminology 2.3.14. The isomorphism $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \to \mathbb{Z}_p^\times$ of Example 2.3.13 called the *p-adic cyclotomic character*.

An abelian extension is a Galois extension with abelian Galois group. The compositum of two abelian extensions inside a fixed algebraic closure is abelian.

Notation 2.3.15. The maximal abelian extension of K in a fixed algebraic closure is denoted K^{ab}.

Remark 2.3.16. The topological abelianization $G_K^{\mathrm{ab}} = G_K/\overline{[G_K, G_K]}$ is canonically isomorphic to $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ by restriction.

2.4 Galois cohomology

Definition 2.4.1. Let L/K be Galois, and let A be a discrete $\mathrm{Gal}(L/K)$-mod for the Krull topology. For $i \geq 0$, the ith Galois cohomology group of L/K with coefficients in A is $H^i_{\mathrm{cont}}(\mathrm{Gal}(L/K), A)$.

Example 2.4.2. Let L/K be a Galois extension with Galois group G. Then the additive and multiplicative groups of L are discrete G-modules. That is, L is the union of the finite Galois subextensions E of K in L, and $E = L^{\mathrm{Gal}(L/E)}$ by the fundamental theorem of infinite Galois theory.

Hilbert's Theorem 90 admits the following generalization to Galois cohomology.

Theorem 2.4.3. *Let L/K be a Galois extension of fields. Then $H^1(\mathrm{Gal}(L/K), L^\times) = 0$.*

Proof. Let E denote the set of finite Galois extensions of K in L. Then

$$H^1(\mathrm{Gal}(L/K), L^\times) = \varprojlim_{E \in \mathscr{E}} H^1(\mathrm{Gal}(E/K), E^\times),$$

which reduces us to the case that L/K is finite Galois. Let $G = \mathrm{Gal}(L/K)$, and let $f : G \to L^\times$ be a 1-cocycle. We may view the elements $\sigma \in G$ as abelian characters $L^\times \to L^\times$. As distinct characters of $L^\times$, these characters form a linearly independent set. The sum $\sum_{\sigma \in G} f(\sigma)\sigma$ is therefore a nonzero map $L^\times \to L$. Let $\alpha \in L^\times$ be such that $z = \sum_{\sigma \in G} f(\sigma)\sigma(\alpha) \neq 0$. For any $\tau \in G$, we have

$$\begin{aligned}\tau^{-1}(z) &= \sum_{\sigma \in G} \tau^{-1}(f(\sigma)) \cdot \tau^{-1}\sigma(\alpha) = \sum_{\sigma \in G} \tau^{-1}(f(\tau\sigma))\sigma(\alpha) \\ &= \sum_{\sigma \in G} \tau^{-1}(f(\tau) \cdot \tau f(\sigma))\sigma(\alpha) = \tau^{-1}(f(\tau)) \sum_{\sigma \in G} f(\sigma)\sigma(\alpha) = \tau^{-1}(f(\tau))z.\end{aligned}$$

Thus,

$$f(\tau) = \frac{z}{\tau(z)},$$

so f is the 1-coboundary of z^{-1}. ∎

This has the usual statement of Hilbert's Theorem 90 as a corollary.

Corollary 2.4.4. *Let L/K be a finite cyclic extension of fields, and let $N_{L/K} : L^\times \to K^\times$ be the norm map. Then*

$$\ker N_{L/K} = \left\{ \alpha \in L^\times \mid \alpha = \frac{\sigma(\beta)}{\beta} \text{ for some } \beta \in L^\times \right\},$$

where σ is a generator of $\mathrm{Gal}(L/K)$.

Proof. Since σ generates $G = \mathrm{Gal}(L/K)$, the element $\sigma - 1 \in \mathbb{Z}[G]$ generates I_G, and so the statement at hand is $\ker N_{L/K} = I_G L^\times$, which is to say $\hat{H}^{-1}(G, L^\times) = 0$. Since G is cyclic, we have $\hat{H}^{-1}(G, L^\times) \cong H^1(G, L^\times)$. Thus, the result follows from Theorem 2.4.3. ∎

For the additive group, we have the following much stronger generalization of the additive version of Hilbert's Theorem 90.

Theorem 2.4.5. *Let L/K be a Galois extension of fields. Then $H^i(\mathrm{Gal}(L/K), L) = 0$ for all $i \geq 1$.*

Proof. As in the proof of Theorem 2.4.3, this reduces quickly to the case that L/K is finite, which we therefore suppose. As a $K[G]$-module, L is free on a single generator by the normal basis theorem, and therefore it is isomorphic to

$$Z[G] \otimes_{\mathbb{Z}} K \cong \mathrm{Ind}^G(K) \cong \mathrm{CoInd}^G(K).$$

So, the result follows from the acyclicity of coinduced modules. ∎

Notation 2.4.6. For a field K, we let K^{sep} denote a fixed separable closure and G_K denote its absolute Galois group.

Definition 2.4.7. The Brauer group $\mathrm{Br}(K)$ of a field K is $H^2(G_K, (K^{\mathrm{sep}})^\times)$.

We have the following inflation-restriction theorem for Brauer groups.

Proposition 2.4.8. *For any Galois extension L/K, there is an exact sequence*

$$0 \to H^2(\mathrm{Gal}(L/K), L^\times) \xrightarrow{\mathrm{Inf}} \mathrm{Br}(K) \xrightarrow{\mathrm{Res}} \mathrm{Br}(L)$$

of abelian groups.

Proof. Let K^{sep} be a separable closure of K containing L. Note that $((K^{\mathrm{sep}})^\times)^{G_L} = L^\times$ by the fundamental theorem of Galois theory, and we have $H^1(G_L, (K^{\mathrm{sep}})^\times) = 0$ by Theorem 2.4.3. The sequence is then just the inflation-restriction sequence of Proposition 2.2.18 for $i = 2, G = G_K$, $N = G_L$, and $A = (K^{\mathrm{sep}})^\times$. ∎

Example 2.4.9. Consider the finite field $\mathbb{F}_q$ for a prime power q. For $n \geq 1$, we know that $\mathbb{F}_{q^n}/\mathbb{F}_q$ is cyclic of degree n, so we have an isomorphism

$$H^2(\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q), \mathbb{F}_{q^n}^\times) \cong \hat{H}^0(\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q), \mathbb{F}_{q^n}^\times) \cong \mathbb{F}_q^\times / N_{\mathbb{F}_{q^n}/\mathbb{F}_q} \mathbb{F}_{q^n}^\times.$$

Now, the norm of any primitive $(q^n - 1)$th root of unity ξ is

$$N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\xi) = \prod_{i=0}^{n-1} \xi^{q^i} = \xi^{\frac{q^n-1}{q-1}},$$

which is a primitive $(q-1)$th root of unity. In other words, the norm map is surjective, so

$$\mathrm{Br}(\mathbb{F}_q) = \varinjlim_n H^2(\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q), \mathbb{F}_{q^n}^\times) = 0.$$

2.5 Kummer theory

Notation 2.5.1. For a field K of characteristic not dividing $n \geq 1$, we use μ_n to denote the group of nth roots of unity in K^{sep}.

Notation 2.5.2. For an abelian group A and $n \geq 1$, let $A[n]$ denote the elements of exponent dividing n in A.

Example 2.5.3. We have $K^{\mathrm{sep}}[n] = \mu_n$ for any $n \geq 1$ not divisible by $\mathrm{char}(K)$.

Proposition 2.5.4. *Let K be a field of characteristic not dividing $n \geq 1$, and let μ_n be the group of roots of unity in a separable closure K^{sep} of K. Let $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ be the absolute Galois group. Then there are canonical isomorphisms*

$$K^\times/K^{\times n} \xrightarrow{\sim} H^1(G_K, \mu_n) \quad \text{and} \quad H^2(G_K, \mu_n) \xrightarrow{\sim} \mathrm{Br}_K[n].$$

Proof. Since K^{sep} is separably closed, we have an exact sequence

$$1 \to \mu_n \to (K^{\mathrm{sep}})^\times \xrightarrow{n} (K^{\mathrm{sep}})^\times \to 1 \tag{2.5.1}$$

of discrete G_K-modules. By Hilbert's Theorem 90, the long exact sequence attached to (2.5.1) breaks into exact sequences

$$K^\times \xrightarrow{n} K^\times \to H^1(G_K, \mu_n) \to 0 \quad \text{and} \quad 0 \to H^2(G_K, \mu_n) \to \mathrm{Br}(K) \xrightarrow{n} \mathrm{Br}(K).$$

[

Terminology 2.5.5. The sequence in (2.5.1) is often called a *Kummer sequence.*

Definition 2.5.6. Let K be a field of characteristic not dividing $n \geq 1$, let $a \in K^\times$, and choose an nth

sep × root $\alpha \in (K^{\text{sep}})$ of a. The *Kummer cocycle* $\chi_a \colon G_K \to \mu_n$ attached to a (or more precisely, α) is the 1-cocycle defined on $\sigma \in G_K$ by

$$\chi_a(\sigma) = \frac{\sigma(\alpha)}{\alpha}.$$

Remarks 2.5.7. We maintain the notation of Definition 2.5.6.

a. If $\mu_n \subset K$, then χ_a is independent of the choice of α and is in fact a group homomorphism, since G_K acts trivially on μ_n. In this case, we refer to χ_a as the *Kummer character* attached to a.

b. The class of χ_a in $H^1(G_K, \mu_n)$ is independent of the choice of α, as the difference between two such choices is the 1-coboundary of an nth root of unity.

Lemma 2.5.8. *Let K be a field of characteristic not dividing $n \geq 1$. Then the isomorphism $K^\times/K^{\times n} \xrightarrow{\sim} H^1(G_K, \mu_n)$ of Proposition 2.5.4 takes the image of $a \in K^\times$ to χ_a.*

Proof. The connecting homomorphism yielding the map is the snake lemma map in the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu_n & \longrightarrow & (K^{\text{sep}})^\times & \xrightarrow{n} & (K^{\text{sep}})^\times & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle d^0} & & \downarrow{\scriptstyle d^0} & & \downarrow{\scriptstyle d^0} & & \\ 0 & \longrightarrow & Z^1(G_K, \mu_n) & \longrightarrow & Z^1(G_K, (K^{\text{sep}})^\times) & \xrightarrow{n} & Z^1(G_K, (K^{\text{sep}})^\times) & \longrightarrow & 0, \end{array}$$

so given on $a \in K^\times$ by picking $\alpha \in (K^{\text{sep}})^\times$ with $\alpha^n = a$, taking $d^0(\alpha) \in Z^1(G_K, K^\times)$ and noting that it takes values in μ_n. Since $d^0(\alpha) = \chi_a$ by definition, we are done. ∎

Terminology 2.5.9. The isomorphism $K^\times/K^{\times n} \xrightarrow{\sim} H^1(G_K, \mu_n)$ of Lemma 2.5.8 is called the *Kummer isomorphism.*

Proposition 2.5.10. *Let L/K be a Galois extension of fields of characteristic not dividing $n \geq 1$, and suppose that μ_n is contained in L. Then the Kummer isomorphism restricts to an isomorphism*

$$(K^\times \cap L^{\times n})/K^{\times n} \xrightarrow{\sim} H^1(\text{Gal}(L/K), \mu_n).$$

Proof. This is a simple consequence of the inflation-restriction sequence combined with the Kummer isomorphisms for K and L. These yield a left exact sequence

$$0 \to H^1(\text{Gal}(L/K), \mu_n) \to K^\times/K^{\times n} \to L^\times/L^{\times n}$$

that provides the isomorphism. ∎

Proposition 2.5.11. *Let K be a field of characteristic not dividing $n \geq 1$, and suppose that K contains the nth roots of unity. Let L/K be a cyclic extension of degree n. Then $L = K(\sqrt[n]{a})$ for some $a \in K^\times$.*

Proof. Let ζ be a primitive nth root of unity in K. Note that $N_{L/K}(\zeta) = \zeta^n = 1$, so Hilbert's

Theorem 90 tells us that there exists $\alpha \in L$ and a generator σ of $\text{Gal}(L/K)$ with $\frac{\sigma(\alpha)}{\alpha} = \zeta$. Note that

$$N_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma^i \alpha = \prod_{i=1}^{n} \zeta^i \alpha = \zeta^{n(n-1)/2} \alpha^n = (-1)^{n-1} \alpha^n,$$

so setting $a = -N_{L/K}(-\alpha)$, we have $\alpha^n = a$. Since α has n distinct conjugates in L, we have that $L = K(\alpha)$. ∎

Notation 2.5.12. Let Δ be a subset of a field K, and let $n \geq 1$ be such that K contains the nth roots of unity in K. Then the field $K(\sqrt[n]{\Delta})$ is the field given by adjoining an nth root of each element of Δ to K.

Theorem 2.5.13 (Kummer duality)**.** *Let K be a field of characteristic not dividing $n \geq 1$, and suppose that K contains the nth roots of unity. Let L be an abelian extension of K of exponent dividing n, and set $\Delta = L^{\times n} \cap K^\times$. Then $L = K(\sqrt[n]{\Delta})$, and there is a perfect bimultiplicative pairing*

$$\langle\ ,\ \rangle\colon \mathrm{Gal}(L/K) \times \Delta/K^{\times n} \to \mu_n$$

given by $\langle \sigma, a\rangle = \chi_a(\sigma)$ for $\sigma \in \mathrm{Gal}(L/K)$ and $a \in \Delta$.

Proof. Since $\mu_n \subset K$, Proposition 2.5.10 tells us that the map taking $a \in \Delta$ to its Kummer cocycle χ_a yields

$$\Delta/K^{\times n} \cong \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n).$$

This isomorphism gives rise to the bimultiplicative pairing $\langle\ ,\ \rangle$, and it implies that any $a \in \Delta/K^{\times n}$ of order d dividing n pairs with some element of $\mathrm{Gal}(L/K)$ to a dth root of unity. It remains to show that the pairing also induces an isomorphism

$$\mathrm{Hom}(\Delta/K^{\times n}, \mu_n) \cong \mathrm{Gal}(L/K).$$

Clearly, $K(\sqrt[n]{\Delta})$ is contained in L. On the other hand, L/K is a compositum of cyclic extensions of exponent dividing n, we have by Proposition 2.5.11 that $L = K(\sqrt[n]{\Gamma})$ for some subset Γ of $K^\times$, which then can be taken to be Δ. So, let $\sigma \in \mathrm{Gal}(L/K)$ be of order d dividing n. Since $L = K(\sqrt[n]{\Delta})$, we have that there exists $a \in \Delta$ such that $\sigma(\alpha)/\alpha$ for $\alpha \in L$ with $\alpha^n = a$ is a primitive dth root of unity times α. Hence, the pairing is perfect. ∎

Remark 2.5.14. One may replace Δ in Theorem 2.5.13 by any $\Gamma \subseteq \Delta$ with $\Delta = \Gamma K^{\times n}$. Then $\Delta/K^{\times n}$ should be replaced by the isomorphic $\Gamma/(\Gamma \cap K^{\times n})$.

Remark 2.5.15. The pairing of Proposition 2.5.13 is perfect with respect to the Krull topology on $\mathrm{Gal}(L/K)$ and the discrete topology on Δ.

Terminology 2.5.16. We say that $\mathrm{Gal}(L/K)$ and $\Delta/K^{\times n}$ in Proposition 2.5.13 are *Kummer dual* to each other.

Corollary 2.5.17. *Let K be a field of characteristic not dividing $n \geq 1$, and suppose that K contains the nth roots of unity. The Galois group of the maximal abelian extension of K of exponent n is Kummer dual to $K^\times/K^{\times n}$.*

Remark 2.5.18. Suppose that K contains μ_n, where n is not divisible by the residue characteristic of K. Let L/K be abelian of exponent n and $G = \mathrm{Gal}(L/K)$. Write $L = K(\sqrt[n]{\Delta})$ for some $\Delta \leq K^\times$. Then $L_d = K(\sqrt[d]{\Delta})$ is the maximal subextension of exponent dividing d, and $G_d = \mathrm{Gal}(L_d/K) \cong G/G^d$. Moreover, we have a commutative diagram of pairings

$$\begin{array}{ccc} G \times \Delta/(\Delta \cap K^{\times n}) & \xrightarrow{\langle\ ,\ \rangle} & \mu_n \\ \downarrow & & \downarrow \\ G_d \times \Delta/(\Delta \cap K^{\times d}) & \xrightarrow{\langle\ ,\ \rangle_d} & \mu_d, \end{array}$$

where the left vertical map is the direct product of the restriction (or the quotient map) with the map induced by the identity and the map $\mu_n \to \mu_d$ is the n/d-power map. That is, we have

$$\langle \sigma, a\rangle_d = \frac{\sigma(\sqrt[d]{a})}{\sqrt[d]{a}} = \left(\frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}\right)^{n/d} = \langle \sigma, a\rangle^{n/d},$$

where σ denotes both an element of G and its image in G_d and a denotes the image of an element of Δ. In particular, the composition

$$G \to \mathrm{Hom}(\Delta, \mu_n) \to \mathrm{Hom}(\Delta, \mu_d)$$

in which the first map is given by $\langle\ ,\ \rangle$ and the second by the (n/d)-power map agrees with the map $G \to \mathrm{Hom}(\Delta, \mu_d)$ given by $\langle\ ,\ \rangle_d$.

Remark 2.5.19. By Kummer duality, if K has characteristic 0 and contains all roots of unity, then

$$G_K^{\mathrm{atab}} \cong \varprojlim_n G_K^{\mathrm{atab}}/(G_K^{\mathrm{atab}})^n \cong \varprojlim_n \mathrm{Hom}(K^\times, \mu_n) \cong \varprojlim_n \mathrm{Hom}_{\mathrm{cts}}(\widehat{K^\times}, \mu_n) \cong \mathrm{Hom}_{\mathrm{cts}}\Big(\widehat{K^\times}, \varprojlim_n \mu_n\Big),$$

where $\widehat{K^\times}$ denotes the profinite completion of $K^\times$.

Example 2.5.20. Let K be a field of characteristic not p containing the group μ_{p^∞} of all p-power roots of unity, and let $a \in K^\times$ with $a \notin K^{\times p}$. Then the field $L = K(\sqrt[p^\infty]{a})$ given by adjoining all p-power roots of a to K is the union of the fields $L_n = K(\sqrt[p^n]{a})$, each of which has degree p^n over K by Theorem 2.5.13 since a has order p^n in $K^\times/K^{\times p^n}$. Let $\Delta = \langle a \rangle$. Then

$$\mathrm{Gal}(L/K) \cong \varprojlim \mathrm{Gal}(L_n/K) \cong \varprojlim_n \mathrm{Hom}(\Delta, \mu_{p^n}) \cong \varprojlim_n \mu_{p^n} \cong \mathbb{Z}_p,$$

since a homomorphism from Δ is determined by where it sends a.

Definition 2.5.21. Let K be a field of characteristic p. The *Tate module* $\mathbb{Z}_p(1)$ is the topological G_K-module that is $\mathbb{Z}_p$ as a topological group together with the action of the G_K given by

$$\sigma \cdot a = \chi(\sigma)a$$

for $a \in \mathbb{Z}_p$, where $\chi : G_K \to \mathbb{Z}_p^\times$ is the p-adic cyclotomic character.

Remark 2.5.22. Let K be a field of characteristic not p, set $G = \mathrm{Gal}(K(\mu_{p^\infty})/K)$. The group

$$T_p = \varprojlim_n \mu_{p^n}$$

is a Galois module also referred to as the Tate module, the action of G given by multiplication by the p-adic cyclotomic character $\chi : G \to \mathbb{Z}_p^\times$ (which factors through G) in the sense that

$$\sigma((\xi_n)_n) = (\xi_n^{\chi(\sigma)})_n$$

for all $(\xi_n)_n \in T_p$. The group T_p is noncanonically topologically isomorphic to the Tate module $\mathbb{Z}_p(1)$, with the isomorphism given by choice of a compatible sequence $(\zeta_{p^n})_n$ of primitive p^nth roots of unity, which is taken to 1.

Example 2.5.23. Let K be a field of characteristic not p and $a \in K^\times - K^{\times p}$. Set $L = K(\mu_{p^\infty})$ and $M = L(\sqrt[p^\infty]{a})$. By Example 2.5.20, we know that $\mathrm{Gal}(M/L) \cong \mathbb{Z}_p$ as topological groups. But note that M/K is Galois. In fact, take $\sigma \in \mathrm{Gal}(L/K)$ and lift it to an embedding δ of M into a separable closure of M. Then

$$\tilde{\sigma}(\sqrt[p^n]{a})^{p^n} = a,$$

so $\tilde{\sigma}(\sqrt[p^n]{a}) = \xi\sqrt[p^n]{a}$ for some p^nth root of unity ξ, which is in M by definition. To determine the Galois group, take $\tau \in \mathrm{Gal}(M/L)$, and let ζ be the p^nth root of unity such that $\tau(\sqrt[p^n]{a}) = \zeta\sqrt[p^n]{a}$. For $n \geq 1$, we then have

$$\tilde{\sigma}\tau\tilde{\sigma}^{-1}(\sqrt[p^n]{a}) = \tilde{\sigma}(\tau(\tilde{\sigma}^{-1}(\xi^{-1})\sqrt[p^n]{a})) = \tilde{\sigma}(\sigma^{-1}(\xi^{-1})\xi\sqrt[p^n]{a}) = \sigma(\zeta)\xi\sqrt[p^n]{a} = \zeta^{\chi(\sigma)}\sqrt[p^n]{a},$$

where χ is the p-adic cyclotomic character. In other words, we have

$$\mathrm{Gal}(M/L) \cong \mathrm{Gal}(M/L) \rtimes \mathrm{Gal}(L/K) \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p^\times,$$

where through the conjugation action of $\mathrm{Gal}(L/K)$ on $\mathrm{Gal}(M/L)$, the latter module is isomorphic to the Tate module $\mathbb{Z}_p(1)$.

2. LOCAL CLASS FIELD THEORY: COHOMOLOGY

J. S. Milne, Class Field Theory (v4.03)

In this chapter, we develop the cohomological approach to local class field theory. We first prove that there exists a local Artin map (Theorem 3.4). Together with the theorems of Chapter I, §§1–3, this suffices to complete the proofs of the main theorems of local class field theory. For those who skipped the Lubin-Tate theory, we then give a proof of the main theorems that is independent of Chapter I (except for §1).

Throughout this chapter, "local field" means "nonarchimedean local field". As before, K^{al} denotes an algebraic closure of K (or separable algebraic closure in the case that K has characteristic $p \neq 0$), and "extension of K" means "subfield of K^{al} containing K". All cohomology groups will computed using continuous cochains (see II, §4). For a Galois extension of fields L/K (possibly infinite), set

$$H^2(L/K) = H^2(\mathrm{Gal}(L/K), L^\times).$$

For the moment, $H^2(L/K)$ is just a cohomology group, but in the next chapter we shall see that it has an explicit interpretation as the relative Brauer group of L/K.

1 The Cohomology of Unramified Extensions

The cohomology of the units

Let K be a local field.

PROPOSITION 1.1 *Let L/K be a finite unramified extension with Galois group G, and let U_L be the group of units in L. Then*

$$H_T^r(G, U_L) = 0, \quad \text{all } r.$$

PROOF. If π is a prime element of L, then every element of $L^\times$ can be written uniquely in the form $\alpha = u\pi^m$, $u \in U_L$, $m \in \mathbb{Z}$. Thus

$$L^\times = U_L \cdot \pi^{\mathbb{Z}} \simeq U_L \times \mathbb{Z}. \tag{26}$$

Since L is unramified over K, we can choose $\pi \in K$. Then $\tau\alpha = \tau(u\pi^m) = (\tau u)\pi^m$ for $\tau \in \mathrm{Gal}(L/K)$, and so (26) becomes a decomposition of G-modules when we let G act trivially on $\pi^{\mathbb{Z}} \simeq \mathbb{Z}$. Therefore, $H^r(G, U_L)$ is a direct summand of $H^r(G, L^\times)$ (see II, 1.25). Since $H^1(G, L^\times) = 0$ by Hilbert's theorem 90 (II, 1.22), this shows that $H^1(G, U_L) = 0$. Because G is cyclic, to complete the proof of the theorem, it suffices (by II, 3.4) to show that $H_T^0(G, U_L) = 0$. This is accomplished by the next proposition. □

PROPOSITION 1.2 *Let L/K be a finite unramified extension. Then the norm map $\mathrm{Nm}_{L/K}\colon U_L \to U_K$ is surjective.*

We first need some lemmas. Let l and k be the residue fields of L and K. Because L/K is unramified, the action of G on $\mathcal{O}_L$ defines an isomorphism $G \simeq \mathrm{Gal}(l/k)$.

LEMMA 1.3 *For $m > 0$, let $U_L^{(m)} = 1 + \mathfrak{m}_L^m$. Then*

$$U_L/U_L^{(1)} \xrightarrow{\simeq} l^\times$$
$$U_L^{(m)}/U_L^{(m+1)} \xrightarrow{\approx} l$$

as G-modules.

PROOF. Let π be a prime element of K. It remains prime in L, and

$$U_L^{(m)} = \{1 + a\pi^m \mid a \in \mathcal{O}_L\}.$$

The maps

$$\begin{aligned} u &\mapsto u \mod \mathfrak{m}_L : U_L \to l^\times \\ 1 + a\pi^m &\mapsto a \mod \mathfrak{m}_L : U_L^{(m)} \to l \end{aligned}$$

induce the required isomorphisms. □

LEMMA 1.4 *For all r, $H_T^r(G, l^\times) = 0$. In particular, the norm map $l^\times \to k^\times$ is surjective.*

PROOF. By Hilbert's Theorem 90 (II, 1.22), $H^1(G, l^\times) = 0$, and because $l^\times$ is finite, its Herbrand quotient $h(l^\times) = 1$ (see II 3.8). Therefore $H^2(G, l^\times) = 0$, and this implies that all the groups are zero (by II, 3.4). □

LEMMA 1.5 *The group $H_T^r(G, l) = 0$ for all r. In particular, the trace map $l \to k$ is surjective.*

PROOF. In (II, 1.24) this is proved for $r > 0$, which implies it for all r (by II, 3.4). □

PROOF (OF PROPOSITION 1.2) There are commutative diagrams ($m > 0$)

$$\begin{array}{ccc} U_L & \longrightarrow & l^\times \\ \downarrow{\scriptstyle \mathrm{Nm}} & & \downarrow{\scriptstyle \mathrm{Nm}} \\ U_K & \longrightarrow & k^\times \end{array} \qquad \begin{array}{ccc} U_L^{(m)} & \longrightarrow & l \\ \downarrow{\scriptstyle \mathrm{Nm}} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ U_K^{(m)} & \longrightarrow & k. \end{array}$$

Consider $u \in U_K$. Because the norm map $l^\times \to k^\times$ is surjective, there exists a $v_0 \in U_L$ such that $\mathrm{Nm}(v_0)$ and u have the same image in $k^\times$, i.e., such that $u/\mathrm{Nm}(v_0) \in U_K^{(1)}$. Because the trace map $l \to k$ is surjective, there exists a $v_1 \in U_L^{(1)}$ such that

$\mathrm{Nm}(v_1) \equiv u/\mathrm{Nm}(v_0) \mod U_K^{(2)}$. Continuing in this fashion, we obtain a sequence of elements $v_0, v_1, v_2, v_3, \ldots, v_i \in U_L^{(i)}$, such that $u/\mathrm{Nm}(v_0 \cdots v_i) \in U_K^{(i+1)}$. Let $v =$ $\lim_{m\to\infty} \prod_{j=0}^m v_j$. Then $u/\mathrm{Nm}(v) \in \bigcap U_K^{(i)} = \{1\}$. □

COROLLARY 1.6 *Let L/K be an infinite unramified extension with Galois group G. Then $H^r(G, U_L) = 0$ for $r > 0$ (continuous cochains).*

PROOF. The field L is a union of finite extensions K' of K, and so (see II, 4.2),

$$H^r(\mathrm{Gal}(L/K), U_L) \simeq \varinjlim_{K'} H^r(\mathrm{Gal}(K'/K), U_{K'}) = 0.$$ □

The invariant map

Let L be an unramified extension of K (possibly infinite), and let $G = \mathrm{Gal}(L/K)$.

As $H^2(G, U_L) = 0 = H^3(G, U_L)$, the cohomology sequence of the short exact sequence

$$0 \to U_L \to L^\times \xrightarrow{\mathrm{ord}_L} \mathbb{Z} \to 0,$$

gives an isomorphism

$$H^2(G, L^\times) \xrightarrow[\simeq]{H^2(\mathrm{ord}_L)} H^2(G, \mathbb{Z}).$$

The groups $H^r(G,\mathbb{Q})$ are torsion for $r>0$ (see II, 4.3) and uniquely divisible (because $\mathbb{Q}$ is), and hence zero. Therefore the cohomology sequence of the short exact sequence

$$0\to\mathbb{Z}\to\mathbb{Q}\to\mathbb{Q}/\mathbb{Z}\to 0$$

(trivial G-actions) gives an isomorphism

$$H^1(G,\mathbb{Q}/\mathbb{Z})\xrightarrow{\delta}H^2(G,\mathbb{Z}).$$

Recall that

$$H^1(G,\mathbb{Q}/\mathbb{Z})\simeq\mathrm{Hom}_{\mathrm{cts}}(G,\mathbb{Q}/\mathbb{Z})$$

and that G has a canonical topological generator, namely, the Frobenius element $\sigma=\mathrm{Frob}_{L/K}$. The composite of

$$H^2(L/K)\xrightarrow[\simeq]{\mathrm{ord}_L}H^2(G,\mathbb{Z})\xleftarrow[\simeq]{\delta}H^1(G,\mathbb{Q}/\mathbb{Z})\simeq\mathrm{Hom}_{\mathrm{cts}}(G,\mathbb{Q}/\mathbb{Z})\xrightarrow{f\mapsto f(\sigma)}\mathbb{Q}/\mathbb{Z}$$

is called the **invariant map**

$$\mathrm{inv}_{L/K}\colon H^2(L/K)\to\mathbb{Q}/\mathbb{Z}.$$

Consider a tower of field extensions

$$E\supset L\supset K$$

with both E and L unramified (hence Galois) over K. Then

$$\begin{array}{ccc}H^2(L/K)&\xrightarrow{\mathrm{inv}_{L/K}}&\mathbb{Q}/\mathbb{Z}\\ \downarrow{\scriptstyle\mathrm{Inf}}&&\|\\ H^2(E/K)&\xrightarrow{\mathrm{inv}_{E/K}}&\mathbb{Q}/\mathbb{Z}\end{array}$$

commutes, because all the maps in the definition of inv are compatible with Inf.

THEOREM 1.7 *There exists a unique isomorphism*

$$\mathrm{inv}_K\colon H^2(K^{\mathrm{un}}/K)\to\mathbb{Q}/\mathbb{Z},$$

with the property that, for every $L\subset K^{\mathrm{un}}$ of finite degree n over K, inv_K induces the isomorphism

$$\mathrm{inv}_{L/K}\colon H^2(L/K)\to\tfrac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}.$$

PROOF. This is an immediate consequence of the above discussion. □

PROPOSITION 1.8 *Let L be a finite extension of K of degree n, and let K^{un} and L^{un} be the largest unramified extensions of K and L. Then the following diagram commutes:*

$$\begin{array}{ccc}H^2(K^{\mathrm{un}}/K)&\xrightarrow{\mathrm{Res}}&H^2(L^{\mathrm{un}}/L)\\ \downarrow{\scriptstyle\mathrm{inv}_K}&&\downarrow{\scriptstyle\mathrm{inv}_L}\\ \mathbb{Q}/\mathbb{Z}&\xrightarrow{\quad n\quad}&\mathbb{Q}/\mathbb{Z}.\end{array}\tag{27}$$

PROOF. The largest unramified extension of a local field is obtained by adjoining all mth roots of 1 for m not divisible by the residue characteristic. Therefore, $L^{\mathrm{un}}=L\cdot K^{\mathrm{un}}$, and so the map

$$\mapsto\tau|K^{\mathrm{un}}\colon\mathrm{Gal}(L^{\mathrm{un}}/L)\to\mathrm{Gal}(K^{\mathrm{un}}/K)$$

is injective. The map denoted Res in (27) is that defined by the compatible homomorphisms

$$\begin{array}{ccc}\mathrm{Gal}(K^{\mathrm{un}}/K)&\leftarrow&\mathrm{Gal}(L^{\mathrm{un}}/L)\\ K^{\mathrm{un}\times}&\to&L^{\mathrm{un}\times}\end{array}$$

(II, 1.27b).

Let $\Gamma_K = \mathrm{Gal}(K^{\mathrm{un}}/K)$ and $\Gamma_L = \mathrm{Gal}(L^{\mathrm{un}}/L)$, and consider the diagram,

$$\begin{array}{ccccccc} H^2(K^{\mathrm{un}}/K) & \xrightarrow[\simeq]{\mathrm{ord}_K} & H^2(\Gamma_K,\mathbb{Z}) & \xleftarrow[\simeq]{\delta} & H^1(\Gamma_K,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{g\mapsto g(\sigma_K)} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle e\,\mathrm{Res}} & & \downarrow{\scriptstyle e\,\mathrm{Res}} & & \downarrow{\scriptstyle fe} \\ H^2(L^{\mathrm{un}}/L) & \xrightarrow[\simeq]{\mathrm{ord}_L} & H^2(\Gamma_L,\mathbb{Z}) & \xleftarrow[\simeq]{\delta} & H^1(\Gamma_L,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{g\mapsto g(\sigma_L)} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

Here e is the ramification index for L/K and f is the residue class degree. The first square is obtained from the commutative square

$$\begin{array}{ccc} K^{\mathrm{un}\times} & \xrightarrow{\mathrm{ord}_K} & \mathbb{Z} \\ \downarrow & & \downarrow{\scriptstyle e} \\ L^{\mathrm{un}\times} & \xrightarrow{\mathrm{ord}_L} & \mathbb{Z}. \end{array}$$

The second square expresses the fact that the restriction map commutes with the boundary map. Apart from the factor "e", the third square is

$$\begin{array}{ccc} \mathrm{Hom}(\Gamma_K,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{g\mapsto g(\sigma_K)} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle g\mapsto g|\Gamma_L} & & \downarrow{\scriptstyle f} \\ \mathrm{Hom}(\Gamma_L,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{g\mapsto g(\sigma_L)} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

The Frobenius elements σ_K and σ_L are determined by the fact that they induce $x \mapsto x^q$ and $x \mapsto x^{q^f}$ respectively on the residue fields, where $q = |k|$ and $q^f = |l|$, and so $\sigma_L|K^{\mathrm{un}} = \sigma_K^f$. It is now clear that the square commutes, and since $n = ef$, this proves the proposition. □

The local Artin map

Let L be a finite unramified extension of K with Galois group G, and let $n = [L\colon K]$. The **local fundamental class** $u_{L/K}$ is the element of $H^2(L/K)$ mapped to the generator $\frac{1}{[L:K]}$ of $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ by the invariant map $\mathrm{inv}_{L/K}\colon H^2(L/K) \xrightarrow{\simeq} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$. The pair $(G, L^\times)$ satisfies the hypotheses of Tate's theorem (II, 3.11),[1] and so cup-product with the fundamental class $u_{L/K}$ defines an isomorphism

$$H_T^r(G,\mathbb{Z}) \to H_T^{r+2}(G, L^\times)$$

for all $r \in \mathbb{Z}$. For $r = -2$, this becomes

$$\begin{array}{ccc} H^{-2}(G,\mathbb{Z}) & \xrightarrow{\simeq} & H^0(G,L^\times) \\ \|_{\text{II, 2.7}} & & \| \\ G & & K^\times/\mathrm{Nm}(L^\times). \end{array}$$

We now compute this map explicitly.

A prime element π of K is also a prime element of L, and defines a decomposition

$$L^\times = U_L \cdot \pi^{\mathbb{Z}} \simeq U_L \times \mathbb{Z}$$

of G-modules. Thus

$$H^r(G,L^\times) \simeq H^r(G,U_L) \oplus H^r(G,\pi^{\mathbb{Z}}).$$

Choose a generator σ of G (e.g., the Frobenius generator), and let

$$f \in H^1(G, \mathbb{Q}/\mathbb{Z}) \simeq \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$$

be the element such that $f(\sigma^i) = \frac{i}{n} \bmod \mathbb{Z}$ for all i. It generates $H^1(G, \mathbb{Q}/\mathbb{Z})$.

From the exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

and the fact that $H^r(G, \mathbb{Q}) = 0$ for all r, we obtain an isomorphism

$$\delta\colon H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z}).$$

According to the description of δ in (II, 1.21), to construct δf , we first choose a lifting of f to 1-cochain $\tilde{f}\colon G \to \mathbb{Q}$. We take $\tilde{f}$ to be the map $\sigma^i \mapsto \frac{i}{n}$, where $0 \le i < n-1$. Then

$$d\tilde{f}(\sigma^i, \sigma^j) = \sigma^i \tilde{f}(\sigma^j) - \tilde{f}(\sigma^{i+j}) + \tilde{f}(\sigma^i) = \begin{cases} 0 & \text{if} \quad i+j \le n-1 \\ 1 & \text{if} \quad i+j > n-1. \end{cases}$$

[1]For the condition on H^1, use Hilbert's Theorem 90, and for the condition on H^2, use the invariant map. When we identify $\mathbb{Z}$ with the subgroup $\pi^{\mathbb{Z}}$ of $L^\times$, we find that the fundamental class $u_{L/K} \in H^2(G, L^\times)$ is represented by the cocycle:

$$\varphi(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{if} \quad i+j \le n-1 \\ \pi & \text{if} \quad i+j > n-1 \end{cases}$$

From the exact sequences

$$0 \to I \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

$$0 \to L^\times \to L^\times(\varphi) \to I \to 0$$

(see the proof of II, 3.11) we obtain boundary maps

$$H^{-2}(G, \mathbb{Z}) \to H^{-1}(G, I)$$

$$H^{-1}(G, I) \to H^0(G, L^\times),$$

which are isomorphisms because $\mathbb{Z}[G]$ and $L^\times(\varphi)$ have trivial cohomology. Here $L^\times(\varphi)$ is the splitting module $L^\times \oplus \bigoplus_{\sigma \in G, \sigma \ne 1} \mathbb{Z}x_\sigma$ of φ.

Finally, $H^{-2}(G, \mathbb{Z}) \overset{\text{def}}{=} H_1(G, \mathbb{Z}) \simeq G$ (see II, 2.7).

PROPOSITION 1.9 *Under the composite*

$$\begin{array}{ccc} H^{-2}(G, \mathbb{Z}) & \xrightarrow{\simeq} & H^0(G, L^\times) \\ \|_{\text{II, 2.7}} & & \| \\ G & & K^\times / \mathrm{Nm}(L^\times). \end{array}$$

of the above maps, the Frobenius element $\sigma \in G$ maps to the class of π in $K^\times / \mathrm{Nm}(L^\times)$.

Note that, because all units in K are norms from $L^\times$ (see 1.2), the class of π mod $\mathrm{Nm}(L^\times)$ is independent of the prime element π. On the other hand, the G-module $L^\times(\varphi)$ and the map depend on the choice of the generator σ for G.

PROOF. From the construction of the isomorphism $H^{-2}(G, \mathbb{Z}) \simeq G$, we see that the image of σ under the boundary map $H^{-2}(G, \mathbb{Z}) \to H^{-1}(G, I_G) \subset I_G/I_G^2$ is represented by $\sigma - 1$.

The boundary map $H^{-1}(G, I_G) \to H^0(G, L^\times)$ is that given by the snake lemma from the diagram (we write I for I_G):

$$\begin{array}{ccccccc} & & & & & & H^{-1}(G,I) \\ & & & & & & \downarrow \\ & & (L^\times)_G & \longrightarrow & L^\times(\varphi)_G & \longrightarrow & (I)_G & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & L^{\times G} & \longrightarrow & L^\times(\varphi)^G & \longrightarrow & I^G & & \\ & & \downarrow & & & & & & \\ & & H^0(G,L^\times). & & & & & & \end{array}$$

The vertical maps connecting the rows are $\mathrm{Nm}_G = \sum_{i=0}^{n-1} \sigma^i$. The element $(\sigma - 1) + I^2$ is the image of $x_\sigma + I \cdot L^\times(\varphi)$ in $L^\times(\varphi)_G$, and $\mathrm{Nm}_G(x_\sigma + I \cdot L^\times(\varphi))$ is the sum of the elements:

$$\begin{array}{rcl} x_\sigma & = & x_\sigma \\ \sigma x_\sigma & = & x_{\sigma^2} - x_\sigma + \varphi(\sigma,\sigma) \\ \sigma^2 x_\sigma & = & x_{\sigma^3} - x_{\sigma^2} + \varphi(\sigma,\sigma^2) \\ \cdots & & \cdots \\ \sigma^{n-1} x_\sigma & = & `x_1' - x_{\sigma^{n-1}} + \varphi(\sigma,\sigma^{n-1}) \end{array} .$$

On summing these, remembering that $`x_1' = \varphi(1,1) = 1$ and that $+$ on the factor $L^\times$ of $L(\varphi)$ is actually $\cdot$, we find that

$$\mathrm{Nm}_G(x_\sigma) = \prod_{i=1}^{n-1} \varphi(\sigma, \sigma^i) = \pi.$$

This completes the proof. □

REMARK 1.10 The above proof of Proposition 1.9, using Tate's original definition of the isomorphism $H^r(G,\mathbb{Z}) \to H^{r+2}(G, C)$, is simpler than that found in other references, which uses the description of the map in terms of cup products.

2 The Cohomology of Ramified Extensions

Because of Hilbert's Theorem 90 (II, 1.22), there is an exact sequence

$$0 \to H^2(L/K) \xrightarrow{\mathrm{Inf}} H^2(E/K) \xrightarrow{\mathrm{Res}} H^2(E/L)$$

for any tower of Galois extensions $E \supset L \supset K$ (see II, 1.36).

The next theorem extends Theorem 1.7 to ramified extensions.

THEOREM 2.1 *For every local field K, there exists a canonical isomorphism*

$$\mathrm{inv}_K \colon H^2(K^{\mathrm{al}}/K) \to \mathbb{Q}/\mathbb{Z}.$$

Let L be a Galois extension of K of degree $n < \infty$. Then the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^2(L/K) & \longrightarrow & H^2(K^{\mathrm{al}}/K) & \xrightarrow{\mathrm{Res}} & H^2(K^{\mathrm{al}}/L) \\ & & & & \downarrow{\scriptstyle \mathrm{inv}_K} & & \downarrow{\scriptstyle \mathrm{inv}_L} \\ 0 & \longrightarrow & \frac{1}{n}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z} \end{array} \qquad (28)$$

commutes, and therefore defines an isomorphism

$$\mathrm{inv}_{L/K}\colon H^2(L/K) \to \tfrac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

The proof will occupy most of the rest of the section.

LEMMA 2.2 *If L/K is Galois of finite degree n, then $H^2(L/K)$ contains a subgroup canonically isomorphic to $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$.* PROOF. Consider the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Ker}(\mathrm{Res}) & \longrightarrow & H^2(K^{\mathrm{un}}/K) & \xrightarrow{\mathrm{Res}} & H^2(L^{\mathrm{un}}/L) \\ & & \downarrow & & \downarrow{\scriptstyle \mathrm{Inf}} & & \downarrow{\scriptstyle \mathrm{Inf}} \\ 0 & \longrightarrow & H^2(L/K) & \longrightarrow & H^2(K^{\mathrm{al}}/K) & \xrightarrow{\mathrm{Res}} & H^2(K^{\mathrm{al}}/L) \end{array}$$

Since the two inflation maps are injective, so also is the first vertical map, but 1.8 shows that the kernel of the restriction map on the top row is canonically isomorphic to $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$. □

To complete the proof of Theorem 2.1, it suffices to prove that the map $\frac{1}{n}\mathbb{Z}/\mathbb{Z} \hookrightarrow H^2(L/K)$ is an isomorphism. There are two different approaches to proving this. In the next chapter on Brauer groups, we shall show that $H^2(K^{\mathrm{un}}/K) \simeq H^2(K^{\mathrm{al}}/K)$ (every central simple algebra over K is split by an unramified extension; see IV §4), and so the vertical maps in the above diagram are isomorphisms. The second proof, which we now present, shows that $\left|H^2(L/K)\right| \le n$.

LEMMA 2.3 *Let L be a finite Galois extension of K with Galois group G. Then there exists an open subgroup V of $\mathcal{O}_L$, stable under G, such that $H^r(G,V) = 0$ for all $r > 0$.*

PROOF. Let $\{x_\tau \mid \tau \in G\}$ be a normal basis for L over K (see FT, 5.18). The x have a common denominator d in $\mathcal{O}_K$ (see ANT, 2 .6). After replacing each x with $d\cdot x_\tau$, we may suppose that they lie in $\mathcal{O}_L$. Take $V = \sum \mathcal{O}_K x_\tau$. It is stable under G because the normal basis is. Let π be a prime element of $\mathcal{O}_L$. Then $V \supset \pi^m\mathcal{O}_L$ for some $m > 0$, which shows that V is open (it is union of cosets of $\pi^m\mathcal{O}_L$). Finally,

$$V \simeq \mathcal{O}_K[G] \simeq \mathrm{Ind}^G \mathcal{O}_K$$

as G-modules, and so $H^r(G,V) = 0$ for all $r > 0$ (II, 1.12). □

LEMMA 2.4 *Let L, K, and G, be as in the last lemma. Then there exists an open subgroup V of U_L stable under G such that $H^r(G,V) = 0$ for all $r > 0$.*

PROOF. I prove this only for K of characteristic zero.[2] The power series

$$e^x = 1 + x + \cdots + x^n/n! + \cdots$$

converges for $\mathrm{ord}(x) > \mathrm{ord}(p)/(p-1)$ (ANT, 7.29). It defines an isomorphism of an open neighbourhood of 0 in L onto an open neighbourhood of 1 in $L^\times$, with inverse mapping

$$\log(x) = (x-1) - (x-1)^2/2 + (x-1)^3/3 - \cdots.$$

Both maps commute with the actions of G (because G acts continuously). If V' is an open neighbourhood of 0 as in (2.3), then $\pi^M V'$ will have the same properties, and we can take $V = \exp(\pi^M V')$ with M chosen to be sufficiently large that the exponential function is defined and an isomorphism on $\pi^M V'$. □

LEMMA 2.5 *Let L/K be a cyclic extension of degree n; then $h(U_L) = 1$ and $h(L^\times) = n$.*

---

[2] For a proof of the characteristic p case, see p. 134 of Serre 1967b.

PROOF. Let V be an open subgroup of U_L with $H^r(G,V)=0$ for all r. Because U_L is compact, the quotient U_L/V is finite, and so $h(U_L)=h(V)=1$ by II, 3.9. Now $h(L^\times)=h(U_L)\cdot h(\mathbb{Z})=h(\mathbb{Z})$, and

$$h(\mathbb{Z})=\left|H^0_T(G,\mathbb{Z})\right|/\left|H^1(G,\mathbb{Z})\right|=\left|H^0_T(G,\mathbb{Z})\right|=|\mathbb{Z}/n\mathbb{Z}|=n. \qquad \square$$

LEMMA 2.6 *Let L be a finite Galois extension of K of order n, then $H^2(L/K)$ has order n.*

PROOF. We know that the order of $H^2(L/K)$ is divisible by n, and that it equals n when L/K is cyclic. We prove the lemma by induction on $[L\colon K]$. Because the group $\mathrm{Gal}(L/K)$ is solvable (ANT, 7.59), there exists a Galois extension K'/K with $L\supsetneq K'\supsetneq K$. From the exact sequence

$$0\to H^2(K'/K)\to H^2(L/K)\to H^2(L/K')$$

we see that

$$|H^2(L/K)|\le|H^2(K'/K)|\cdot|H^2(L/K')|$$
$$|H^2(L/K)|\le|H^2(K'/K)|\cdot|H^2(L/K')|=n. \qquad \square$$

PROOF (OF THEOREM 2.1) From the diagram in the proof of (2.2) we see that, for every finite Galois extension L of K, the subg roup $H^2(L/K)$ of $H^2(K^{\mathrm{al}}/K)$ is contained in $H^2(K^{\mathrm{un}}/K)$. Since $H^2(K^{\mathrm{al}}/K)=\bigcup H^2(L/K)$, this proves that the inflation map $H^2(K^{\mathrm{un}}/K)\to H^2(K^{\mathrm{al}}/K)$ is an isomorphism. Compose the inverse of this with the invariant map $\mathrm{inv}_K\colon H^2(K^{\mathrm{un}}/K)\to\mathbb{Q}/\mathbb{Z}$ of Theorem 1.7. $\square$

In fact, the diagram in Theorem 2.1 commutes even when L/K is not Galois:

$$\mathrm{inv}_L\circ\mathrm{Res}=[L:K]\,\mathrm{inv}_K\,. \tag{29}$$

(In this setting, we define $H^2(L/K)$ to be the kernel of the restriction map.)

I claim that

$$\mathrm{inv}_K\circ\mathrm{Cor}=\mathrm{inv}_L\,. \tag{30}$$

Because Res is surjective (see diagram (28)), to prove this it suffices to show that

$$\mathrm{inv}_K\circ\mathrm{Cor}\circ\mathrm{Res}=\mathrm{inv}_L\circ\mathrm{Res}\,.$$

But $\mathrm{Cor}\circ\mathrm{Res}=[L:K]$ by (II, 1.30), and so this is the preceding equality (29).

The fundamental class

Let L be a finite Galois extension of K with Galois group G. As in the unramified case, we define the **fundamental class** $u_{L/K}$ of L/K to be the element $u_{L/K}$ of $H^2(L/K)$ such that

$$\mathrm{inv}_{L/K}(u_{L/K})=\frac{1}{[L\colon K]}\bmod\mathbb{Z},$$

or, equivalently, such that

$$\mathrm{inv}_K(u_{L/K})=\frac{1}{[L:K]}\bmod\mathbb{Z}.$$

LEMMA 2.7 *Let $L\supset E\supset K$ with L/K finite and Galois. Then*

$$\mathrm{Res}(u_{L/K})=u_{L/E}, \tag{31}$$
$$\mathrm{Cor}(u_{L/E})=[E:K]u_{L/K}. \tag{32}$$

Moreover, if E/K is also Galois, then

$$\mathrm{Inf}(u_{E/K})=[L\colon E]u_{L/K}. \tag{33}$$

PROOF. Consider

$$\begin{array}{ccccc} H^2(K^{\mathrm{al}}/K) & \xrightarrow{\text{Res}} & H^2(K^{\mathrm{al}}/E) & \xrightarrow{\text{Res}} & H^2(K^{\mathrm{al}}/L) \\ \simeq\downarrow{\scriptstyle \mathrm{inv}_K} & & \simeq\downarrow{\scriptstyle \mathrm{inv}_E} & & \simeq\downarrow{\scriptstyle \mathrm{inv}_L} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{[E:K]} & \mathbb{Q}/\mathbb{Z} & \xrightarrow{[L:E]} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

On applying the kernel-cokernel lemma (II, A.2) to the rows (and using that the lemma is functorial), we obtain a commutative diagram,

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^2(E/K) & \xrightarrow{\text{Inf}} & H^2(L/K) & \xrightarrow{\text{Res}} & H^2(L/E) \\ & & \downarrow{\scriptstyle \mathrm{inv}_{E/K}} & & \downarrow{\scriptstyle \mathrm{inv}_{L/K}} & & \downarrow{\scriptstyle \mathrm{inv}_{L/K}} \\ 0 & \longrightarrow & \frac{1}{[E:K]}\mathbb{Z}/\mathbb{Z} & \xrightarrow{\text{id}} & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} & \xrightarrow{[E:K]} & \frac{1}{[L:E]}\mathbb{Z}/\mathbb{Z}. \end{array}$$

Here $H^2(E/K)$ is defined to be the kernel of $\mathrm{Res}\colon H^2(K^{\mathrm{al}}/K) \to H^2(K^{\mathrm{al}}/E)$. The equality (31) expresses the fact that the second square commutes. When E/K is Galois, the equality (33) expresses the fact that the first square commutes.

Equality (32) follows from comparing

$$\mathrm{inv}_K(\mathrm{Cor}_{E/K}(u_{L/E})) \overset{(30)}{=} \mathrm{inv}_E(u_{L/E}) = \frac{1}{[L\colon E]} \bmod \mathbb{Z}$$
$$\mathrm{inv}_K(u_{L/K}) = \frac{1}{[L\colon K]} \bmod \mathbb{Z}. \qquad \square$$

REMARK 2.8 There are groups $K^\times/\mathrm{Nm}(L^\times)$ and $H^2(L/K)$ attached to every finite extension L/K of local fields. When L/K is cyclic, they are isomorphic, but not otherwise. The first group is always isomorphic to $\mathrm{Gal}(M/K)$, where M is the largest abelian subextension of L/K (see 3.4, 3.5), and the second is always cyclic of order $[L:K]$. Thus, when L/K is abelian but not cyclic, the two groups have the same order but are not isomorphic, and when L/K is not abelian, they have different orders.

3 The Local Artin Map

The pair $(G, L^\times)$ satisfies the hypotheses of Tate's theorem (II, 3.11),and so we have proved the following result.

THEOREM 3.1 *For every finite Galois extension of local fields L/K and $r \in \mathbb{Z}$, the homo- morphism*

$$H_T^r(\mathrm{Gal}(L/K), \mathbb{Z}) \to H_T^{r+2}(\mathrm{Gal}(L/K), L^\times)$$

defined by $x \mapsto x \cup u_{L/K}$ is an isomorphism. When $r = -2$, this becomes an isomorphism

$$G^{\mathrm{ab}} \simeq K^\times/\mathrm{Nm}_{L/K}(L^\times).$$

If $L \supset E \supset K$ with L/K Galois, then the homomorphism in the theorem commutes with both Res and Cor. For example, to prove the statement for Res we must show that

$$\mathrm{Res}(x \cup u_{L/K}) = \mathrm{Res}(x) \cup u_{L/E}$$

for all $x \in H_T^r(\mathrm{Gal}(L/K), L^\times)$. But a standard property of cup-products (II, 1.39c) is that

$$\mathrm{Res}(x \cup u_{L/K}) = \mathrm{Res}(x) \cup \mathrm{Res}(u_{L/K}),$$

and so this follows from (31). The proof for Cor is similar.

If $L \supset E \supset K$ with L/K and E/K Galois and $x \in H^r(\mathrm{Gal}(E/K), E^\times)$ with $r \geq 1$, then

$$\mathrm{Inf}(x \cup u_{E/K}) = [L : E]\,\mathrm{Inf}(x) \cup u_{L/K}.$$

Again, this follows from a standard property of cup-products (1.39e) and the formula (33).

For $r = -2$, the map in the theorem becomes

$$\mathrm{Gal}(L/K)^{\mathrm{ab}} \xrightarrow{\simeq} K^\times / \mathrm{Nm}_{L/K} L^\times.$$

We denote the inverse map by

$$\theta_{L/K} : K^\times / \mathrm{Nm}_{L/K} L^\times \to \mathrm{Gal}(L/K)^{\mathrm{ab}}$$

and call it the **local Artin map**, or by $\mathrm{rec}_{L/K}$ and call it the **local reciprocity map.** (The second name is more common, but it is hard to see any reciprocity in the map.)

LEMMA 3.2 *Let $L \supset E \supset K$ be local fields with L/K Galois. Then the following diagrams commute:*

$$\begin{array}{ccc} E^\times & \xrightarrow{\phi_{L/E}} & \mathrm{Gal}(L/E)^{\mathrm{ab}} \\ \downarrow{\scriptstyle \mathrm{Nm}_{E/K}} & & \downarrow \\ K^\times & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K)^{\mathrm{ab}} \end{array} \qquad \begin{array}{ccc} E^\times & \xrightarrow{\phi_{L/E}} & \mathrm{Gal}(L/E)^{\mathrm{ab}} \\ \uparrow & & \uparrow{\scriptstyle \mathrm{Ver}} \\ K^\times & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K)^{\mathrm{ab}} \end{array}$$

The unmarked vertical arrows are induced by the inclusions $\mathrm{Gal}(L/E) \subset \mathrm{Gal}(L/K)$ and $K \subset E$.

PROOF. To be added (the second is not really needed). □

3.3 Let $L \supset E \supset K$ be local fields with both L and E Galois over K. Then the following diagram commutes:

$$\begin{array}{ccc} K^\times & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K)^{\mathrm{ab}} \\ & {\scriptstyle \phi_{E/K}} \searrow & \downarrow \\ & & \mathrm{Gal}(E/K)^{\mathrm{ab}} \end{array}$$

The unmarked vertical arrow is induced by the surjection $\sigma \mapsto \sigma|E : \mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(E/K)$.

PROOF. This follows directly from the definition of the local Artin map, using (33).[3] □

In particular, if $L \supset E \supset K$ is a tower of finite abelian extensions of K, then

$$\theta_{L/K}(a)|E = \phi_{E/K}(a) \text{ for all } a \in K^\times, \text{ and so we can define } \varphi_K : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

to be the homomorphism such that, for every finite abelian extension L/K, $\phi_K(a)|L = \varphi_{L/K}(a)$.

THEOREM 3.4 *For every local field K, there exists a homomorphism (local Artin map)*

$$\theta_K : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

with the following properties:

(a) *for every prime element π of K, $\phi_K(\pi)|K^{\mathrm{un}} = \mathrm{Frob}_K$;*

(b) *for every finite abelian extension L of K, $\mathrm{Nm}_{L/K}(L^\times)$ is contained in the kernel of*

$$a \mapsto \phi_K(a)|L, \text{ and } \phi_K \text{ induces an isomorphism}$$

$$\phi_{L/K} : K^\times / \mathrm{Nm}_{L/K}(L^\times) \to \mathrm{Gal}(L/K).$$

PROOF. Everything is obvious from the above, except (a), which follows from the fact that, for an unramified extension L of K, $\varphi_{L/K}$ agrees with that defined in §1, and so we can apply Proposition 1.9. □

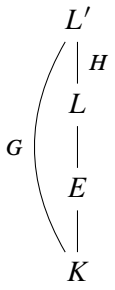
For those who have read §3 of Chapter I, this completes the proof of the main theorems of local class field theory — they can now skip to Chapter V if they wish. Others will need to continue to the end of the chapter.

THEOREM 3.5 (NORM LIMITATION THEOREM) *Let L be a finite extension of K, and let E be the largest abelian extension of K contained in L; then*

$$\mathrm{Nm}_{L/K}(L^\times) = \mathrm{Nm}_{E/K}(E^\times).$$

PROOF. Because of the transitivity of the norm map, $\mathrm{Nm}_{L/K}(L^\times)$ is a subgroup of $\mathrm{Nm}_{E/K}(E^\times)$. If L/K is Galois, then $\mathrm{Gal}(E/K) = \mathrm{Gal}(L/K)^{\mathrm{ab}}$, and so Theorem 3.1 shows that both norm groups have index $[E\colon K]$ in $K^\times$. This implies that they are equal.

In the general case, we let L' be a finite Galois extension of K containing L. Let $G = \mathrm{Gal}(L'/K)$ and $H = \mathrm{Gal}(L'/L)$. Thus:



[3]Herve´ Jacquet has pointed out that this doesn't appear to be correct, but that the statement can be proved using Proposition 3.6. I don't know whether it can be proved without using 3.6.

Then E is the largest subfield of L' that is abelian over K and contained in L. Therefore, the subgroup of G fixing it is $G'\cdot H$, where G' is the derived group of G. Let $a \in \mathrm{Nm}(E^\times)$. We have to show that $a \in \mathrm{Nm}(L^\times)$. Consider the commutative diagram

$$\begin{array}{ccc} L^\times & \xrightarrow{\phi_{L'/L}} & H/H' \\ \downarrow{\scriptstyle \mathrm{Nm}} & & \downarrow \\ K^\times & \xrightarrow{\phi_{L'/K}} & G/G' \\ \| & & \downarrow \\ K^\times & \xrightarrow{\phi_{E/K}} & G/G'H. \end{array}$$

The element $\phi_{L'/K}(a)$ of G/G' maps to 1 in $G/G'H$. As $\phi_{L'/L}$ is surjective, we see from the diagram that there exists a $b \in L^\times$ such $\phi_{L'/K}(a) = \phi_{L'/K}(\mathrm{Nm}(b))$, and hence $a/\mathrm{Nm}(b) \in \mathrm{Nm}(L'^\times)$, say, $a/\mathrm{Nm}(b) = \mathrm{Nm}(c)$. Now

$$a = \mathrm{Nm}_{L/K}(b\cdot \mathrm{Nm}_{L'/L}(c)) \in \mathrm{Nm}_{L/K}(L^\times). \qquad \square$$

Theorem 3.5 shows that there is no hope of classifying nonabelian extensions of a local field in terms of the norm groups.

Alternative description of the local Artin map

Let L/K be a finite abelian extension with Galois group G, and let $u_{L/K} \in H^2(G, L^\times)$ be the fundamental class. The local Artin map $\varphi_{L/K}$ is the inverse to the isomorphism

$$x \mapsto x \cup u_{L/K} : H_T^{-2}(G,\mathbb{Z}) \to H_T^0(G, L^\times).$$

This definition is difficult to work with because cup-products involving both homology and cohomology groups have no very convenient description. Instead, we re-interprete the map purely in terms of cohomology groups. Consider the cup-product pairing

$$H^0(G,L^\times)\times H^2(G,\mathbb{Z}) \longrightarrow H^2(G,L^\times) \xrightarrow{\text{inv}_{L/K}} \mathbb{Q}/\mathbb{Z}.$$

Given an element $a \in H^0(G,L^\times) = K^\times$ and a class $c \in H^2(G,\mathbb{Z})$ represented by a cocycle $f: G\times G \to \mathbb{Z}$, the cup-product class $a\cup c$ is represented by the cocycle $(\sigma,\tau)\mapsto a^{f(\sigma,\tau)}$. Recall also that we have an isomorphism

$$\text{Hom}(G,\mathbb{Q}/\mathbb{Z}) = H^1(G,\mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta} H^2(G,\mathbb{Z}).$$

PROPOSITION 3.6 *For every $\chi \in \text{Hom}cts(G,\mathbb{Q}/\mathbb{Z})$ and $a \in K^\times$,*

$$(\phi_{L/K}(a)) = \text{inv}_K(a\cup\delta\chi).$$

PROOF. See Serre 1962, "Annexe" to Chapter XI, and Serre 1967a, p. 140. □

Using this, we can get another proof of Proposition 3.4.

LEMMA 3.7 *If L/K is unramified, $\varphi_{L/K}$ sends $a \in K^\times$ to $Frob^{\text{ord}_K(a)}$.* PROOF. Recall that inv_K is defined to be the composite

$$H^2(G,L^\times) \xrightarrow{\text{ord}} H^2(G,\mathbb{Z}) \xleftarrow{\delta} \text{Hom}(G,\mathbb{Q}/\mathbb{Z}) \xrightarrow{\chi\mapsto\chi(\sigma)} \mathbb{Q}/\mathbb{Z}.$$

Because of the functoriality of cup-products

$$\text{ord}(a\cup\delta\chi) = \text{ord}(a)\cup\delta\chi, \quad a\in K^\times, \quad \chi\in\text{Hom}(G,\mathbb{Q}/\mathbb{Z})$$

where, on the left ord denotes the map on H^2 induced by $\text{ord}_L: L^\times \twoheadrightarrow \mathbb{Z}$, and on the right it is the map itself. Let $a \in H^0(G,L^\times) = K^\times$, and let $m = \text{ord}_L(a)$. For every

$$\in \text{Hom}(G,\mathbb{Q}/\mathbb{Z}), \text{ in the above diagram,}$$

$$a\cup\delta\chi \mapsto \text{ord}(a)\cup\delta\chi \mapsto m\chi \mapsto \chi(\sigma^m), \quad \sigma = \text{Frob},$$

i.e., $\text{inv}_K(a\cup\delta\chi) = \chi(\sigma^m)$. On combining this with the formula in (3.6) we find that

$$(\phi(\alpha)) = \chi(\sigma^{\text{ord}(\alpha)})$$

for all $\chi\in\text{Hom}(G,\mathbb{Q}/\mathbb{Z})$, and so $\phi(\alpha) = \sigma^{\text{ord}(\alpha)}$. □

For every character of G, we get a character $a\mapsto \text{inv}_K(a\cup\delta\chi)$ of $K^\times$. By duality we get a map $K^\times \to G$. Proposition 3.6 shows that this map is $\phi_{L/K}: K^\times \to \text{Gal}(L/K)$.

4 The Hilbert symbol

Since the subgroups of finite index in $K^\times$ intersect in $\{1\}$, the existence theorem implies that the norm groups intersect in 1. The following key result is the starting point in our proof of the existence theorem.

PROPOSITION 4.1 *Let K be a local field containing a primitive nth root of 1. Any element of $K^\times$ that is a norm from every cyclic extension of K of degree dividing n is an nth power.*

This will be a consequence of the theory of the Hilbert symbol.

A VERY SPECIAL CASE

We explain in this subsection how to obtain the proposition in the special case $K = \mathbb{Q}_p$, $n = 2$, by using only elementary results from Serre 1970, Chapter III.

For $a, b \in \mathbb{Q}_p^\times$, define

$$(a,b)_p = \begin{cases} 1 & \text{if } z^2 = ax^2 + by^2 \text{ has a nontrivial solution in } \mathbb{Q}_p \\ -1 & \text{otherwise.} \end{cases}$$

Clearly, $(a,b)_p$ depends only a and b modulo squares, and so this is a pairing

$$a, b \mapsto (a,b)_p : \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \times \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \to \{\pm 1\}.$$

Serre shows (ibid. 1.1, 1.2) that this pairing is bi-multiplicative

$$(aa', b)_p = (a,b)_p(a',b)_p, \quad (a, bb')_p = (a,b)_p(a,b')_p,$$

symmetric (which in this case is the same as skew-symmetric)

$$(b,a)_p = (a,b)_p^{-1} = (a,b)_p,$$

and nondegenerate (i.e., the left and right kernels are trivial).

Let a be an element of $\mathbb{Q}_p^\times$ that is not a square. Then

$$\begin{aligned} b \text{ is a norm from } \mathbb{Q}_p[\sqrt{a}] &\iff b = z^2 - ax^2 \text{ has a solution in } \mathbb{Q}_p \\ &\iff z^2 = ax^2 + by^2 \text{ has a nontrivial solution in } \mathbb{Q}_p \\ &\iff (a,b)_p = 1. \end{aligned}$$

Thus,

$$b \text{ is a norm from } \mathbb{Q}_p[\sqrt{a}] \text{ for all } a \implies (a,b)_p = 1 \text{ for all } a \implies b \in \mathbb{Q}_p^{\times 2},$$

by the nondegeneracy of the pairing. This proves the proposition in this case.

ASIDE 4.2 The map $a, b \mapsto (a,b)_p$ is called the **Hilbert symbol.** It is defined also for $\mathbb{R}$, and Serre proves **(Hilbert product formula)**

$$\prod_{p \le \infty} (a,b)_p = 1. \tag{34}$$

The general case

In this subsection, $\mathrm{Hom}(G, \mathbb{Z}/n\mathbb{Z})$ denotes the group of *continuous* homomorphisms $G \to \mathbb{Z}/n\mathbb{Z}$.

STEP 1. REVIEW. Recall that for every cyclic group $\bar{G}$ and $\bar{G}$ -module M, there are isomorphisms

$$H_T^r(\bar{G}, M) \to H_T^{r+2}(\bar{G}, M),$$

which become canonical once one chooses a generator σ of $\bar{G}$. More precisely, let $n = (\bar{G} : 1)$ and let be the isomorphism $\bar{G} \to \mathbb{Z}/n\mathbb{Z}$ sending σ to 1 mod n. From the cohomology sequence of

$$0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0,$$

we obtain a boundary map $\delta\colon H^1(\bar{G}, \mathbb{Z}/n\mathbb{Z}) \to H^2(\bar{G}, \mathbb{Z})$. The isomorphism

$$H_T^r(\bar{G}, M) \to H_T^{r+2}(\bar{G}, M)$$

is $b \mapsto \delta\chi \cup b$.

Now let K be a field (not necessarily local), and let L/K cyclic extension with Galois group $\bar{G}$ (of order n). When $r = 0$ and $M = L^\times$, the isomorphism becomes

$$b \mapsto \delta\chi \cup b : K^\times/\operatorname{Nm} L^\times \to H^2(\bar{G}, L^\times).$$

For $\chi \in \operatorname{Hom}(\bar{G}, \mathbb{Z}/n\mathbb{Z})$ and $b \in K^\times$, define

$$(\chi, b)' = \delta\chi \cup b \in H^2(\bar{G}, L^\times).$$

The above discussion shows that, if is an isomorphism $\bar{G} \to \mathbb{Z}/n\mathbb{Z}$, then

$$\overline{(\chi, b)' = 0 \iff b \text{ is a norm from } L^\times.}$$

STEP 2. Let K be a field (not necessarily local). If K has characteristic $p \neq 0$, then we require n to be relatively prime to p. Let K^{al} be a separable algebraic closure of K (thus, simply an algebraic closure if K is perfect), and let $G = \operatorname{Gal}(K^{\mathrm{al}}/K)$. Let μ_n be the group of nth roots of 1 in K^{al}, regarded as a G-module. Under our assumption on n, μ_n is a cyclic group of order n.

From the cohomology sequence of

$$0 \longrightarrow \mu_n \longrightarrow K^{\mathrm{al}\times} \xrightarrow{x \mapsto x^n} K^{\mathrm{al}\times} \longrightarrow 0$$

and Hilbert's theorem 90 (II, 1.22) we find that

$$\delta : K^\times/K^{\times n} \xrightarrow{\simeq} H^1(G, \mu_n), \qquad H^2(G, \mu_n) \xrightarrow{\simeq} H^2(G, K^{\mathrm{al}\times})_n.$$

Here $H^2(G, K^{\mathrm{al}\times})_n$ denotes the group of elements in $H^2(G, K^{\mathrm{al}\times})$ killed by n.

Consider the cup-product pairing

$$\begin{array}{ccccc} H^1(G, \mathbb{Z}/n\mathbb{Z}) & \times & H^1(G, \mu_n) & \to & H^2(G, \mu_n) \\ \wr & & \wr & & \wr \\ \operatorname{Hom}(G, \mathbb{Z}/n\mathbb{Z}) & & K^\times/K^{\times n} & & H^2(G, K^{\mathrm{al}\times})_n. \end{array}$$

For $\chi \in \operatorname{Hom}(G, \mathbb{Z}/n\mathbb{Z})$ and $b \in K^\times/K^{\times n}$, we write (χ, b) for the image of the pair under the above pairing: $(\chi, b) = \chi \cup \delta b$ (as an element of $H^2(G, K^{\mathrm{al}\times})$).

Let $\chi \in \operatorname{Hom}(G, \mathbb{Z}/n\mathbb{Z})$ and (for simplicity) assume that has order n. Let L be the subfield of K^{al} fixed by $\operatorname{Ker}(\chi)$. Thus L is a cyclic extension of K of degree n, and induces an isomorphism of its Galois group $\bar{G}$ with $\mathbb{Z}/n\mathbb{Z}$. Let $b \in K^\times$, and let

$$(\chi, b)' = \delta\chi \cup b \in H^2(\bar{G}, L^\times),$$

as in Step 1. Then

$$\operatorname{Inf}((\chi, b)') = (\chi, b).$$

Since the inflation map $H^2(\bar{G}, L_\chi) \to H^2(G, K^{\mathrm{al}\times})$ is injective (see II, 1.36), we deduce that

$$(\chi, b) = 0 \iff b \text{ is a norm from } L_\chi^\times.$$

STEP 3. Now assume that K is a local field, so that we have a canonical isomorphism

$$\operatorname{inv}_K : H^2(G, K^{\mathrm{al}\times}) \to \mathbb{Q}/\mathbb{Z}.$$

For $\chi \in \operatorname{Hom}(G, \mathbb{Z}/n\mathbb{Z}) \simeq H^1(G, \mathbb{Z}/n\mathbb{Z})$ and $b \in K^\times/K^{\times n} \simeq H^1(G, \mu_n)$, we now define

$$(\chi, b) = \operatorname{inv}_K(\chi \cup \delta b) \in \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

Thus, we have a canonical pairing

$$, b \mapsto (\chi, b)\colon H^1(G, \mathbb{Z}/n\mathbb{Z}) \times H^1(G, \mu_n) \to H^2(G, \mu_n) \simeq \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

PROPOSITION 4.3 *The left kernel of this pairing is zero.* PROOF. Let $\chi \in \mathrm{Hom}(G, \mathbb{Z}/n\mathbb{Z})$; we have to show that if $(\chi, b) = 0$ for all $b \in K^\times/K^{\times n}$, then $\chi = 0$.

Recall that the composite of the local Artin map $\phi_K\colon K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ with

$$\mapsto \tau|L\colon \mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathrm{Gal}(L/K)$$

is surjective for every finite extension L of K contained in K^{ab}. This implies that the image of ϕ_K is dense in $\mathrm{Gal}(K^{\mathrm{ab}}/K)$. Recall (3.6) that, for $b \in K^\times$,

$$(\chi, b \bmod K^{\times n}) = \chi(\phi_K(b)).$$

Because is continuous, if it is zero on $\phi_K(K^\times)$, then it is zero on the whole of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$.□

STEP 4. Now assume that K contains a primitive nth root of 1. Thus, $\mu_n \approx \mathbb{Z}/n\mathbb{Z}$ as a Gmodule (the isomorphism depends on the choice of a primitive nth root of 1). In particular, $\mu_n \otimes \mu_n \approx \mu_n$, and so $H^2(G, \mu_n \otimes \mu_n) \approx H^2(G, \mu_n)$ (noncanonically). There is a *canonical* isomorphism

$$H^2(G, \mu_n) \otimes \mu_n \xrightarrow{\simeq} H^2(G, \mu_n \otimes \mu_n),$$

which can be defined as $x, y \mapsto x \cup y$. On combining this with the isomorphism $H^2(G, \mu_n) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ given by the invariant map, we obtain an isomorphism

$$H^2(G, \mu_n \otimes \mu_n) \simeq \mu_n.$$

Thus, we have a cup-product pairing

$$\begin{array}{ccccc} H^1(G, \mu_n) & \times & H^1(G, \mu_n) & \to & H^2(G, \mu_n \otimes \mu_n) \\ \wr & & \wr & & \wr \\ K^\times/K^{\times n} & & K^\times/K^{\times n} & & \mu_n. \end{array}$$

For $a, b \in K^\times$, their image in μ_n under this pairing is denoted (a, b). The pairing is called the **Hilbert symbol**.

THEOREM 4.4 *The Hilbert symbol has the following properties.*

(a) *It is bi-multiplicative, i.e.,*

$$(aa', b) = (a, b)(a', b), \quad (a, bb') = (a, b)(a, b').$$

(b) *It is skew-symmetric, i.e.,*

$$(b, a) = (a, b)^{-1}.$$

(c) *It is nondegenerate, i.e.,*

$$(a, b) = 1 \text{ for all } b \in K^\times/K^{\times n} \implies a \in K^{\times n},$$

$$(a, b) = 1 \text{ for all } a \in K^\times/K^{\times n} \implies b \in K^{\times n}.$$

(d) $(a, b) = 1$ *if and only if* b *is a norm from* $K[\sqrt[n]{a}]$. PROOF. Statements (a) and (b) are immediate from the definition of the Hilbert symbol in terms of cup-products.

We next prove (c). Choose an nth root of 1, and use it to define isomorphisms $\mathbb{Z}/n\mathbb{Z} \to \mu_n$ and $\mu_n \to \mu_n \otimes \mu_n$. The diagram defined by these maps,

$$\begin{array}{ccccccc} H^1(G,\mu_n) & \times & H^1(G,\mu_n) & \to & H^2(G,\mu_n\otimes\mu_n) & \simeq & H^2(G,\mu_n)\otimes\mu_n \\ \uparrow & & \| & & \uparrow & & \\ H^1(G,\mathbb{Z}/n\mathbb{Z}) & \times & H^1(G,\mu_n) & \to & H^2(G,\mu_n), & & \end{array}$$

commutes. By Proposition 4.3, the left kernel of the lower pairing is zero. Hence, the left kernel of the upper pairing is also zero, which, by skew-symmetry, implies that the right kernel is zero.

Finally, we prove (d). Assume (for simplicity), that $K[\sqrt[n]{a}]$ has degree n over K. Choose a primitive nth root ζ of 1. Then $K[\sqrt[n]{a}]$ is cyclic of degree n over K, and its Galois group is generated by the map σ sending $\sqrt[n]{a}$ to $\zeta\sqrt[n]{a}$. With this choice of ζ, $a \in K^\times/K^{\times n}$ corresponds to the element of $\chi_a \in \operatorname{Hom}(G,\mathbb{Z}/n\mathbb{Z})$ sending σ to 1 mod $n\mathbb{Z}$. As $K[\sqrt[n]{a}] = L_{\chi_a}$, (d) follows from the boxed formula above. □

PROOF (OF PROPOSITION 4.1) We can deduce Proposition 4.1 from Theorem 4.4 by the same argument as in the case $K = \mathbb{Q}_p$, $n = 2$, namely, if b is a norm from $K[\sqrt[n]{a}]$ for all a, then $(a,b) = 1$ for all a (by 4.4d), and hence $b \in K^{\times n}$ (by 4.4c). □

REMARK 4.5 The Hilbert symbol is related to the local Artin map by the formula

$$'_K(b)(a^{\frac{1}{n}}) = (a,b)a^{\frac{1}{n}}.$$

Note that Galois theory tells us that, for every $\tau \in \operatorname{Gal}(K[a^{\frac{1}{n}}]/K)$, $\tau a^{\frac{1}{n}} = \zeta a^{\frac{1}{n}}$ for some nth root of one ζ (remember, we are assuming that K contains the nth roots of 1), and so the point of the formula is that roots of 1 are the same. The proof of the formula is an exercise in cup-products, starting from Proposition 3.6.(a)

REMARK 4.6 The existence theorem will show that φ_K defines an isomorphism $K^\times/K^{\times n} \to \operatorname{Gal}(L/K)$, where L/K is the largest abelian extension of K of exponent n (without the existence theorem we know only that the map is surjective). Clearly, $\operatorname{Hom}(G,\mathbb{Z}/n\mathbb{Z}) = \operatorname{Hom}(\operatorname{Gal}(L/K),\mathbb{Z}/n\mathbb{Z})$, which is the dual of $\operatorname{Gal}(L/K)$. Thus, $K^\times/K^{\times n}$ and $\operatorname{Hom}(G,\mathbb{Z}/n\mathbb{Z})$ have the same order. This shows that the pairing in Step 2,

$$H^1(G,\mathbb{Z}/n\mathbb{Z}) \times H^1(G,\mu_n) \to H^2(G,\mu_n) \simeq \tfrac{1}{n}\mathbb{Z}/\mathbb{Z}$$

is nondegenerate. More generally, for every finite G-module M, the cup-product pairing

$$H^r(G,M) \times H^{2-r}(G,\check{M}) \to H^2(G,\mu_n) \simeq \frac{1}{n}\mathbb{Z}/\mathbb{Z}$$

is nondegenerate — here $\check{M} = \operatorname{Hom}(M,\mu_n)$. This duality theorem was proved by Poitou and Tate in the early 1950s, and was a starting point for the theorems in my book "Arithmetic Duality Theorems". Note that it implies that $H^2(G,\mu_n\otimes\mu_n) \simeq (\mu_n)_G$.

REMARK 4.7 The Hilbert symbol has an interpretation in terms of central simple algebras (see the next chapter). For $a,b \in K^\times$ and ζ a primitive nth root of 1, define $A(a,b;\zeta)$ to be the K-algebra with generators i and j satisfying the relations $i^n = a$, $j^n = b$, and $ij = \zeta ji$. Then, $(a,b)_v$ is the class in $\operatorname{Br}(K)_n$ represented by $A(a,b;\zeta)$. Note that for $n = 2$, we recover the quaternion algebra $H(a,b)$.

REMARK 4.8 The Hilbert symbol

$$(\ ,\ ): K^\times/K^{\times n} \times K^\times/K^{\times n} \to \mu_n$$

is defined also for $K = \mathbb{R}$ and $n = 2$. Moreover, the product formula (34) holds for all number fields and all n (see V, 5.4 below).

5 The Existence Theorem

Let K be a local field. Recall that a subgroup N of $K^\times$ is a **norm group** if there is a finite abelian extension L/K such that $\mathrm{Nm}_{L/K}(L^\times) = N$. Because $K^\times/N \xrightarrow{\sim} \mathrm{Gal}(L/K)$, such a group N is of finite index in $K^\times$ and hence open (I, 1.3).

THEOREM 5.1 (EXISTENCE THEOREM) *Every open subgroup of finite index in $K^\times$ is a norm group.*

In this draft, I prove this only for K of characteristic zero. Then subgroups of finite index are open, and we can use the theory of the Hilbert symbol.

REMARK 5.2 Before starting the proof of Theorem 5.1, we should consider the abstract situation: Let Z be an infinite abelian group, and let $\mathcal{N}$ be a family of subgroups of finite index; what do we need to know in order to prove that $\mathcal{N}$ contains all subgroups of Z of finite index? Clearly, a start is to know,

(a) if I contains an element of $\mathcal{N}$, then I is in $\mathcal{N}$;

(b) if N_1 and N_2 are in $\mathcal{N}$, then $N_1 \cap N_2$ contains an element of $\mathcal{N}$ (and hence is in $\mathcal{N}$).

We know that the family of norm subgroups of $K^\times$ has these properties (Corollary 1.2), but so also, for example, does the set of subgroups of $\mathbb{Z}$ containing $5\mathbb{Z}$. Clearly, we need to know more. Let D be the intersection of all the groups in $\mathcal{N}$. If every subgroup I of finite index in Z contains an element of $\mathcal{N}$, then it contains D. Conversely, if D is divisible, i.e., $D = nD$ for all integers n, then D is contained in every subgroup of finite index (a subgroup of Z of index n contains nZ, which contains $nD = D$). Therefore, we need that D be divisible, but even t his isn't sufficient. For example, let $Z = \mathbb{Z}$ and $\mathcal{N} = \{p^n\mathbb{Z} \mid n \in \mathbb{N}\}$. Then $D = \bigcap p^n\mathbb{Z} = 0$ is divisible, but not every subgroup of finite index in $\mathbb{Z}$ contains an element of $\mathcal{N}$. [Probably I should include a complete list of "axioms" that a family $\mathcal{N}$ should satisfy in order to contain all open subgroups of finite index — see Serre 1962, XI.5, or Artin and Tate 1961, Chapter 14. This may be useful when we come to the global existence theorem.]

Proof of Theorem 5.1

STEP 1. *For all finite extensions L/K, the norm map $L^\times \to K^\times$ has closed image and compact kernel.* PROOF. Since the image has finite index, it is open (see I, 1.3), and hence closed. The kernel is closed, and the equality

$$\mathrm{ord}_L(\mathrm{Nm}(a)) = [L\colon K]\,\mathrm{ord}_L(a) = f \cdot \mathrm{ord}_K(a),$$

shows that it contained in U_K, which is compact. □

Let $D_K = \bigcap \mathrm{Nm}_{L/K}(L^\times)$, where L runs over the finite extensions of K (or only the finite abelian extensions — after Theorem 3.5, it is the same).

STEP 2. *For any finite extension K'/K, $\mathrm{Nm}_{K'/K} D_{K'} = D_K$.*

PROOF. Let $a \in D_K$, and consider the sets

$$\mathrm{Nm}_{L/K'} L^\times \cap \mathrm{Nm}^{-1}_{K'/K}(a)$$

for L/K' finite. They are compact and nonempty, and any two contain a third. Therefore their intersection is nonempty (pointset topology). An element in the intersection lies in $D_{K'}$ and has norm a. □

STEP 3. *The group D_K is divisible.*

PROOF. Let $n > 1$ be an integer — we have to show that $nD_K = D_K$. Let $a \in D_K$. For each finite extension L of K containing a primitive nth root of 1, consider the set

$$E(L) = \{b \in K^\times \mid b^n = a, \quad b \in \mathrm{Nm}_{L/K} L^\times\}.$$

It is nonempty: $a = \mathrm{Nm}_{L/K} a'$ for some $a' \in D_L$; according to Proposition 4.1, $a' = c^n$ for some $c \in L$, and

$$\mathrm{Nm}_{L/K}(c)^n = \mathrm{Nm}_{L/K}(a') = a;$$

def
$\in E(L) \cap E(L')$ therefore $b \overset{\text{def}}{=} \mathrm{Nm}_{L/K}(c) \in E(L)$. Moreover, $E(L \cdot L') \subset E(L) \cap E(L')$. Since each set is finite, their intersection is nonempty. An element in their intersection lies in D_K and has nth power a. □

STEP 4. $D_K = \{1\}$. [Actually, we don't use this here.]

PROOF. Choose a prime element of K. Let $V_{m,n} = U^{(m)} \times \pi^{n\mathbb{Z}}$. Then $V_{m,n}$ is an (open) subgroup of finite index in $K^\times$, and therefore contains D_K. Now $D_K \subset \bigcap_{m,n} V_{m,n} = \{1\}$. □

STEP 5. *Every subgroup I of finite index in $K^\times$ that contains U_K is a norm subgroup.*

PROOF. Since $\mathrm{ord}_K\colon K^\times \to \mathbb{Z}$ is surjective with kernel U_K, the subgroups I in question are the subgroups of $K^\times$ of the form $\mathrm{ord}_K^{-1}(n\mathbb{Z})$, $n \geq 1$. Let K_n be the unramified extension of K of degree n. Then $\mathrm{Nm}_{K_n/K}(K_n^\times)$ is a subgroup of $K^\times$ containing U_K (see 1.2) with image $n\mathbb{Z}$ in $\mathbb{Z}$. The statement follows. □

We now prove the theorem. Let $\mathcal{N}$ be the set of norm groups in $K^\times$, so that $D_K = \bigcap_{N\in\mathcal{N}} N$. Let I be a subgroup of $K^\times$ of finite index. Because D_K is divisible, $I \supset D_K$, and so $I \supset \bigcap_{N\in\mathcal{N}} N \supset \bigcap_{N\in\mathcal{N}}(N \cap U_K)$. Therefore the sets $(N \cap U_K) \smallsetminus I$ have empty intersection. As they are compact some finite subfamily has empty intersection, i.e., for some finite subset $\mathcal{S}$ of $\mathcal{N}$, $I \supset \bigcap_{N\in\mathcal{S}}(N \cap U_K)$. As any two of the sets $N \cap U_K$ contains a third, this implies that $I \supset N \cap U_K$ for some N.

Fix a norm group N such that $N \cap U_K \subset I$. I claim that I contains

$$N \cap (U_K \cdot (N \cap I)).$$

Indeed, every element of the intersection is of the form ab, $a \in U_K$, $b \in N \cap I$, $ab \in N$. The last two statements imply that $a \in N$. Hence $a \in N \cap U_K \subset I$, and so $ab \in I$.

Now $N \cap I$ is of finite index in $K^\times$ because both N and I are and $K^\times/N \cap I$ injects into $(K^\times/N)\times(K^\times/I)$. Hence $U_K\cdot(N \cap I)$ is a subgroup of finite index in $K^\times$ containing U_K, and so is a norm group (Step 5). Now $N \cap (U_K \cdot (N \cap I))$, being the intersection of two norm groups, contains a norm group. Therefore, I contains a norm group, which implies that it is a norm group.

NOTES It follows from Krasner's lemma (ANT, 7.60) that every finite abelian extension of local fields arises by completing a finite abelian extension of global fields. In the 1930s Hasse and F.K. Schmidt[4] were able to deduce the main theorems of local class field theory from those of global class field theory.

From the modern perspective, this seems a strange way to do things. In the 1940s, in his algebraic approach to class field theory Chevalley developed local class field theory directly, and used it in the construction of global class field theory. F. K. Schmidt also showed that local class field theory can be constructed independently of global class field theory.

At that time, there was no good description of the local Artin map, and nor was there an explicit way of constructing the maximal abelian extension of a local field (except for $\mathbb{Q}_p$ of course).

In 1958 Dwork gave an explicit description of the local Artin map, which is reproduced in Serre 1962, but it was not very pleasant.

In 1965 Lubin and Tate introduced the Lubin-Tate formal group laws, and gave an explicit construction of K^{ab} and an explicit description of the local Artin map. However, they made use of the existence of the local Artin map (our Theorem I, 1.1) in their proofs.

In the early 1980s Lubin, Gold, and Rosen independently gave "elementary" proofs that $K^{\mathrm{ab}} = K_\pi \cdot K^{\mathrm{un}}$. In his book (Iwasawa 1986), Iwasawa develops the whole of local class field theory from the Lubin-Tate perspective, and also gives explicit formulas (due to de Shalit and Wiles) for the Hilbert symbols etc..

Other noncohomological approaches can be found in Hazewinkel 1975, Neukirch 1986, and Fesenko and Vostokov 1993. The disadvantage of the noncohomological approaches is, naturally, that they provide no information about the cohomology groups of local fields, which have important applications to other topics, for example elliptic curves.

For an explicit description of the local Artin map in the case of tame extensions, see Newton, Rachel, Explicit local reciprocity for tame extensions. Math. Proc. Cambridge Philos. Soc. 152 (2012), no. 3, 425–454.

In this chapter, I have largely followed Serre 1962 and Serre 1967a.

---

[4]H. Hasse, Die Normenresttheorie relative-Abelscher Zahlko¨rper als Klassenko¨rper im Kleinen, J. fu¨r Mathematik (Crelle) 162 (1930), 145–154.

F. K. Schmidt, Zur Klassenko¨rpertheorie im Kleinen, ibid. 155–168.

3. BRAUER GROUPS

J. S. Milne, Class Field Theory (v4.03)

In this chapter, I define the Brauer group of a field, and show that it provides a concrete interpretation of the cohomology group $H^2(K^{\mathrm{al}}/K)$. Besides clarifying the class field theory, Brauer groups have many applications, for example, to the representation theory of finite groups and to the classification of semisimple algebraic groups over nonalgebraically closed fields.

Throughout the chapter, k will be a field, and all vector spaces over k will be finitedimensional. A k-**algebra** is a ring A containing k in its centre and finite dimensional as a k-vector space. We *do not* assume A to be commutative; for example, A could be the ring $M_n(k)$ of $n \times n$ matrices over k. A k-**subalgebra** of a k-algebra is a subring containing k. A homomorphism $\varphi\colon A \to B$ of k-algebras is a homomorphism of rings with the property that $\varphi(a) = a$ for all $a \in k$. The **opposite** A^{opp} of a k-algebra A is the algebra with the same underlying set and addition, but with multiplication $\cdot$ defined by $\alpha \cdot \beta = \beta\alpha$. Let $e_1, \dots, e_n$ be a basis for A as a k-vector space. Then

$$e_i e_j = \sum_l a_{ij}^l e_l$$

for some $a_{ij}^l \in k$, called the **structure constants** of A relative to the basis $(e_i)_i$. Once a basis has been chosen, the algebra A is uniquely determined by its structure constants.

1 Simple Algebras; Semisimple Modules

Semisimple modules

In this section, A is a k-algebra.

By an A-**module**, we mean a finitely generated left A-module V. In particular, this means that $1v = v$ for all $v \in V$. Such a V is also finite-dimensional when considered as a k-vector space, and so to give an A-module is the same as to give a (finite-dimensional) vector space over k together with a homomorphism of k-algebras $A \to \mathrm{End}_k(V)$, i.e., a **representation** of A on V. The module is said to be **faithful** if this homomorphism is injective, i.e., if $ax = 0$ for all $x \in V$ implies $a = 0$.

An A-module V is **simple** if it is nonzero and contains no proper A-submodule except 0, and it is **semisimple** if it is isomorphic to a direct sum of simple A-modules. It is **in- decomposable** if it can not be written as a direct sum of two nonzero A-modules. Thus a simple module is semisimple, and an indecomposable module is semisimple if and only if it is simple. [1]

Example 1.1. Let $V = k^2$, and let $A = k[\alpha]$ for some $\alpha \in M_2(k)$. The A-submodules of V are the k-subspaces stable under α.

If $\alpha = \left(\begin{smallmatrix} a & 1 \\ 0 & a \end{smallmatrix}\right)$, then $k\binom{1}{0}$ is an A-submodule of V. In fact, it is the only nontrivial submodule, so V is indecomposable but not semisimple.

If $\alpha = \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ with $a \neq b$, the only lines stable under α are $L_1 = k\binom{1}{0}$ and $L_2 = k\binom{0}{1}$. Since $V = L_1 \oplus L_2$ as an A-module, it is semisimple.

If $\alpha = \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$, then V again decomposes as the direct sum of two lines, but the decomposition is no longer unique.

Finally, if $A = M_2(k)$, then V is a simple A-module. For every nonzero $v \in V$, we have $V = M_2(k) \cdot v$.

THEOREM 1.2 *Every A-module V admits a filtration*

$$V = V_0 \supset \cdots \supset V_r = 0$$

whose quotients V_i/V_{i+1} are simple A-modules. If

$$V = W_0 \supset \cdots \supset W_s = 0$$

is a second such filtration, then $r = s$ and there is a permutation σ of $\{0, \dots, r-1\}$ such that $V_i/V_{i+1} \approx W_{\sigma(i)}/W_{\sigma(i)+1}$ for all i.

PROOF. If V is simple, then $V \supset 0$ is such a filtration. Otherwise, V contains a submodule W, $V \neq W \neq 0$, and we can apply the same argument to V/W and to W. This procedure terminates after finitely many steps because V is a finite dimensional k-vector space.

The uniqueness statement can be proved exactly as in the Jordan-Ho¨lder theorem (GT 6.2). □

COROLLARY 1.3 *Suppose that*

$$\begin{aligned} V &\approx V_1 \oplus \cdots \oplus V_r \\ &\approx W_1 \oplus \cdots \oplus W_s \end{aligned}$$

with all the A-modules V_i and W_j simple. Then $r = s$ and there is a permutation σ of $\{1, \dots, r\}$ such that $V_i \approx W_{\sigma(i)}$ for all i.

PROOF. The decompositions define filtrations of the A-module with quotients $\{V_1, \dots, V_r\}$ and $\{W_1, \dots, W_s\}$. □

PROPOSITION 1.4 *Let V be an A-module. If V is a sum of simple submodules (not nec- essarily direct), say $V = \sum_{i \in I} S_i$, then for any submodule W of V, there is a subset J of I such that*

$$V = W \oplus \bigoplus_{i \in J} S_i.$$

[1]Some authors use "irreducible" and "completely reducible" for "simple" and "semisimple" respectively so, for them "irreducible" implies "completely reducible". PROOF. Let J be maximal among the subsets of I such that the sum $S_J = \sum_{j \in J} S_j$ is direct and $W \cap S_J = 0$. I claim that $W + S_J = V$ (hence V is the direct sum of W and the S_j with $j \in J$). To prove this, it suffices to show that every S_i is contained in $W + S_J$. Because S_i is simple, $S_i \cap (W + S_J)$ equals 0 or S_i. In the first case, $W \cap (S_i + S_J) = 0$, because otherwise there exist vectors $w \in W$, $s_i \in S_i$, $s_J \in S_J$, such that $w = s_i + s_J \neq 0$; then $s_i = w - s_J \neq 0$, contradicting $S_i \cap (W + S_J) = 0$. Therefore the second case holds, and $S_i \subset W + S_J$. □

COROLLARY 1.5 *The following conditions on an A-module V are equivalent:*

(a) *V is semisimple;*

(b) *V is a sum of simple submodules;*

(c) *every submodule of V has a complement.*

PROOF. Obviously, (a) implies (b), and the proposition shows that (b) implies (c). Assume (c). If V is simple, then it is semisimple. Otherwise it contains a nonzero proper submodule W, which has a complement W', i.e., $V = W \oplus W'$. If W and W' are simple, then V is semisimple. Otherwise, we can continue the argument, which terminates in a finite number of steps because V has finite dimension as a k-vector space. □

COROLLARY 1.6 *Sums, submodules, and quotient modules of semisimple modules are semisimple.*

PROOF. Each is a sum of simple modules: for sums this follows from (1.5); for quotients it follows from (1.4); for submodules it follows from the fact that every submodule has a complement and therefore is also a quotient. □

Every semisimple A-module V can be written as a direct sum

$$V \simeq m_1S_1 \oplus \cdots \oplus m_rS_r \tag{35}$$

with each S_i simple and no two isomorphic. An A-module is said to be **isotypic** (of type the isomorphism class of S) if it isomorphic to a direct sum of copies of a simple module S. The decomposition (35) shows that every semisimple module V is a direct sum of isotypic modules of distinct types, called the **isotypic components** of V . The isotypic component of V corresponding to a simple module S is the sum of all simple submodules of V isomorphic to S. From this description, we see that a homomorphism $V \to V'$ of semisimple Amodules maps each isotypic component of V into the isotypic component of V' of the same type.

PROPOSITION 1.7 *Let V be a semisimple A-module. A submodule of V is stable under all endomorphisms of V if and only if it is a sum of isotypic components of V .*

PROOF. Every endomorphism of V preserves its isotypic components, which proves the sufficiency. For the necessity, let W be a submodule of V stable under all endomorphisms of V , and let S be a simple submodule of W . If S' is a submodule of V isomorphic to S, then the endomorphism

$$V \xrightarrow{\text{project}} S \xrightarrow{\approx} S' \hookrightarrow V$$

of V maps W into W , and so $S' \subset W$. Therefore W contains the isotypic component of V of type the isomorphism class of S. □ 1.8 Let ${}_AA$ denote A regarded as a left A-module. Right multiplication $x \mapsto xa$ on ${}_AA$ by an element a of A is an A-linear endomorphism of ${}_AA$. Moreover, every A-linear map $\varphi\colon {}_AA \to {}_AA$ is of this form with $a = \varphi(1)$. Thus

$$\varphi \mapsto \varphi(1)\colon \operatorname{End}_A({}_AA) \xrightarrow{\simeq} A \qquad \text{(as } k\text{-vector spaces)}.$$

Let φ_a be the map $x \mapsto xa$. Then

$$(\varphi_a \circ \varphi_b)(1) \overset{\text{def}}{=} \varphi_a(\varphi_b(1)) = \varphi_a(b) = ba = \varphi_{ba}(1),$$

and so

$$\operatorname{End}_A({}_AA) \simeq A^{\text{opp}} \quad \text{(as } k\text{-algebras)}.$$

More generally, if V is a free A-module of rank n, then the choice of a basis for V determines an isomorphism

$$\operatorname{End}_A(V) \to M_n(A^{\text{opp}}).$$

A k-algebra A is said to be **semisimple** if every A-module is semisimple. As every Amodule is a quotient of a direct sum of copies of ${}_AA$, it suffices to check that the A-module ${}_AA$ is semisimple.

PROPOSITION 1.9 *Let A be a semisimple k-algebra. The isotypic components of the A- module ${}_AA$ are the minimal two-sided ideals of A. Every two-sided ideal of A is a direct sum of minimal two-sided ideals.*

PROOF. The two-sided ideals of A are the submodules of ${}_AA$ stable under right multiplication by the elements of A, i.e., by the endomorphisms of ${}_AA$ (1.8), and so they are the sums of isotypic components of ${}_AA$ (1.7). In particular, the minimal two-sided ideals are exactly the isotypic components of ${}_AA$. The second statement is obvious from the above discussion. □

Simple k-algebras

A k-algebra A is said to be **simple** if it contains no proper two-sided ideals other than 0. We shall make frequent use of the following observation:

The kernel of a homomorphism $f: A \to B$ of k-algebras is an ideal in A not containing 1; therefore, if A is simple, then f is injective.

EXAMPLE 1.10 A k-algebra A is said to be a **division algebra** if every nonzero element a of A has an inverse, i.e., there exists a b such that $ab = 1 = ba$. Thus a division algebra satisfies all the axioms to be a field except commutativity (and for this reason is sometimes called a **skew field**). Clearly, a division algebra has no nonzero proper ideals, left, right, or two-sided, and so is simple.

Much of linear algebra does not require that the field be commutative. For example, the usual arguments show that a finitely generated module V over a division algebra D has a basis, and that all bases have the same number n of elements—n is called the dimension of V . In particular, all finitely generated D-modules are free.

EXAMPLE 1.11 Let D be a division algebra over k, and consider the matrix algebra $M_n(D)$. For $A, B \in M_n(D)$, the jth column $(AB)_j$ of AB is AB_j , where B_j is the jth column of B. Therefore, given a matrix B,

$$B_j = 0 \Rightarrow (AB)_j = 0$$
$$B_j \neq 0 \Rightarrow (AB)_j \text{ arbitrary.}$$

It follows that the sets of the form $L(I)$, where I is a subset of $\{1, 2, \dots, n\}$ and $L(I)$ is the set of matrices whose j th columns are zero for $j \notin I$, are left ideals in $M_n(D)$.[2] Moreover, each set $L(\{j\})$ is a minimal ideal in $M_n(k)$. For example, when $n = 4$,

$$L(\{1,3\}) = \left\{ \begin{pmatrix} * & 0 & * & 0 \\ * & 0 & * & 0 \\ * & 0 & * & 0 \\ * & 0 & * & 0 \end{pmatrix} \right\} \text{ and } L(\{3\}) = \left\{ \begin{pmatrix} 0 & 0 & * & 0 \\ 0 & 0 & * & 0 \\ 0 & 0 & * & 0 \\ 0 & 0 & * & 0 \end{pmatrix} \right\}$$

are, respectively, a left ideal and a minimal left ideal. Similar statements hold for the right ideals. It follows that every nonzero two-sided ideal in $M_n(D)$ is the whole ring, and so $M_n(D)$ is a simple k-algebra.

EXAMPLE 1.12 For $a, b \in k^\times$, let $H(a, b)$ be the k-algebra with basis $1, i, j, ij$ (as a k-vector space) and with the multiplication determined by

$$i^2 = a, \quad j^2 = b, \quad ij = -ji.$$

Then $H(a, b)$ is a k-algebra, called a **quaternion algebra** over k. For example, if $k = \mathbb{R}$, then $H(-1, -1)$ is the usual quaternion algebra. One can show (see Exercise 5.7) that $H(a, b)$ is either a division algebra or it is isomorphic to $M_2(k)$. In particular, it is simple.

Centralizers

Let A be a k-subalgebra of a k-algebra B. The **centralizer** of A in B is

$$C_B(A) = \{b \in B \mid ba = ab \text{ for all } a \in A\}.$$

It is again a k-subalgebra of B.

EXAMPLE 1.13 In the following examples, the centralizers are taken in $M_n(k)$.

(a) Let A be the set of scalar matrices in $M_n(k)$, i.e., $A = kI_n$. Clearly $C(A) = M_n(k)$.

(b) Let $A = M_n(k)$. Then $C(A)$ is the centre of $M_n(k)$, which we now compute. Let e_{ij} be the matrix with 1 in the (i, j)th position and zeros elsewhere, so that

$$e_{ij}e_{lm} = \begin{cases} e_{im} & \text{if } j = l \\ 0 & \text{if } j \neq l. \end{cases}$$

Let $\alpha = (a_{ij}) \in M_n(k)$. Then $\alpha = \sum_{i,j} a_{ij}e_{ij}$, and so $\alpha e_{lm} = \sum_i a_{il}e_{im}$ and $e_{lm}\alpha = \sum_j a_{mj}e_{lj}$. If α is in the centre of $M_n(k)$, then $\alpha e_{lm} = e_{lm}\alpha$, and so $a_{il} = 0$ for $i \neq l$, $a_{mj} = 0$ for $j \neq m$, and $a_{ll} = a_{mm}$. It follows that the centre of $M_n(k)$ is k (identified with the set of scalar matrices).

(c) Let A be the set of diagonal matrices in $M_n(k)$. In this case, $C(A) = A$.

---

[2]Not all left ideals in $M_n(D)$ are of the form $L(I)$ — for example, imposing a linear relation on the columns defines a left ideal in $M_n(D)$.

Notice that in all three cases, $C(C(A)) = A$.

THEOREM 1.14 (DOUBLE CENTRALIZER THEOREM) *Let A be a k-algebra, and let V be a faithful semisimple A-module. Then $C(C(A)) = A$ (centralizers taken in $\mathrm{End}_k(V)$).*

PROOF. Let $D = C(A)$ and $B = C(D)$. Clearly $A \subset B$, and the reverse inclusion follows from the next lemma when we take $v_1, \dots, v_n$ to generate V as a k-vector space. □

LEMMA 1.15 *For any $v_1, \dots, v_n \in V$ and $b \in B$, there exists an $a \in A$ such that*

$$av_1 = bv_1, \quad av_2 = bv_2, \quad \dots, \quad av_n = bv_n.$$

PROOF. We first prove this for $n = 1$. Note that Av_1 is an A-submodule of V, and so (see 1.5) there exists an A-submodule W of V such that $V = Av_1 \oplus W$. Let $\pi\colon V \to V$ be the map $(av_1, w) \mapsto (av_1, 0)$ (projection onto Av_1). It is A-linear, hence lies in D, and has the property that $\pi(v) = v$ if and only if $v \in Av_1$. Now

$$\pi(bv_1) = b(\pi v_1) = bv_1,$$

and so $bv_1 \in Av_1$, as required.

We now prove the general case. Let W be the direct sum of n copies of V with A acting diagonally, i.e.,

$$a(v_1, \dots, v_n) = (av_1, \dots, av_n), \quad a \in A, \quad v_i \in V.$$

Then W is again a semisimple A-module (1.6). The centralizer of A in $\mathrm{End}_k(W)$ consists of the matrices $(\gamma_{ij})_{1\le i,j\le n}$, $\gamma_{ij} \in \mathrm{End}_k(V)$, such that $(\gamma_{ij}\alpha) = (\alpha\gamma_{ij})$ for all $\alpha \in A$, i.e., such that $\gamma_{ij} \in D$. In other words, the centralizer of A in $\mathrm{End}_k(W)$ is $M_n(D)$. An argument as in Example 1.13(b), using the matrices $e_{ij}(\delta)$ with δ in the ijth position and zeros elsewhere, shows that the centralizer of $M_n(D)$ in $\mathrm{End}_k(W)$ consists of the diagonal matrices

$$\begin{pmatrix} \beta & 0 & \cdots & 0 \\ 0 & \beta & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \beta \end{pmatrix}$$

with $\beta \in B$. We now apply the case $n = 1$ of the lemma to A, W, b, and the vector $(v_1, \dots, v_n)$ to complete the proof. □

Classification of simple k-algebras

LEMMA 1.16 (SCHUR'S LEMMA) *The endomorphism algebra of a simple A-module is a division algebra.*

PROOF. Let be an A-linear map $S \to S$. Then $\mathrm{Ker}(\gamma)$ is an A-submodule of S, and so it is either S or 0. In the first case, is zero, and in the second it is an isomorphism, i.e., it has an inverse that is also A-linear. □

THEOREM 1.17 *Every simple k-algebra A is isomorphic to $M_n(D)$ for some n and some division k-algebra D.* PROOF. Choose a simple A-module S, for example, any minimal left ideal of A. Then A acts faithfully on S, because the kernel of $A \to \mathrm{End}_k(S)$ will be a two-sided ideal of A not containing 1, and hence is 0.

Let D be the centralizer of A in the k-algebra $\mathrm{End}_k(S)$ of k-linear maps $S \to S$. According to the double centralizer theorem (1.14), the centralizer of D in $\mathrm{End}_k(S)$ is A, i.e., $A = \mathrm{End}_D(S)$. Schur's lemma implies that D is a division algebra. Therefore, S is a free D-module (1.10), say, $S \approx D^n$, and so $\mathrm{End}_D(S) \approx M_n(D^{\mathrm{opp}})$ (see 1.8). □

Modules over simple k-algebras

Let A be an k-algebra. The submodules of ${}_AA$ are the left ideals in A, and the simple submodules of ${}_AA$ are the minimal left ideals.

PROPOSITION 1.18 *Simple k-algebras are semisimple.*

PROOF. Let A be a simple k-algebra. It suffices to show that the A-module ${}_AA$ is semisimple.After Theorem 1.17, we may assume that $A = M_n(D)$ for some division algebra D. We saw in 1.11 that the sets $L(i)$ are minimal left ideals in $M_n(D)$, and that $M_n(D) = L(1) \oplus \cdots \oplus L(n)$ as an $M_n(D)$-module. This shows that ${}_AA$ is semisimple. □

THEOREM 1.19 *Let A be a semisimple k-algebra. The following conditions on A are equivalent:*

(a) *A is simple;*

(b) *the A-module ${}_AA$ is isotypic;*

(c) *any two simple A-modules are isomorphic.*

PROOF. The equivalence of (a) and (b) follows from Proposition 1.9, and (c) obviously implies (b). Finally (b) implies (c) because, if ${}_AA$ is isotypic, so also is a direct sum of copies of ${}_AA$, and every A-module is a quotient of such a direct sum. □

COROLLARY 1.20 *Let A be a simple k-algebra. Any two minimal left ideals of A are isomorphic as left A-modules, and A is a direct sum of its minimal left ideals.*

PROOF. Minimal left ideals are simple A-modules, and so the first statement follows from (c) of the theorem. The second statement was proved in the proof of 1.18. □

COROLLARY 1.21 *Let A be a simple k-algebra, and let S be a simple A-module. Every A-module is isomorphic to a direct sum of copies of S. Any two A-modules having the same dimension over k are isomorphic.*

PROOF. As A is semisimple, the first assertion follows from (c) of the theorem, and the second assertion follows from the first. □

COROLLARY 1.22 *The integer n in Theorem 1.17 is uniquely determined by A, and D is uniquely determined up to isomorphism.*

PROOF. If $A \approx M_n(D)$, then $D^{\mathrm{opp}} \approx \mathrm{End}_A(S)$ for any simple A-module S, and n is the dimension of S as a D-vector space. Since any two simple A-modules are isomorphic (1.19), this implies the statement. □

2 Definition of the Brauer Group

Tensor products of algebras

Let A and B be k-algebras, and let $A \otimes_k B$ be the tensor product of A and B as k-vector spaces. There is a unique k-bilinear multiplication on $A \otimes_k B$ such that

$$(a \otimes b)(a' \otimes b') = aa' \otimes bb', \quad a, a' \in A, \quad b, b' \in B.$$

When we identify k with $k \cdot (1 \otimes 1) \subset A \otimes_k B$, then $A \otimes_k B$ becomes a k-algebra. If $(e_i)_i$ and $(f_j)_j$ are bases of A and B as k-vector spaces, then $(e_i \otimes f_j)_{i,j}$ is a basis for $A \otimes_k B$, and the structure constants for $A \otimes_k B$ can be obtained from those of A and B by an obvious formula. We shall use that tensor products are commutative in the sense that, for any two k-algebras A and B, the map $a \otimes b \mapsto b \otimes a$ extends to an isomorphism of k-algebras

$$A \otimes_k B \to B \otimes_k A,$$

and that they are associative in the sense that, for any three k-algebras A, B, and C, the map $a \otimes (b \otimes c) \mapsto (a \otimes b) \otimes c$ extends to an isomorphism of k-algebras

$$A \otimes_k (B \otimes_k C) \to (A \otimes_k B) \otimes_k C.$$

EXAMPLE 2.1 For every k-algebra A,

$$A \otimes_k M_n(k) \simeq M_n(A).$$

To see this, note that a ring B containing a subring R in its centre is isomorphic to $M_n(R)$ if and only if it admits a basis $(e_{ij})_{1 \le i,j \le n}$ as a left R-module such that

$$e_{ij} e_{lm} = \begin{cases} e_{im} & \text{if } j = l \\ 0 & \text{if } j \neq l. \end{cases}$$

If (e_{ij}) is the standard basis for $M_n(k)$, then $(1 \otimes e_{ij})$ is an A-basis for $A \otimes M_n(k)$ with the correct property.

More generally,

$$A \otimes_k M_n(A') \simeq M_n(A \otimes_k A') \tag{36}$$

for any k-algebras A and A'.

EXAMPLE 2.2 For any m, n, $M_m(k) \otimes M_n(k) \simeq M_{mn}(k)$. To see this, note that according to the preceding example, $M_m(k) \otimes_k M_n(k) \simeq M_m(M_n(k))$, and an $m \times m$-matrix whose entries are $n \times n$-matrices is an $mn \times mn$-matrix (delete the inner parentheses). Alternatively, let (e_{ij}) and $(f_{i'j'})$ be standard bases for $M_m(k)$ and $M_n(k)$, and check that $(e_{ij} \otimes f_{i'j'})$ has the correct multiplication properties.

Centralizers in tensor products

The next proposition shows that the centralizer of a tensor product of subalgebras is the tensor product of their centralizers.

PROPOSITION 2.3 *Let A and A' be k-algebras, with subalgebras B and B', and let $C(B)$ and $C(B')$ be the centralizers of B and B' in A and A' respectively. Then the centralizer of $B \otimes_k B'$ in $A \otimes_k A'$ is $C(B) \otimes_k C(B')$, i.e.,*

$$C_{A \otimes_k A'}(B \otimes_k B') = C_A(B) \otimes_k C_{A'}(B').$$

PROOF. Certainly $C(B \otimes_k B') \supset C(B) \otimes_k C(B')$.

Let $(f_i)_i$ be a basis for A' as a k-vector space. Then $(1 \otimes f_i)_i$ is a basis for $A \otimes_k A'$ as an A-module, and so an element α of $A \otimes_k A'$ can be written uniquely in the form $\alpha = \sum_i \alpha_i \otimes f_i$,

$\alpha_i \in A$. Let $\beta \in B$. Then α commutes with $\beta \otimes 1$ if and only if $\beta\alpha_i = \overline{\alpha}_i\beta$ for all i. Therefore, the centralizer of $B \otimes 1$ in $A \otimes A'$ is $C(B) \otimes A'$. Similarly, the centralizer of $1 \otimes B'$ in $C(B) \otimes A'$ is $C(B) \otimes C(B')$.

Certainly, $C(B \otimes B') \subset C(B \otimes 1)$, and so $C(B \otimes B')$ is contained in $C(B) \otimes A'$, and, in fact, is contained in the centralizer of $1 \otimes B'$ in $C(B) \otimes A'$, which is $C(B) \otimes C(B')$. This completes the proof. □

In particular, the centre of the tensor product of two k-algebras is the tensor product of their centres: $Z(A \otimes_k B) = Z(A) \otimes_k Z(B)$.

COROLLARY 2.4 *The centre of a simple k-algebra is a field.*

PROOF. Obviously, the centre of a division algebra is a field, but Wedderburn's theorem (1.17) shows that every simple k-algebra is isomorphic to $M_n(D)$ for some division algebra D. Now $M_n(D) \simeq M_n(k) \otimes_k D$, and so $Z(M_n(D)) \simeq k \otimes_k Z(D) \simeq Z(D)$. □

A k-algebra A is said to be **central** if its centre is k, and a k-algebra that is both central and simple is said to be **central simple.** The corollary shows that every simple k-algebra is central simple over a finite extension of k.

Primordial elements

Before continuing, it will be useful to review a little linear algebra from the second edition of Bourbaki's Algebra.

Let V be a k-vector space, possibly infinite dimensional, and let $(e_i)_{i\in I}$ be a basis for V. Any $v \in V$ can be written uniquely $v = \sum a_i e_i$, and we define

$$J(v) = \{i \in I \mid a_i \neq 0\};$$

it is a finite subset of I, which is empty if and only if $v = 0$.

Let W be a subspace of V. A nonzero element w of W is said to be **primordial** (relative to V and the basis $(e_i)_{i\in I}$) if $J(w)$ is mini mal among the sets $J(w')$ for w' a nonzero element of W and, in the expression $w = \sum a_i e_i$, at least one $a_i = 1$.

PROPOSITION 2.5 *(a) Let w be a nonzero element of W such that $J(w)$ is minimal, and let w' be a second nonzero element of W. Then $J(w') \subset J(w)$ if and only if $w' = cw$ for some nonzero $c \in k$, in which case $J(w') = J(w)$.*

(b) The set of primordial elements of W spans it.

PROOF. (a) If $w' = cw$, $c \neq 0$, then certainly $J(w') = J(w)$. For the converse, let $w = \sum_{i\in J(w)} a_i e_i$ and $w' = \sum_{i\in J(w')} b_i e_i$ be nonzero elements of W with $J(w') \subset J(w)$. Let $j \in J(w')$. Then $J(w - a_j b_j^{-1} w') \subset J(w) \smallsetminus \{j\}$, and so $w - a_j b_j^{-1} w' = 0$ by the minimality of $J(w)$.

(b) Let $w = \sum_{i\in J(w)} a_i e_i \in W$. We have to show that w lies in the subspace spanned by primordial elements. We may assume that $w \neq 0$. Among the nonzero elements w' of W with $J(w') \subset J(w)$, there is one for which $J(w')$ has the fewest possible elements. Some scalar multiple w_0 of w' will be primordial, say, $w_0 = \sum_{i\in J(w_0)} b_i e_i$ with $b_j = 1$.

Now $w = a_j w_0 + (w - a_j w_0)$ with $w - a_j w_0 \in W$ and $\big|J(w - a_j w_0)\big| < |J(w)|$. If $w - a_j w_0$ is a k-linear combination of primordial elements, so is w; if not, repeat the process. As $|J(w)|$ is finite, it will terminate in a finite number of steps. □

The results (and proofs) of this section do not require k to be commutative, i.e., k can be a division algebra.

Simplicity of tensor products

PROPOSITION 2.6 *The tensor product of two simple k-algebras, at least one of which is central, is again simple.*

PROOF. After 1.17, we may suppose that one of the algebras is $M_n(D)$, where D is a division algebra with centre k. Let A be the second simple k-algebra. In the next lemma, we show that $A \otimes_k D$ is simple. Therefore, $A \otimes_k D \approx M_m(D')$ with D' a division algebra, and so

$$A \otimes_k M_n(D) \simeq M_n(A \otimes_k D) \approx M_n(M_m(D')) \simeq M_{mn}(D'),$$

which is simple. □

LEMMA 2.7 *Let A be a k-algebra, and let D be a division algebra with centre k. Then any two-sided ideal $\mathfrak{A}$ in $A \otimes D$ is generated as a left D-module by $\mathfrak{a} \overset{\text{def}}{=} \mathfrak{A} \cap (A \otimes 1)$.*

PROOF. We make $A \otimes_k D$ into a left D-module by the rule,

$$\delta(\alpha \otimes \delta') = \alpha \otimes \delta\delta', \quad \alpha \in A, \quad \delta, \delta' \in D.$$

The ideal $\mathfrak{A}$ of $A \otimes_k D$ is, in particular, a D-submodule of $A \otimes_k D$.

Let (e_i) be a basis for A as a k-vector space. Then $(e_i \otimes 1)$ is a basis for $A \otimes_k D$ as a left D-vector space. Let $\alpha \in \mathfrak{A}$ be primordial with respect to this basis, say

$$\alpha = \sum_{i \in J(\alpha)} \delta_i (e_i \otimes 1) = \sum_{i \in J(\alpha)} e_i \otimes \delta_i .$$

For any nonzero $\delta \in D$, $\alpha\delta \in \mathfrak{A}$, and $\alpha\delta = \sum e_i \otimes \delta_i\delta = \sum_{i \in I} (\delta_i\delta)(e_i \otimes 1)$. In particular, $J(\alpha\delta) = J(\alpha)$, and so $\alpha\delta = \delta'\alpha$ for some $\delta' \in D$ (see 2.5a). As some $\delta_i = 1$, this implies that $\delta = \delta'$, and so each δ_i commutes with every $\delta \in D$. Hence δ_i lies in the centre k of D, and $\alpha \in A \otimes 1$. We have shown that every primordial element of $\mathfrak{A}$ is in $A \otimes 1$, which completes the proof because $\mathfrak{A}$ is generated as a D-module by its primordial elements (see 2.5b). □

COROLLARY 2.8 *The tensor product of two central simple k-algebras is again central sim- ple.*

PROOF. Combine Proposition 2.3 with Proposition 2.6. □

Let A be a central simple algebra over k, and let V denote A regarded as a k-vector space. Then left multiplication makes V into a left A-module, and right multiplication makes it into a right A-module, or, what is the same thing, a left A^{opp}-module. These actions identify A and A^{opp} with commuting subalgebras of $\text{End}_k(V)$. From the universality of the tensor product, we obtain a homomorphism

$$a \otimes a' \mapsto (v \mapsto ava') : A \otimes_k A^{\text{opp}} \to \text{End}_k(V).$$

As $A \otimes_k A^{\text{opp}}$ is simple and the kernel of the homomorphism does not contain 1, it is injective. On counting degrees, we find that

$$[A \otimes_k A^{\text{opp}} : k] = [A : k]^2 = (\dim V)^2 = [\text{End}_k(V) : k],$$

and so the homomorphism is an isomorphism. We have proved the following result.

COROLLARY 2.9 *For a central simple k-algebra A,*

$$A \otimes_k A^{\text{opp}} \simeq \text{End}_k(A) \approx M_n(k), \quad n = [A : k].$$

The Noether-Skolem Theorem

THEOREM 2.10 (SKOLEM, NOETHER) *Let $f, g : A \to B$ be homomorphisms from a k- algebra A to a k-algebra B. If A is simple and B is central simple, then there exists an invertible element*

$b \in B$ such that $f(a) = b \cdot g(a) \cdot b^{-1}$ for all $a \in A$, i.e., f and g differ by an inner automorphism of B.

PROOF. If $B = M_n(k) = \mathrm{End}_k(k^n)$, then the homomorphisms define actions of A on k^n—let V_f and V_g denote k^n with the actions defined by f and g. According to (1.21), two A-modules with the same dimension are isomorphic, but an isomorphism $b\colon V_g \to V_f$ is an element of $M_n(k)$ such that $f(a) \cdot b = b \cdot g(a)$ for all $a \in A$.

In the general case, we consider the homomorphisms

$$f \otimes 1, g \otimes 1\colon A \otimes_k B^{\mathrm{opp}} \to B \otimes_k B^{\mathrm{opp}}.$$

Because $B \otimes_k B^{\mathrm{opp}}$ is a matrix algebra over k, the first part of the proof shows that there exists a $b \in B \otimes_k B^{\mathrm{opp}}$ such that

$$(f \otimes 1)(a \otimes b') = b \cdot (g \otimes 1)(a \otimes b') \cdot b^{-1}$$

for all $a \in A$, $b' \in B^{\mathrm{opp}}$. On taking $a = 1$ in this equation, we find that $(1 \otimes b') = b \cdot (1 \otimes b') \cdot b^{-1}$ for all $b' \in B^{\mathrm{opp}}$. Therefore (see 2.3), $b \in C_{B \otimes_k B^{\mathrm{opp}}}(k \otimes B^{\mathrm{opp}}) = B \otimes_k k$, i.e., $b = b_0 \otimes 1$ with $b_0 \in B$. On taking $b' = 1$ in the equation, we find that

$$f(a) \otimes 1 = (b_0 \cdot g(a) \cdot b_0^{-1}) \otimes 1$$

for all $a \in A$, and so b_0 is the element sought. □

COROLLARY 2.11 *Let A be a central simple algebra over k, and let B_1 and B_2 be simple k-subalgebras of A. Any isomorphism $f\colon B_1 \to B_2$ is induced by an inner automorphism of A, i.e., there exists an invertible $a \in A$ such that $f(b) = aba^{-1}$ for all $b \in B_1$.*

PROOF. This is the special case of the theorem in which the two maps are $B_1 \xrightarrow{f} B_2 \hookrightarrow A$ and $B_1 \xrightarrow{\mathrm{id}} B_1 \hookrightarrow A$. □

COROLLARY 2.12 *All automorphisms of a central simple k-algebra are inner.*

For example, the automorphism group of $M_n(k)$ is $\mathrm{PGL}_n(k) \stackrel{\mathrm{def}}{=} \mathrm{GL}_n(k)/k^\times I_n$. *Definition of the Brauer group*

Let A and B be central simple algebras over k. We say that A and B are **similar,** $A \sim B$, if $A \otimes_k M_n(k) \approx B \otimes_k M_m(k)$ for some m and n. This is an equivalence relation: it is obviously reflexive and symmetric, and 2.2 implies that it is transitive. Define $\mathrm{Br}(k)$ to be the set of similarity classes of central simple algebras over k, and write $[A]$ for the similarity class of A. For classes $[A]$ and $[B]$, define

$$[A][B] = [A \otimes_k B].$$

This is well-defined (i.e., if $A \sim A'$ and $B \sim B'$, then $A \otimes_k B \sim A' \otimes_k B'$), and the associativity and commutativity of tensor products show that it is associative and commutative. For every n, $[M_n(k)]$ is an identity element, and because $A \otimes_k A^{\mathrm{opp}} \approx M_n(k)$ (see 2.9) $[A]$ has $[A^{\mathrm{opp}}]$ as inverse. Therefore $\mathrm{Br}(k)$ is an abelian group, called the **Brauer group** of k.

REMARK 2.13 (a) Wedderburn's theorem (1.17, 1.22) shows that every central simple algebra over k is isomorphic to $M_n(D)$ for some central division algebra D and that D is uniquely determined by A (even by the similarity class of A) up to isomorphism. Therefore, each similarity class is represented by a central division algebra, and two central division algebras represent the same similarity class if and only if they are isomorphic.

(b) We should verify[3] that the similarity classes form a set, and not merely a class. For each $n > 0$, consider the families $(a_{ij}^l)_{1 \le i,j,l \le n}$, $a_{ij}^l \in k$, that are structure constants for central division al-

gebras over k. Clearly, these families form a set, each family defines a central division algebra over k, and these division algebras contain a set of representatives for the Brauer group of k.

EXAMPLE 2.14(a) If k is algebraically closed, then $\mathrm{Br}(k) = 0$. To prove this, we have to show that any central division algebra D over k equals k. Let $\alpha \in D$, and let $k[\alpha]$ be the subalgebra of D generated by k and α. Then $k[\alpha]$ is a commutative field of finite degree over k (because it is an integral domain of finite degree over k). Hence $k[\alpha] = k$, and $\alpha \in k$. Since α was arbitrary, this shows that $D = k$.

(b) Frobenius showed that Hamilton's quaternion algebra is the only central division algebra over $\mathbb{R}$. Therefore, the Brauer group of $\mathbb{R}$ is cyclic of order 2, equal to $\{[\mathbb{R}], [\mathbb{H}]\}$ (see §4 below).

(c) Wedderburn showed that all finite division algebras are commutative. Therefore, the Brauer group of a finite field is zero (Theorem 4.1 below).

(d) Hasse showed that the Brauer group of a nonarchimedean local field is canonically isomorphic to $\mathbb{Q}/\mathbb{Z}$ (see p. 138 below).

(e) Albert, Brauer, Hasse, and Noether showed that, for a number field K, there is an exact sequence

$$0 \to \mathrm{Br}(K) \to \bigoplus\nolimits_v \mathrm{Br}(K_v) \xrightarrow{\Sigma} \mathbb{Q}/\mathbb{Z} \to 0.$$

[3]I once heard Brauer, who normally had a gentle manner, deliver a tirade against "modern" mathematicians who ignored the distinction between sets and classes. As he pointed out, if you ignore the distinction, then you obtain a contradiction (Russell's paradox), and once you have one contradiction in your system, you can prove anything.

The sum is over all the primes of K (including the infinite primes). This statement is of the same depth as that of the main theorems of class field theory (see Chapters VII and VIII).

Extension of the base field

PROPOSITION 2.15 *Let A be a central simple algebra over k, and let K be a field containing k (not necessarily of finite degree over k). Then $A \otimes_k K$ is a central simple algebra over K.*

PROOF. The same argument as in the proof of Proposition 2.3 shows that the centre of $A \otimes_k K$ is $k \otimes_k K = K$ (the argument does not require K to have finite degree over k). Also, the proof of Lemma 2.7 does not use that D is finite-dimensional over k. Therefore, when A is a division algebra, every two-sided ideal in $A \otimes_k K$ is generated as an A-module by its intersection with K, and therefore is 0 or $A \otimes_k K$. In the general case, $A \approx M_n(D)$, and so

$$\begin{aligned} A \otimes_k K \approx M_n(D) \otimes_k K &\simeq (M_n(k) \otimes_k D) \otimes_k K \\ &\simeq M_n(k) \otimes_k (D \otimes_k K) \\ &\simeq M_n(D \otimes_k K) \\ &\simeq M_n(K) \otimes_K (D \otimes_k K) \end{aligned}$$

which is simple. □

COROLLARY 2.16 *For a central simple algebra A over k, $[A : k]$ is a square.*

PROOF. Clearly $[A : k] = [A \otimes_k k^{\mathrm{al}} : k^{\mathrm{al}}]$, and $A \otimes_k k^{\mathrm{al}} \approx M_n(k^{\mathrm{al}})$ for some n. □

Let L be a field containing k (not necessarily of finite degree). Then

$$M_n(k) \otimes L \simeq M_n(L),$$

and

$$(A \otimes_k L) \otimes_L (A' \otimes_k L) = A \otimes_k (L \otimes_L (A' \otimes_k L)) = (A \otimes_k A') \otimes_k L.$$

Therefore the map $A \mapsto A \otimes_k L$ defines a homomorphism

$$\mathrm{Br}(k) \to \mathrm{Br}(L).$$

We denote the kernel of this homomorphism by $\mathrm{Br}(L/k)$ — it consists of the similarity classes represented by central simple k-algebras A such that the L-algebra $A \otimes_k L$ is a matrix algebra.

A central simple algebra A (or its class in $\mathrm{Br}(k)$) is said to be **split** by L, and L is called a **splitting field** for A, if $A \otimes_k L$ is a matrix algebra over L. Thus $\mathrm{Br}(L/k)$ consists of the elements of $\mathrm{Br}(k)$ split by L.

PROPOSITION 2.17 *For every field k, $\mathrm{Br}(k) = \bigcup \mathrm{Br}(K/k)$, where K runs over the finite extensions of k contained in some fixed algebraic closure k^{al} of k.*

PROOF. We have to show that every central simple algebra A over k is split by a finite extension of k. We know that $A \otimes_k k^{\mathrm{al}} \approx M_n(k^{\mathrm{al}})$, i.e., that there exists a basis $(e_{ij})_{1\le i,j\le n}$ for $A \otimes_k k^{\mathrm{al}}$ such that $e_{ij}e_{lm} = \delta_{jl}e_{im}$ for all i, j, l, m. Because $A \otimes_k k^{\mathrm{al}} = \bigcup_{[K:k]<\infty} A \otimes_k K$, the e_{ij} all lie in $A \otimes_k K$ for some K, and it follows that $A \otimes_k K \approx M_n(K)$. □

3 The Brauer Group and Cohomology

For a Galois extension L/k of fields, let $H^2(L/k) = H^2(\mathrm{Gal}(L/k), L^\times)$. We shall show that there is a natural isomorphism $H^2(L/k) \simeq \mathrm{Br}(L/k)$, but first we need to investigate the maximal subfields of a central simple algebra.

Maximal subfields

We need a variant of the double centralizer theorem in which $M_n(k)$ is replaced by a central simple algebra.

THEOREM 3.1 *Let B be a simple k-subalgebra of a central simple k-algebra A. Then the centralizer $C = C(B)$ of B in A is simple, and B is the centralizer of C. Moreover,*

$$[B : k][C : k] = [A : k].$$

PROOF. Let V denote B regarded as a k-vector space. Then B and B^{opp} act on V , by right and left multiplication respectively, and each is the centralizer of the other (see 1.8).

Consider the central simple algebra $A \otimes_k \mathrm{End}_k(V)$. Proposition 2.3 shows that the centralizer of $B \otimes 1$ in this algebra is $C \otimes \mathrm{End}_k(V)$ and that of $1 \otimes B$ is $A \otimes B^{\mathrm{opp}}$. On applying the Noether-Skolem theorem (2.10, 2.11) to the two embeddings $b \mapsto b \otimes 1$ and $b \mapsto 1 \otimes b$ of B into $A \otimes_k \mathrm{End}_k(V)$, we obtain an invertible element u of this k-algebra such that $b \otimes 1 = u(1 \otimes b)u^{-1}$ for all $b \in B$. Clearly then

$$C(B \otimes 1) = u \cdot C(1 \otimes B) \cdot u^{-1}$$

(centralizers in $A \otimes_k \mathrm{End}_k(V)$), which shows that these centralizers are isomorphic. Therefore $C \otimes_k \mathrm{End}_k(V)$ is simple because $A \otimes_k B^{\mathrm{opp}}$ is simple (see 2.6), and this implies that C itself is simple because, for every ideal $\mathfrak{a}$ of C, $\mathfrak{a} \otimes_k \mathrm{End}_k(V)$ is an ideal in $C \otimes_k \mathrm{End}_k(V)$. As $\mathrm{End}_k(V)$ has degree $[B : k]^2$ over k,

$$[C \otimes_k \mathrm{End}(V) : k] = [C : k][B : k]^2,$$

and obviously

$$[A \otimes B^{\mathrm{opp}} : k] = [A : k][B : k].$$

On comparing these equalities, we find that

$$[A : k] = [B : k][C : k].$$

If B' denotes the centralizer of C in A, then $B' \supset B$. But after the above, $[A : k] = [C : k][B' : k]$; so $[B : k] = [B' : k]$ and $B = B'$. □

REMARK 3.2 In the case that $A = \mathrm{End}_k(V)$ for V a k-vector space, Theorem 3.1 follows from Theorem 1.14 because V will be a faithful semisimple B-module. This observation can be used to give an alternative proof of the theorem, because A becomes of this form after a finite extension of the base field (see 2.17).

COROLLARY 3.3 *If in the statement of the theorem, B has centre k, then so also does C, and the canonical homomorphism $B \otimes_k C \to A$ is an isomorphism.* PROOF. The centres of B and C both equal $B \cap C$, and so B central implies C central. Therefore the k-algebra $B \otimes_k C$ is central simple, which implies that $B \otimes_k C \to A$ is injective. It is surjective because the algebras have the same dimension over k. □

COROLLARY 3.4 *Let A be a central simple algebra over k, and let L be a subfield of A containing k. The following are equivalent:*

(a) *L equals its centralizer in A;*

(b) *$[A : k] = [L : k]^2$;*

(c) *L is a maximal commutative k-subalgebra of A.*

PROOF. (a) $\iff$ (b). Because L is commutative, it is contained in its centralizer $C(L)$, but

$$[A : k] = [L : k][C(L) : k],$$

and so $C(L) = L$ if and only if $[A : k] = [L : k]^2$.

(b) $\implies$ (c). Let L' be a maximal commutative subalgebra containing L. Then $L' \subset C(L)$, and so

$$[A{:}\,k] \geq [L{:}\,k][L'{:}\,k] \geq [L{:}\,k]^2.$$

Thus (b) implies that $[L'{:}\,k] = [L{:}\,k]$.

(c) $\implies$ (a). If $L \neq C(L)$, then there exists a $\gamma \in C(L) \smallsetminus L$. Now $L[\gamma]$ is a commutative subalgebra of A, contradicting the maximality of L. □

COROLLARY 3.5 *The maxim al subfields containing k of a central division k-algebra D are exactly those with degree $\sqrt{[D : k]}$ over k.*

PROOF. Any commutative k-subalgebra of D is an integral domain of finite degree over k, and hence is a field. □

COROLLARY 3.6 *Let A be a central simple algebra over k. A field L of finite degree over k splits A if and only if there exists an algebra B similar to A containing L and such that*

$$[B : k] = [L : k]^2. \tag{37}$$

In particular, every subfield L of A of degree $[A{:}\,k]^{1/2}$ over k splits A.

PROOF. Suppose L splits A. Then L also splits A^{opp}, say, $A^{\mathrm{opp}} \otimes_k L = \mathrm{End}_L(V)$. This equality states that $A^{\mathrm{opp}} \otimes_k L$ is the centralizer of L in $\mathrm{End}_k(V)$, and so L is the centralizer of $A^{\mathrm{opp}} \otimes_k L$ in $\mathrm{End}_k(V)$ (see 3.1). Let B be the centralizer of A^{opp} in $\mathrm{End}_k(V)$. I claim that B satisfies the required conditions. Certainly, $B \supset L$, and Corollary 3.3 shows that B is central simple and that $B \otimes_k A^{\mathrm{opp}} \simeq \mathrm{End}_k(V)$. On tensoring both sides with A and using that $A \otimes_k A^{\mathrm{opp}}$ is a matrix algebra, we find that $B \sim A$.

For the converse, it suffices to show th at L splits B. Because L is commutative, $L = L^{\mathrm{opp}} \subset B^{\mathrm{opp}}$, and because $[L : k] = \sqrt{[B : k]}$, L is equal to its centralizer in B^{opp}. Therefore the centralizer of $1 \otimes L$ in $B \otimes_k B^{\mathrm{opp}}$ is $B \otimes_k L$. When we identify $B \otimes_k B^{\mathrm{opp}}$ with $\mathrm{End}_k(B)$ (endomorphisms of B as a k-vector space—see 2.9), the centralizer of L becomes identified with $\mathrm{End}_L(B)$ (endomorphisms as an L-vector space). This completes the proof. □

COROLLARY 3.7 *Let D be a central division algebra of degree n^2 over k, and let L be a field of degree n over k. Then L splits D if and only if L can be embedded in D (i.e., there exists a homomorphism of k-algebras $L \to D$).*

PROOF. If L embeds into D, then the last corollary shows that it splits D. Conversely, if L splits D, then there exists a central simple algebra B over k containing L, similar to D, and of degree $[L : k]^2$. But $B \sim D$ implies $B \approx M_m(D)$ for some m (see Remark 2.13a), and the condition on the degrees implies that $m = 1$. □

PROPOSITION 3.8 *Every central division algebra over k contains a maximal subfield sep- arable over k.*

PROOF. Let D be a central division algebra over k, and let L be a subfield that is maximal among the separable subfields of D. If L is not a maximal subfield of D, then its centralizer D' is a central division algebra over L not equal to L (see 3.1). The next lemma shows that D' contains a separable subfield properly containing L, which contradicts the definition of L. □

LEMMA 3.9 *Every central division algebra over k and not equal to it contains a subfield separable over k and not equal to it.*

PROOF. Let D be a central division algebra over k. Choose a basis $(e_i)_{1 \le i \le n^2}$ for D with $e_1 = 1$, and let $x = \sum_i a_i e_i$ be an element of D. For every integer m, $x^m =$

$$\sum_i P_i(m; a_1, \dots, a_{n^2}) e_i, \text{ where the } P_i \text{ are polynomials in the } a_j\text{'s with coefficients in } k$$

that depend only on the structure constants for D. Therefore, if K is a field containing k and

$$x = \sum a_i (e_i \otimes 1), \quad a_i \in K,$$

is an element of $D \otimes_k K$, then $x^m = \sum_i P_i(m; a_1, \dots a_{n^2}) e_i \otimes 1$ with the same polynomials P_i.

When k is perfect we know the lemma, and so we may assume that k has characteristic $p \neq 0$ and is infinite. Suppose that $k[a]$ is purely inseparable over k for every $a \in D$. Then $a^{p^r} \in k$ for some $r > 0$, and one sees easily that there exists an r that works for every element of D. For this particular r and $i \neq 1$, $P_i(p^r; a_1, \dots, a_{n^2}) = 0$ for all $a_1, \dots, a_{n^2} \in k$, which implies that $P_i(p^r; X_1, \dots, X_{n^2})$ is the zero polynomial (see FT, proof of 5.18). Therefore, $a^{p^r} \in k^{\mathrm{al}}$ for every element a of $D \otimes_k k^{\mathrm{al}}$. But $D \otimes_k k^{\mathrm{al}} \approx M_n(k^{\mathrm{al}})$, and so

$$\mathrm{diag}(1, 0, \dots, 0) = \mathrm{diag}(1, 0, \dots, 0)^{p^r} \in k^{\mathrm{al}},$$

which implies that $n = 1$. □

COROLLARY 3.10 *The Brauer group $\mathrm{Br}(k) = \bigcup \mathrm{Br}(L/k)$, where L/k runs over the finite Galois extensions of k contained in a fixed separable algebraic closure of k.*

PROOF. The proposition shows that every element of $\mathrm{Br}(k)$ is split by a finite separable extension, and therefore by a finite Galois extension. □ *Central simple algebras and 2-cocycles*

Fix a finite Galois extension L of k, and let $G = \mathrm{Gal}(L/k)$. Define $\mathcal{A}(L/k)$ to be the class of central simple algebras A over k containing L and of degree $[A : k] = [L : k]^2$ (hence, L equals its centralizer in A).

Fix an $A \in \mathcal{A}(L/k)$. For every $\sigma \in G$, Corollary 2.11 of the Noether-Skolem theorem shows that there exists an element $e_\sigma \in A$ such that

$$\sigma a = e_\sigma a e_\sigma^{-1} \text{ for all } a \in L. \tag{38}$$

Moreover, e_σ is determined by (38) up to multiplication by an element of $L^\times$, because if f_σ has the same property, then $f_\sigma^{-1} e_\sigma$ centralizes L. Note that (38) can be written as

$$e_\sigma \cdot a = \sigma a \cdot e_\sigma \text{ for all } a \in L, \tag{39}$$

which says that moving e_σ past $a \in L$ replaces it with σa. Clearly $e_\sigma e_\tau$ has the property (38) for $\sigma\tau$, and so

$$e_\sigma e_\tau = \varphi(\sigma, \tau) e_{\sigma\tau} \tag{40}$$

for some $\varphi(\sigma, \tau) \in L^\times$. Note that

$$e_\rho(e_\sigma e_\tau) = e_\rho(\varphi(\sigma,\tau)e_{\sigma\tau}) = \rho\varphi(\sigma,\tau) \cdot \varphi(\rho, \sigma\tau) \cdot e_{\rho\sigma}$$

and

$$(e_\rho e_\sigma)e_\tau = \varphi(\rho,\sigma)e_{\rho\sigma}e_\tau = \varphi(\rho,\sigma)\varphi(\rho\sigma,\tau) \cdot e_{\rho\sigma\tau}.$$

Therefore the associative law implies that φ is a 2-cocycle. It is even a normalized 2-cocycle if we choose $e_1 = 1$. A different choice of e_σ's leads to a cohomologous 2-cocycle, and so we have a well-defined map $A \mapsto \gamma(A)\colon \mathcal{A}(L/k) \to H^2(L/k)$.

THEOREM 3.11 *The map $\gamma\colon \mathcal{A}(L/k) \to H^2(L/k)$ is surjective, and its fibres are the isomorphism classes.*

We first need a lemma.

LEMMA 3.12 *Let $A \in \mathcal{A}(L/k)$, and define e_σ to satisfy (38). Then the set $(e_\sigma)_{\sigma\in G}$ is a basis for A as a left vector space over L.*

PROOF. Note that

$$\dim_L(A) = \frac{\dim_k(A)}{\dim_k(L)} = n,$$

and so it suffices to show that the e_σ are linearly independent. Suppose not, and let $(e_\sigma)_{\sigma\in J}$ be a maximal linearly independent set. If $\tau \notin J$, then

$$e_\tau = \sum a_\sigma e_\sigma$$

for some $a_\sigma \in L$. Let $a \in L$. When we compute $e_\tau a$ in two different ways,

$$e_\tau a = \tau a \cdot e_\tau = \sum_{\sigma\in J} \tau a \cdot a_\sigma e_\sigma,$$

$$e_\tau a = \sum_{\sigma\in J} a_\sigma e_\sigma \cdot a = \sum_{\sigma\in J} a_\sigma \cdot \sigma a \cdot e_\sigma$$

we find that $\tau a \cdot a_\sigma = \sigma a \cdot a_\sigma$ for all $\sigma \in J$. For at least one $\sigma \in J$, $a_\sigma \neq 0$, and then the equation shows that $\tau = \sigma$, contradicting the fact that $\tau \notin J$. Therefore $J = G$. □

Now A is uniquely determined by the following properties: $A \supset L$; $(e_\sigma)_{\sigma\in G}$ is a basis for A as an L-vector space; multiplication in A satisfies the equation (38) and (40).

Let $A' \in \mathcal{A}(L/k)$ and suppose that $\gamma(A) = \gamma(A')$. The condition implies that we can choose bases (e_σ) and (e'_σ) for A and A' satisfying (38) and (40) with the *same* 2-cocycle φ. The map $\sum a_\sigma e_\sigma \mapsto \sum a_\sigma e'_\sigma\colon A \to A'$ is an isomorphism of k-algebras.

Next suppose that A and A' are isomorphic elements of $\mathcal{A}(L/k)$. The Noether-Skolem theorem allows us to choose the isomorphism $f: A \to A'$ so that $f(L) = L$ and $f|L$ is the identity map. If e_σ satisfies condition (40) for A, then $f(e_\sigma)$ satisfies (40) for A'. With the choices (e_σ) and $(f(e_\sigma))$, A and A' define the same cocycle.

These remarks show that the map $A \mapsto \gamma(A)$ defines a injection

$$\mathcal{A}(L/k)/\approx \to H^2(L/k).$$

To show that the map is surjective, we construct an inverse.

Let $\varphi: G \times G \to L^\times$ be a normalized 2-cocycle. Define $A(\varphi)$ to be the L-vector space with basis $(e_\sigma)_{\sigma\in G}$ endowed with the multiplication given by (38) and (40). Then e_1 is an identity element for multiplication, and the cocycle condition (exactly) shows that

$$e_\rho(e_\sigma e_\tau) = (e_\rho e_\sigma)e_\tau.$$

It follows that $A(\varphi)$ is a k-algebra. We identify L with the subfield Le_1 of $A(\varphi)$.

LEMMA 3.13 *The algebra $A(\varphi)$ is central simple over K.*

PROOF. Let $\alpha = \sum a_\sigma e_\sigma$ centralize L, and let $a \in L$. On comparing $a\alpha = \sum aa_\sigma \cdot e_\sigma$ with $\alpha a = \sum a_\sigma(\sigma a) \cdot e_\sigma$, we find that $a_\sigma = 0$ for $\sigma \neq 1$, and so $\alpha = a_1e_1 \in L$. Therefore, the centralizer of L in $A(\varphi)$ is L.

Let α lie in the centre of $A(\varphi)$. Then α centralizes L, and so $\alpha \in L$, say $\alpha = ae_1$, $a \in L$. On comparing $e_\sigma \cdot \alpha = (\sigma a)e_\sigma$ with $\alpha \cdot e_\sigma = ae_\sigma$, we see that $\alpha \in k$. Thus $A(\varphi)$ is central.

Let $\mathfrak{A}$ be a two-sided ideal in $A(\varphi)$; in particular, $\mathfrak{A}$ is an L-subspace of $A(\varphi)$. If $\mathfrak{A}$ contains one element e_σ , then (40) shows that it contains all, and so equals $A(\varphi)$. Suppose $\mathfrak{A} \neq 0$, and let $\alpha = \sum a_\sigma e_\sigma$ be a primordial element of $\mathfrak{A}$, with say $a_{\sigma_0} = 1$. If $a_{\sigma_1} \neq 0, \sigma_1 \neq \sigma_0$, then for every $a \in L$,

$$(\sigma_1 a) \cdot \alpha - \alpha \cdot a = \sum a_\sigma(\sigma_1 a - \sigma a)e_\sigma \in \mathfrak{A}.$$

If a is chosen so that $\sigma_1 a \neq \sigma_0 a$, then this element is nonzero but has fewer nonzero coefficients than α, contradicting its primordality. Therefore, $\alpha = e_{\sigma_0}$, and we have shown that $\mathfrak{A} = A(\varphi)$. □

Let φ and φ' be cohomologous 2-cocycles, say,

$$a(\sigma) \cdot \sigma a(\tau) \cdot \varphi'(\sigma, \tau) = a(\sigma\tau) \cdot \varphi(\sigma, \tau)$$

for some map $a: G \to L^\times$. One checks immediately that the L-linear map $A(\varphi) \to A(\varphi')$ sending e_σ to $a(\sigma)e'_\sigma$ is an isomorphism of k-algebras. Therefore $\varphi \mapsto A(\varphi)$ defines a map $H^2(L/K) \to \mathcal{A}(L/k)/\approx$, which is clearly inverse to $A \mapsto \gamma(A)$. This completes the proof of Theorem 3.11.

The algebras $A(\varphi)$ are called **crossed-product algebra.** Before group cohomology existed, 2-cocycles $\varphi: G \times G \to L^\times$ were called **factor sets** (and sometimes still are).

THEOREM 3.14 *For every finite Galois extension L/k, the map $\varphi \mapsto [A(\varphi)]$ defines an isomorphism of abelian groups $H^2(L/k) \to \mathrm{Br}(L/k)$.*

To show that this map is bijective, it suffices (after Theorem 3.11) to show that the map $A \mapsto [A]: \mathcal{A}(L/k)/\approx \to \mathrm{Br}(L/k)$ is bijective.

If A and A' are similar central simple algebras over k, then (see 2.13) there exists a central division algebra D such that $A \sim D \sim A'$, say, $A \approx M_n(D)$, $A' \approx M_{n'}(D)$. But if $[A : k] = [A' : k]$, then $n = n'$, and so $A \approx A'$. This proves that the map $\mathcal{A}(L/k)/\approx \to \mathrm{Br}(L/k)$ is injective, and 3.6 proves that it is surjective.

LEMMA 3.15 *For any two 2-cocycles φ and φ', $A(\varphi+\varphi') \sim A(\varphi) \otimes_k A(\varphi')$.*

PROOF. The proof is a little messy because we have to recognize $A(\varphi) \otimes_k A(\varphi')$, not as a crossed-product algebra, but as matrix algebra over a crossed-product algebra. I merely sketch the proof.[4]

Set $A = A(\varphi)$, $B = A(\varphi')$, and $C = A(\varphi+\varphi')$. Regard A and B as left L-modules (using left multiplication), and define

$$V = A \otimes_L B.$$

Concretely, V is the largest quotient space of $A \otimes_k B$ such that

$$la \otimes_L b = a \otimes_L lb$$

holds for all $a \in A, b \in B, l \in L$.

The k-vector space V has a unique right $A \otimes_k B$-module structure such that

$$(a' \otimes_L b')(a \otimes_k b) = a'a \otimes_L b'b \text{ , all } a', a \in A \text{ , } b', b \in B,$$

and a unique left C-module structure such that

$$(le''_\sigma)(a \otimes_L b) = le_\sigma a \otimes_L e'_\sigma b \text{ , all } l \in L, \sigma \in G, a \in A, b \in B.$$

Here (e_σ), (e'_σ), and (e''_σ) are the standard bases for $A = A(\varphi)$, $B = A(\varphi')$, and $C = A(\varphi+\varphi')$ respectively.

The two actions commute, and so the right action of $A \otimes_k B$ on V defines a homomorphism of k-algebras

$$f\colon (A \otimes_k B)^{\text{opp}} \to \text{End}_C(V).$$

This homomorphism is injective because $A \otimes_k B$ (and hence its opposite) is simple. Since both $(A \otimes_k B)^{\text{opp}}$ and $\text{End}_C(V)$ have degree n^4 over k, where $n = [L : k]$, f is an isomorphism. As we showed in (1.21), any two modules over a simple ring of the same k-dimension are isomorphic, and it follows that $V \approx C^n$ as a C-module. Hence

$$\text{End}_C(V) \approx \text{End}_C(C^n) = M_n(C^{\text{opp}}),$$

and on composing this isomorphism with f we obtain an isomorphism of k-algebras

$$(A \otimes_k B)^{\text{opp}} \to M_n(C)^{\text{opp}}.$$

The same map can be interpreted as an isomorphism

$$A \otimes_k B \to M_n(C).$$

□

[4]See Blanchard 1972, pp. 94–95, or Farb and Dennis 1993, p. 126–128, for the details.

COROLLARY 3.16 *For every separable algebraic closure k^{al} of k, there is a canonical iso- morphism* $\text{Br}(k) \to H^2(k^{\text{al}}/k)$.

PROOF. For every tower of fields $E \supset L \supset k$ with E and L finite and Galois over k, the diagram

$$\begin{array}{ccc} H^2(L/k) & \xrightarrow{\text{Inf}} & H^2(E/k) \\ \downarrow & & \downarrow \\ \text{Br}(L/k) & \hookrightarrow & \text{Br}(E/k) \end{array}$$

commutes (the vertical maps send φ to $[A(\varphi)]$).[5] Now use that

$$\begin{aligned} \mathrm{Br}(k) &= \bigcup \mathrm{Br}(L/k) \qquad (3.10), \\ H^2(k^{\mathrm{al}}/k) &= \Big\lfloor\ \Big\rfloor H^2(L/k), \end{aligned}$$

where both unions run over the finite Galois extensions L of k contained in k^{al}. □

COROLLARY 3.17 *For every field k, $\mathrm{Br}(k)$ is torsion, and for every finite extension L/k, $\mathrm{Br}(L/k)$ is killed by $[L:k]$.*

PROOF. The same statements are true for the cohomology groups. □

4 The Brauer Groups of Special Fields

The results of the last section allow us to interpret some of the results of Chapter III as statements concerning the Brauer group of a field. In this section, we shall derive the same results independently of Chapter III (but not quite of Chapter II).

Finite fields

Let k be a finite field. We saw in III, 1.4 that, for every finite extension L of k, $H^2(L/k) = 0$, and hence $\mathrm{Br}(k) = 0$. The following is a more direct proof of this fact.

THEOREM 4.1 (WEDDERBURN) *Every finite division algebra is commutative.*

PROOF. Let D be a finite division algebra with centre k, and let $[D:k] = n^2$. Every element of D is contained in a subfield $k[\alpha]$ of D, and hence in a maximal subfield. Every maximal subfield of D has q^n elements. They are therefore isomorphic, and hence conjugate (Noether-Skolem). Therefore, for every maximal subfield L, $D^\times = \bigcup \alpha L^\times \alpha^{-1}$, but a finite group can not equal the union of the conjugates of a proper subgroup (because the union has too few elements), and so $D = L$. □

[5] Should add a proof that the diagram commutes.

The real numbers

Let $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{1, \sigma\}$. Then

$$H^2(\mathbb{C}/\mathbb{R}) \simeq H_T^0(G, \mathbb{C}^\times) = \mathbb{R}^\times / \mathrm{Nm}_G(\mathbb{C}^\times) = \{\pm\},$$

and so $\mathrm{Br}(\mathbb{C}/\mathbb{R})$ is a cyclic group of order 2. The nonzero element of $H^2(\mathbb{C}/\mathbb{R})$ is represented by the 2-cocycle $\varphi\colon G \times G \to \mathbb{C}^\times$,

$$\varphi(\rho,\tau) = \begin{cases} -1 & \text{if } \rho = \sigma = \tau \\ 1 & \text{otherwise} \end{cases}.$$

Let $\mathbb{H}$ be the usual quaternion algebra over $\mathbb{R}$. Then the $\mathbb{C}$-linear map $A(\varphi) \to \mathbb{H}$ sending x_σ to j is an isomorphism of $\mathbb{R}$-algebras. It follows that every central simple algebra over $\mathbb{R}$ is isomorphic either to a matrix algebra over $\mathbb{R}$ or to a matrix algebra over $\mathbb{H}$.

A nonarchimedean local field

Let K be a nonarchimedean local field. In Chapter III, Theorem 2.1, we defined an isomorphism $H^2(K^{\mathrm{al}}/K) \simeq \mathbb{Q}/\mathbb{Z}$, and hence an isomorphism $\mathrm{Br}(K) \simeq \mathbb{Q}/\mathbb{Z}$. In this subsection, we explain how to construct this isomorphism more directly.

Let D be a central division algebra over K, and let $n^2 = [D:K]$. For every subfield L of D containing K, the absolute value $|\cdot|$ has a unique extension to L. Since every element α of D is contained in such a subfield of D, for example, in $K[\alpha]$, the absolute value $|\cdot|$ has a unique

extension to D. It is possible to verify that $|\cdot|$ is a nonarchimedean absolute value on D in the obvious sense, i.e.,

(a) $|\alpha| = 0 \iff \alpha = 0$;

(b) for all $\alpha, \beta \in D$, $|\alpha\beta| = |\alpha||\beta|$;

(c) for all $\alpha, \beta \in D$, $|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\}$.

Let q be the number of elements in the residue field k of K, and define $\mathrm{ord}(\alpha)$ for $\alpha \in D$ by the formula:

$$|\alpha| = (1/q)^{\mathrm{ord}(\alpha)}.$$

Then ord extends the additive valuation ord_K on K (normalized to map $K^\times$ onto $\mathbb{Z}$) to D. For any subfield L of D containing K, $[L : K] \leq n$, and so $\mathrm{ord}(L^\times) \subset n^{-1}\mathbb{Z}$. Hence also $\mathrm{ord}(D^\times) \subset n^{-1}\mathbb{Z}$.

Let

$$\mathcal{O}_D = \{\alpha \in D \mid \mathrm{ord}(\alpha) \geq 0\}$$
$$\mathfrak{P} = \{\alpha \in D \mid \mathrm{ord}(\alpha) > 0\}.$$

Then $\mathcal{O}_D$ is a subring in D, called the **ring of integers.** For every subfield L of D containing K, $\mathcal{O}_D \cap L = \mathcal{O}_L$, and so $\mathcal{O}_D$ consists precisely of the elements of D that are integral over $\mathcal{O}_K$. Moreover $\mathfrak{P}$ is a maximal 2-sided ideal in $\mathcal{O}_D$ (obviously), and the powers of it are the only 2-sided ideals in D (the proof is the same as in the commutative case). Hence $\mathfrak{P}^e = \mathfrak{p}\mathcal{O}_D$ for some e. Then $\mathrm{ord}(D^\times) = e^{-1}\mathbb{Z}$, and therefore $e \leq n$.

Clearly, the elements of $\mathcal{O}_D$ not in $\mathfrak{P}$ are units. Therefore $d \stackrel{\text{def}}{=} \mathcal{O}_D/\mathfrak{P}$ is again a division algebra, and hence a field (4.1). Let f be its degree over k. Write $d = k[a]$. We can lift a to an element α of $\mathcal{O}_D$. Because $[K[\alpha] : K] \leq n$, we have $f \leq n$.

The same argument as in the commutative case shows that $n^2 = ef$, namely, $\mathcal{O}_D$ is a free $\mathcal{O}_K$-module of some rank m. Because $\mathcal{O}_D \otimes_{\mathcal{O}_K} K = D$, $m = n^2$. Moreover, because $\mathcal{O}_D \otimes_{\mathcal{O}_K} k = \mathcal{O}_D/\mathfrak{p}\mathcal{O}_D$, it also is free of dimension of n^2 over k. Now consider the filtration of k-vector spaces

$$\mathcal{O}_D \supset \mathfrak{P} \supset \mathfrak{P}^2 \supset \cdots \supset \mathfrak{P}^e = \mathfrak{p}\mathcal{O}_D.$$

From our definition of f , $\mathcal{O}_D/\mathfrak{P} = d$ has dimension f as a k-vector space, and the successive quotients are one-dimensional vector spaces over d. Hence $\mathcal{O}_D/\mathfrak{p}\mathcal{O}_D$ has dimension ef over k, and so $ef = n^2$.

Because $e \leq n$, $f \leq n$, the equality $ef = n^2$ implies that $e = f = n$. In particular, every central division algebra $\neq K$ is ramified. Again write $d = k[a]$, and lift a to an element $\alpha \in D$. Then $K[\alpha]$ is a field with residue field d, and so $[K[\alpha] : K] \geq [d : k] = n$. Therefore $K[\alpha]$ has degree n over K and is unramified. It is a maximal subfield, and hence splits D. We have shown that every element of $\mathrm{Br}(K)$ is split by an unramified extension, i.e., $\mathrm{Br}(K)$ is equal to its subgroup $\mathrm{Br}(K^{\mathrm{un}}/K)$.

We next define the map

$$\mathrm{inv}_K : \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}.$$

An element of $\mathrm{Br}(K)$ is represented by a central division algebra D over K (unique up to isomorphism). According to what we have just proved, there is a maximal subfield L of D that is unramified over K. Let σ be the Frobenius automorphism of L. According to the Noether-

Skolem theorem, there is an element $\alpha \in D$ such that $\sigma x = \alpha x \alpha^{-1}$ for all $x \in L$. If α' also has this property, then $\alpha' = c\alpha$ for some $c \in L$, and so

$$\operatorname{ord}(\alpha') = \operatorname{ord}(c) + \operatorname{ord}(\alpha) \equiv \operatorname{ord}(\alpha) \mod \mathbb{Z}.$$

We define

$$\operatorname{inv}_K(D) = \operatorname{ord}(\alpha) \mod \mathbb{Z}.$$

It depends only on the isomorphism class of D.

EXAMPLE 4.2 Let L be the unramified extension of K of degree n, and let σ be the Frobenius automorphism of L/K, so that $G \overset{\text{def}}{=} \operatorname{Gal}(L/K) = \{\sigma^i \mid 0 \le i \le n-1\}$. Let φ be the 2-cocycle

$$\varphi(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{if} \quad i+j \le n-1 \\ \pi & \text{if} \quad i+j > n-1, \end{cases}$$

where π is a prime element of K (see the discussion preceding III 1.9). The crossed-product algebra $A(\varphi)$ equals $\bigoplus_{0 \le i \le n-1} Le_i$ with the multiplication determined by

$$e_i \cdot a = \sigma^i a \cdot e_i \text{ all } a \in L,$$

and

$$e_i e_j = \begin{cases} e_{i+j} & \text{if} \quad i+j \le n-1 \\ \pi e_{i+j-n} & \text{if} \quad i+j > n-1, \end{cases}$$

We identify L with a subfield of $A(\varphi)$ by identifying e_0 with 1. Because $e_1 a e_1^{-1} = \sigma a$ for $a \in L$, we can use e_1 to compute the invariant of $A(\varphi)$. According to the above rules, $e_1^n = e_{n-1}e_1 = \pi e_0 = \pi$. Hence

$$\operatorname{inv}_K(A(\varphi)) = \operatorname{ord}(e_1) = \tfrac{1}{n}\operatorname{ord}(e_1^n) = \tfrac{1}{n}\operatorname{ord}(\pi) = \tfrac{1}{n},$$

as expected.

PROPOSITION 4.3 *The map* $\operatorname{inv}_K : \operatorname{Br}(K) \to \mathbb{Q}/\mathbb{Z}$ *just defined is a bijection.*

PROOF. Let L be the unramified extension of K of degree n (contained in a fixed algebraic closure K^{al} of K), and let l/k be the corresponding extension of residue fields. Because the norm maps $l \to k, l^\times \to k^\times$ are surjective, and U_L has a filtration whose quotients are $l^\times$ or l one finds that the norm map $U_L \to U_K$ is surjective (see III, 1.2). Therefore, $H_T^0(G, U_L) = 0$, and (because the cohomology of cyclic groups is periodic) this implies that $H^2(G, \hat{U_L}) = 0$. As $L^\times = U_L \times \pi^{\mathbb{Z}}$ for any prime element π of K,

$$H^2(L/K) = H^2(G, \pi^{\mathbb{Z}}).$$

Consideration of the cohomology sequence of

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

shows that $H^2(G, \pi^{\mathbb{Z}})$ is cyclic of order n and is generated by the class of the cocycle φ considered in the last example (see the discussion preceding III, 1.9). Therefore, $\operatorname{Br}(L/K)$ is cyclic of order n, and it is generated by $[A(\varphi)]$. It now follows that $\operatorname{inv}_K : \operatorname{Br}(K^{\text{un}}/K) \to \mathbb{Q}/\mathbb{Z}$ is an isomorphism, and we saw above that $\operatorname{Br}(K^{\text{un}}/K) = \operatorname{Br}(K^{\text{al}}/K)$. □

REMARK 4.4 (a) The calculation in Example 4.2 shows that the invariant map defined in this chapter agrees with that in the preceding chapter using cohomology. In particular, this shows that the map defined here is a homomorphism.

(b) A calculation as in Example 4.2 shows that $\operatorname{inv}_K(A(\varphi^i) = \frac{i}{n} \bmod \mathbb{Z}$. I claim that if i is relatively prime to n, then $A(\varphi^i)$ is a central division algebra. If not, then $A(\varphi^i) \sim M_r(D)$ for a central division algebra D of degree m^2 some $m < n$, and $\operatorname{inv}_K(A(\varphi^i)) = \operatorname{inv}_K(D) \in \frac{1}{m}\mathbb{Z}/\mathbb{Z}$, which is a contradiction. It follows that each central division algebra over K is isomorphic to exactly one division algebra of the form $A(\varphi^i)$ for some $n \geq 1$ and some i relati vely prime to n. In particular, for a central division algebra D, the order of $[D]$ in $\operatorname{Br}(K)$ is $\sqrt{[D:K]}$.

(c) Let D be a central division algebra of degree n^2 over K. Because the map $\operatorname{Br}(K) \to \operatorname{Br}(L)$ multiplies the invariant by $[L:K]$ (see III, 2.1), D is split by every extension L of K of degree n. Therefore every such L can be embedded into D (by 3.7). In other words, *every* irreducible polynomial in $K[X]$ of degree n has a root in D!

NOTES The results for finite fields, the real numbers, and nonarchmidean local fields are due respectively to Wedderburn, Frobenius, and Hasse. The calculation of the Brauer group of a nonarchimedean local field is essentially the original (pre-cohomological) proof of Hasse.

5 Complements

Semisimple algebras

Recall that a k-algebra A is semisimple if every A-module is semisimple. Simple k-algebras are semisimple (1.18) and Maschke's theorem (GT, 7.4) shows that the group algebra $k[G]$ is semisimple when the order of G is not divisible by the characteristic of k.

EXAMPLE 5.1 Let A be a finite product of simple k-algebras. Every minimal left ideal of a simple factor of A is a simple A-submodule of ${}_AA$. Therefore, ${}_AA$ is a sum of simple A-modules, and so is semisimple. Since every A-module is a quotient of a direct sum of copies of ${}_AA$, this shows that A is semisimple.

Before stating the main result of this section, we recall some elementary module theory.

5.2 Let A be an k-algebra, and consider modules

$$M = M_1 \oplus \cdots \oplus M_n$$
$$N = N_1 \oplus \cdots \oplus N_m.$$

Let α be an A-linear map $M \to N$. For $x_j \in M_j$, let

$$\alpha(0, \dots, 0, x_j, 0, \dots, 0) = (y_1, \dots, y_m).$$

Then $x_j \mapsto y_i$ is an A-linear map $M_j \to N_i$, which we denote α_{ij}. Thus, α defines an $m \times n$ matrix whose ij th coefficient is an A-linear map $M_j \to N_i$. Conversely, every such matrix (α_{ij}) defines an A-linear map $M \to N$, namely,

$$\begin{pmatrix} x_1 \\ \vdots \\ x_j \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1j} & \cdots & \alpha_{1n} \\ \vdots & & \vdots & & \vdots \\ \alpha_{i1} & \cdots & \alpha_{ij} & \cdots & \alpha_{jn} \\ \vdots & & \vdots & & \vdots \\ \alpha_{m1} & \cdots & \alpha_{mj} & \cdots & \alpha_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_j \\ \vdots \\ x_n \end{pmatrix} \overset{\text{def}}{=} \begin{pmatrix} \alpha_{11}(x_1) + \cdots + \alpha_{1n}(x_n) \\ \vdots \\ \alpha_{i1}(x_1) + \cdots + \alpha_{in}(x_n) \\ \vdots \\ \alpha_{m1}(x_1) + \cdots + \alpha_{mn}(x_n) \end{pmatrix}.$$

Thus, we see

$$\operatorname{Hom}_A(M, N) \simeq \big(\operatorname{Hom}_A(M_j, N_i)\big)_{1 \leq j \leq n,\, 1 \leq i \leq m} \qquad (41)$$

(isomorphism of k-vector spaces). When $M = N$, this becomes an isomorphism of $k$algebras. For example, if M is a direct sum of m copies of M_0, then

$$\mathrm{End}_A(M) \simeq M_m(\mathrm{End}_A(M_0)) \tag{42}$$

($m \times m$ matrices with coefficients in the ring $\mathrm{End}_A(M_0)$).

THEOREM 5.3 *Let V be a finite-dimensional k-vector space and A a k-subalgebra of $\mathrm{End}_k(V)$. If V is semisimple as an A-module, then the centralizer of A in $\mathrm{End}_k(V)$ is a product of simple k-algebras (hence it is a semisimple k-algebra).*

PROOF. By assumption, we can write $V \approx \bigoplus_i r_i S_i$, where the S_i are simple A-modules, no two of which are isomorphic.The centralizer of A in $\mathrm{End}_k(V)$ is $\mathrm{End}_A(V)$, and $\mathrm{End}_A(V) \approx \mathrm{End}_A(\bigoplus_i r_i S_i)$. Because $\mathrm{Hom}_A(S_j, S_i) = 0$ for $i \neq j$,

$$\begin{aligned} \mathrm{End}_A(\textstyle\bigoplus r_i S_i) &\simeq \textstyle\prod_i \mathrm{End}_A(r_i S_i) \quad \text{by (41)} \\ &\simeq \textstyle\prod_i M_{r_i}(D_i) \quad \text{by (42)} \end{aligned}$$

where $D_i = \mathrm{End}_A(S_i)$. According to Schur's lemma (1.16), D_i is a division algebra, and therefore $M_{r_i}(D_i)$ is a simple k-algebra (1.11). □

THEOREM 5.4 *Every semisimple k-algebra is isomorphic to a product of simple k-algebras.*

PROOF. Choose an A-module V on which A acts faithfully, for example, $V = {}_AA$. Then A is equal to its double centralizer $C(C(A))$ in $\mathrm{End}_k(V)$ (see 1.14). According to Theorem 5.3, $C(A)$ is semisimple, and so $C(C(A))$ is a product of simple algebras (5.3). □ *Modules over a semisimple k-algebra*

Let $A = B \times C$ be a product of k-algebras. A B-module M becomes an A-module with the action $(b, c)m = bm$.

THEOREM 5.5 *Let A be a semisimple k-algebra, say, $A = A_1 \times \cdots \times A_t$ with the A_i simple. For each A_i, let S_i be a simple A_i-module.*

(a) *Each S_i is a simple A-module, and every simple A-module is isomorphic to exactly one of the S_i.*

(b) *Every A -module is isomorphic to $\bigoplus r_i S_i$ for some $r_i \in \mathbb{N}$, and two modules $\bigoplus r_i S_i$ and $\bigoplus r_i' S_i$ are isomorphic if and only if $r_i = r_i'$ for all i.*

PROOF. (a) It is obvious that each S_i is simple when regarded as a n A-module, and that no two of them are isomorphic. It follows from 1.20 that ${}_AA \approx \bigoplus r_i S_i$ for some $r_i \in \mathbb{N}$. Let S be a simple A-module, and let x be a nonzero element of S. Then the map $a \mapsto ax : {}_AA \to S$ is surjective, and so its restriction to some S_i in ${}_AA$ is nonzero, and hence an isomorphism.

(b) The first part follows from (a) and the definition of a semisimple ring, and the second part follows from 1.3. □

PROPOSITION 5.6 *Let A be a semisimple k-algebra and k' a separable extension of k. Then $A \otimes_k F$ is semisimple.*

PROOF. We may suppose that it is simple. Then the centre F of A is a field. Because k'/k is separable, $F \otimes_k k'$ is a product of fields F_i. Now

$$A \otimes_k k' \simeq A \otimes_F (F \otimes_k k') \simeq A \otimes_F (\textstyle\prod F_i) \simeq \prod A \otimes_F F_{\mathrm{i}},$$

and each algebra $A \otimes_F F_i$ is simple (2.15). □

Algebras, cohomology, and group extensions

Let A be a central simple algebra of degree n^2 over k, and assume that A contains a field L that is Galois of degree n over k. Let E be the set of invertible elements $\alpha \in A$ such that $\alpha L \alpha^{-1} = L$. Then each $\alpha \in E$ defines an element $x \mapsto \alpha x \alpha^{-1}$ of $\mathrm{Gal}(L/k)$, and the Noether-Skolem the orem implies that every element of $\mathrm{Gal}(L/k)$ arises from an $\alpha \in E$. Because $[L:k] = \sqrt{[A:k]}$, the centralizer of L is L itself, and so the sequence

$$1 \to L^\times \to E^\times \to \mathrm{Gal}(L/k) \to 1$$

is exact. It is not difficult to show that the map sending A to this sequence defines an isomorphism from $\mathcal{A}(L/k)$ to the set of isomorphism classes of extensions of $\mathrm{Gal}(L/k)$ by $L^\times$, and hence to $H^2(L/k)$ (see II, 1.18). See Serre 1950/51.

Brauer groups and K-theory

Let k be a field containing a primitive nth root ζ of 1. To any elements $a, b \in k^\times$, one attaches the k-algebra $A(a,b;\zeta)$ having generators i and j and relations

$$i^n = a, \quad j^n = b, \quad ij = \zeta ji.$$

It is a central simple algebra over k.

The **Milnor K-group** K_2F of a field F is the quotient of $F^\times \otimes_{\mathbb{Z}} F^\times$ by the abelian group generated by the elements of the form $u \otimes (1-u)$ with u an element of $F^\times$ such that $1-u \in F^\times$. Thus K_2F has as generators pairs $\{a,b\}$, one for each pair of elements in $F^\times$, and relations

$$\begin{aligned} \{ab,c\} &= \{a,c\}\{b,c\} \\ \{a,bc\} &= \{a,b\}\{a,c\} \\ \{u,1-u\} &= 1. \end{aligned}$$

It is known that these relations imply that

$$\begin{aligned} \{u,v\} &= \{v,u\}^{-1} \\ \{u,-u\} &= 1 \end{aligned}$$

(see Rosenberg 1994, p. 214).

It is not difficult to show that the $A(a,b;\zeta)$, considered as elements of $\mathrm{Br}(k)$ satisfy these relations, and so there is a well-defined homomorphism

$$K_2k \to \mathrm{Br}(k).$$

Remarkably, it has been proved (Theorem of Merkuryev-Suslin, early 1980s) that this map defines an isomorphism from K_2k/nK_2k onto the subgroup of $\mathrm{Br}(k)$ of elements killed by n, and so we have an explicit description of $\mathrm{Br}(k)_n$ in terms of generators and relations.[6]

EXERCISE 5.7 Let F be a field of characteristic $\neq 2$, and define the quaternion algebra $H(a,b)$ as in (1.12). Thus $H(a,b)$ has basis $1, i, j, k$ and $i^2 = a$, $j^2 = b$, $k = ij = -ji$. It is a central simple algebra over F.

(a) Show that every 4-dimensional central simple algebra over k is isomorphic to $H(a,b)$ for some $a, b \in F^\times$.

(b) According to Wedderburn's theorem, either $H(a,b) \approx M_2(F)$ or $H(a,b)$ is a division algebra. Show that the first case occurs if and only if $w^2 - ax^2 - by^2 + abz^2$ has a nontrivial zero in F. (Hint: for $\alpha = w + xi + yj + zk$, let $\bar{\alpha} = w - xi - yj - zk$, and note that $\alpha\bar{\alpha} = w^2 - ax^2 - \cdots$)

(c) Show that $H(1,1) \approx M_2(F)$. (Hint: consider the matrices $e_{12} + e_{21}$ and $e_{11} - e_{22}$.)

(d) Show that $H(a,b) \approx H(ax^2, by^2)$ any $x, y \in F^\times$.

(e) Show that $H(a,b) \otimes_F L$ is the quaternion algebra over L defined by a, b regarded as elements of L.

(f) Verify that $H(a,b)$ is in fact central simple over F.

(g) Show that $H(a, 1-a) \approx M_2(F)$, provided $a, 1-a \in F^\times$.

(h) Show that $H(1,b) \approx H(a,-a) \approx M_2(F)$ (Hint: consider $j+k$ and $i+j$.)

(i) Show that $H(a,b) \approx H(a,b)^{\mathrm{opp}}$.

---

[6]See: Merkurjev, A. S.; Suslin, A. A. K-cohomology of Severi-Brauer varieties and the norm residue homomorphism. (Russian) Izv. Akad. Nauk SSSR Ser. Mat. 46 (1982), no. 5, 1011–1046, 1135–1136.

The theorem is discussed in the book: Kersten, Ina. Brauergruppen von Ko¨rpern. (German) [Brauer groups of fields] Aspects of Mathematics, D6. Friedr. Vieweg & Sohn, Braunschweig, 1990.

(j) Show that $H(a,b) \approx M_2(F)$ if and only if $a \in \mathrm{Nm}(F[\sqrt{b}])$.

(k) Show that the map $\{a,b\} \mapsto [H(a,b)]: K_2F \to \mathrm{Br}(F)$ is well-defined.

EXERCISE 5.8 For a given central division algebra D over $\mathbb{Q}$, determine the number fields that admit an embedding into D.

EXERCISE 5.9 Determine the number fields that admit an embedding into some central division algebra over $\mathbb{Q}$.

For a solution to Exercises 5.8 and 5.9, see sx178999.

Notes

Brauer groups were introduced and studied by R. Brauer, and studied by Albert, Brauer, Noether, Hasse, and others, starting in the nineteen-twenties. The classic accounts are: Deuring, M., Algebren, Springer, 1935. Artin, E., Nesbitt, C., and Thrall, R., Rings with Minimum Condition, University of Michigan. Press, 1944. Apart from the quaint terminology (e.g., Kronecker products for tensor products), the latter is still an excellent book.

Other books include Blanchard 1972, Farb and Dennis 1993, and Herstein 1968. These books include the Brauer group, but also cover much more (but no number theory). The second has lots of exercises.

I found the following especially useful when I was writing the first version of this chapter: Serre, J-P., Applications alge´briques de la cohomologie des groupes, I, II, Se´minaire Henri Cartan, 1950/51 (now available at www.numdam.org).

4. GLOBAL CLASS FIELD THEORY: STATEMENTS

J. S. Milne, Class Field Theory (v4.03)

> *La théorie du corps de classes a une réputation de difficulté qui est en partie justifiée. Mais il faut faire une distinction: il n'est peut-être pas en effet dans la science de théorie où tout à la fois les démonstrations soient aussi ardues, et les résultats d'une aussi parfaite simplicité et d'une aussi grande puissance.*
> J. Herbrand, 1936, p. 2.[1]

In this chapter, I state and explain the main theorems of global class field theory. They will be proved in Chapter VII

Throughout this chapter, K is a number field, although most of the results hold also for finite extensions of $\mathbb{F}_p(T)$.

Recall that for a number field K, we define a **prime** of K to be an equivalence class of nontrivial absolute values of K. There are two types of primes: the **finite primes**, which can be identified with the prime ideals of $\mathcal{O}_K$, and the **infinite primes.** A **real** infinite prime can be identified with an embedding of K into $\mathbb{R}$, and a **complex** infinite prime can be identified with a conjugate pair of embeddings of K into $\mathbb{C}$. We use $\mathfrak{p}$ or v to denote a prime, finite or infinite. We use S to denote a finite set of primes of K, and also the set of primes of a finite extension L of K lying over K. The set of infinite primes is denoted by S_∞.

The completion of K at a prime $\mathfrak{p}$ (resp. v) is denoted by $K_\mathfrak{p}$ (resp. K_v), and the inclusion $K \hookrightarrow K_\mathfrak{p}$ (resp. $K \hookrightarrow K_v$) is denoted $a \mapsto a_\mathfrak{p}$ (resp. $a \mapsto a_v$).

1 Ray Class Groups

Ideals prime to S

Let $I = I_K$ be the group of fractional ideals in K. For a finite set S of primes of K, we define I^S to be the subgroup of I generated by the prime ideals not in S. Each element $\mathfrak{a}$

[1]Class field theory has a reputation for being difficult, which is partly justified. But it is necessary to make a distinction: there is perhaps nowhere in science a theory in which the proofs are so difficult but at the same time the results are of such perfect simplicity and of such great power.

of I^S factors uniquely as

$$\mathfrak{a} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_s^{n_s}, \quad \mathfrak{p}_i \notin S, \quad n_i \in \mathbb{Z},$$

and so I^S can be identified with the free abelian group generated by the prime ideals not in S. Define

$$K^S = \{a \in K^\times \mid (a) \in I^S\} = \{a \in K^\times \mid \operatorname{ord}_\mathfrak{p}(a) = 0 \text{ all finite } \mathfrak{p} \in S\}.$$

Let $i\colon K^S \to I^S$ be the map sending an element a of K^S to the ideal $a\mathcal{O}_K$.

For example, when $K = \mathbb{Q}$ and S is the set of prime numbers dividing and integer n, I^S is the set of fractional ideals

$$\{(r/s) \mid r, s \in \mathbb{Z}\,,\ \gcd(r,n) = 1 = \gcd(s,n)\}$$

and

$$\mathbb{Q}^S = \{r/s \mid r, s \in \mathbb{Z},\ \gcd(r,n) = 1 = \gcd(s,n)\}.$$

In this case, the natural map $\mathbb{Q}^S \to I^S$ is surjective with kernel $\{\pm 1\}$.

LEMMA 1.1 *For every finite set S of prime ideals in $\mathcal{O}_K$, the sequence*

$$0 \to U_K \to K^S \to I^S \to C \to 0$$

is exact. (Here $U_K = \mathcal{O}_K^\times$ and C is the full ideal class group $I/i(K^\times)$.)

PROOF. To show that $I^S \to C$ is surjective, we have to show that every ideal class $\mathcal{C}$ is represented by an ideal in I^S. Let $\mathfrak{a}$ represent $\mathcal{C}$. Then $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1}$ with $\mathfrak{b}$ and $\mathfrak{c}$ integral ideals, and for any $c \in \mathfrak{c}$, $\mathfrak{a}\cdot(c) = \mathfrak{b}\cdot\mathfrak{c}^{-1}\cdot(c)$ is integral, and so we may suppose that $\mathfrak{a}$ itself is an integral ideal. Write $\mathfrak{a} = \prod_{\mathfrak{p}\in S}\mathfrak{p}^{n(\mathfrak{p})}\mathfrak{b}$, where $\mathfrak{b} \in I^S$. For each $\mathfrak{p} \in S$, choose a $\pi_\mathfrak{p} \in \mathfrak{p} \smallsetminus \mathfrak{p}^2$, so that $\operatorname{ord}_\mathfrak{p}(\pi_\mathfrak{p}) = 1$. By the Chinese Remainder Theorem, there exists an $a \in \mathcal{O}_K$ such that

$$a \equiv \pi_\mathfrak{p}^{n(\mathfrak{p})} \bmod \mathfrak{p}^{n(\mathfrak{p})+1}$$

for all $\mathfrak{p} \in S$. These congruences imply that $\operatorname{ord}_\mathfrak{p}(a) = n(\mathfrak{p})$ for all $\mathfrak{p} \in S$, and so $(a) = \prod_{\mathfrak{p}\in S}\mathfrak{p}^{n(\mathfrak{p})}\mathfrak{b}'$ with $\mathfrak{b}' \in I^S$. Now $a^{-1}\mathfrak{a} \in I^S$ and represents the same class as $\mathfrak{a}$ in C.

Next, if $\mathfrak{a} \in I^S$ maps to zero in C, then $\mathfrak{a} = (\alpha)$ for some $\alpha \in K^S$, and α is uniquely determined up to a unit. This proves the exactness at the remaining places. □

REMARK 1.2 In fact, every class in C is represented by an *integral* ideal $\mathfrak{a}$ in I^S: suppose the class is represented by $\mathfrak{a} \in I^S$; write $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1}$ with $\mathfrak{b}$ and $\mathfrak{c}$ integral ideals in I^S, choose a nonzero $c \in \mathfrak{c} \cap K^S$ (exists by the Chinese remainder theorem), and note that $c\mathfrak{a}$ is integral.

Moduli

DEFINITION 1.3 A **modulus** for K is a function

$$m\colon \{\text{ primes of } K\} \to \mathbb{Z}$$

such that

(a) $m(\mathfrak{p}) \geq 0$ for all primes $\mathfrak{p}$, and $m(\mathfrak{p}) = 0$ for all but finitely many $\mathfrak{p}$;

(b) if $\mathfrak{p}$ is real, then $m(\mathfrak{p}) = 0$ or 1;

(c) if $\mathfrak{p}$ is complex, then $m(\mathfrak{p}) = 0$.

Traditionally, one writes

$$\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{m(\mathfrak{p})}.$$

A modulus $\mathfrak{m} = \prod \mathfrak{p}^{m(\mathfrak{p})}$ is said to **divide** a modulus $\mathfrak{n} = \prod_\mathfrak{p} \mathfrak{p}^{n(\mathfrak{p})}$ if $m(\mathfrak{p}) \leq n(\mathfrak{p})$ for all $\mathfrak{p}$. In particular, a prime $\mathfrak{p}$ divides a modulus $\mathfrak{m}$ if and only if $m(\mathfrak{p}) > 0$.

A modulus $\mathfrak{m}$ can be written

$$\mathfrak{m} = \mathfrak{m}_\infty\mathfrak{m}_0,$$

where $\mathfrak{m}_\infty$ is a product of real primes and $\mathfrak{m}_0$ is product of positive powers of prime ideals, and hence can be identified with an ideal in $\mathcal{O}_K$.

The ray class group

For a modulus $\mathfrak{m}$, define $K_{\mathfrak{m},1}$ to be the set of $a \in K^\times$ such that

$$\begin{cases} \operatorname{ord}_\mathfrak{p}(a-1) \geq m(\mathfrak{p}) & \text{all finite } \mathfrak{p} \text{ dividing } \mathfrak{m} \\ a_\mathfrak{p} > 0 & \text{all real } \mathfrak{p} \text{ dividing } \mathfrak{m}. \end{cases}$$

Note that

$$\begin{aligned} \operatorname{ord}_\mathfrak{p}(a-1) \geq m(\mathfrak{p}) &\iff \pi^{m(\mathfrak{p})} | (a_\mathfrak{p} - 1) \\ &\iff a \mapsto 1 \text{ in } (\mathcal{O}_\mathfrak{p}/\mathfrak{p}^{m(\mathfrak{p})})^\times \simeq (\hat{\mathcal{O}}_\mathfrak{p}/\hat{\mathfrak{p}}^{m(\mathfrak{p})})^\times, \end{aligned}$$

where π is a prime element in the completion $K_\mathfrak{p}$ of K at $\mathfrak{p}$. Let

$$S(\mathfrak{m}) = \{ \text{primes dividing } \mathfrak{m} \}.$$

For any $a \in K_{\mathfrak{m},1}$ and prime ideal $\mathfrak{p}$ dividing $\mathfrak{m}$, $\operatorname{ord}_\mathfrak{p}(a-1) > 0 = \operatorname{ord}_\mathfrak{p}(1)$, and so

$$\operatorname{ord}_\mathfrak{p}(a) = \operatorname{ord}_\mathfrak{p}((a-1)+1) = 0.$$

Therefore, for any $a \in K_{\mathfrak{m},1}$, the ideal (a) lies in $I^{S(\mathfrak{m})}$. Let i denote the map $a \mapsto (a)\colon K_{\mathfrak{m},1} \to I^{S(\mathfrak{m})}$. The quotient

$$C_\mathfrak{m} = I^{S(\mathfrak{m})}/i(K_{\mathfrak{m},1})$$

is called the **(ray) class group modulo** $\mathfrak{m}$.

EXAMPLE 1.4 The expression $\mathfrak{m} = (2)^3 \cdot (17)^2 \cdot (19) \cdot \infty$ is a modulus for $\mathbb{Q}$ with $\mathfrak{m}_0 = (2)^3 \cdot (17)^2 \cdot (19)$ and $\mathfrak{m}_\infty = \infty$ (here ∞ denotes the unique infinite prime of $\mathbb{Q}$). Moreover, $\mathbb{Q}_{\mathfrak{m},1}$ consists of the positive rational numbers a such that

$$\begin{cases} \operatorname{ord}_2(a-1) \geq 3 \\ \operatorname{ord}_{17}(a-1) \geq 2 \\ \operatorname{ord}_{19}(a-1) \geq 1 \end{cases}.$$

The condition at 2 says that a is the quotient of two odd integers, $a = b/c$, and that the image of bc^{-1} in $(\mathbb{Z}/8\mathbb{Z})^\times$ is 1. The other conditions can be expressed similarly.

LEMMA 1.5 *Let S be a finite set of prime ideals of K. Then every element $\alpha \in K^S$ can be written $\alpha = a/b$ with $a, b \in \mathcal{O}_K \cap K^S$.*

PROOF. Because $\alpha \in K^S$, $(\alpha) = \mathfrak{a}/\mathfrak{b}$ with $\mathfrak{a}, \mathfrak{b}$ integral ideals in I^S. Clearly $\mathfrak{a}$ and $\mathfrak{b}$ represent the same element $\mathcal{C}$ of the ideal class group, and according to Remark 1.2 we can choose an integral ideal $\mathfrak{c}$ in I^S to represent $\mathcal{C}^{-1}$. Now $(\alpha) = \mathfrak{ac}/\mathfrak{bc} = (a)/(b)$ for some $a, b \in \mathcal{O}_K \cap K^S$. □

PROPOSITION 1.6 *Every class in $C_\mathfrak{m}$ is represented by an integral ideal $\mathfrak{a}$, and two integral ideals $\mathfrak{a}$ and $\mathfrak{b}$ represent the same class in $C_\mathfrak{m}$ if and only if there exist nonzero $a, b \in \mathcal{O}_K$ such that $a\mathfrak{a} = b\mathfrak{b}$ and*

$$a \equiv b \equiv 1 \bmod \mathfrak{m}_0$$

a and b have the same sign for every real prime dividing $\mathfrak{m}$.

PROOF. Suppose that the class is represented by $\mathfrak{a} \in I^S$, and let $\mathfrak{a} = \mathfrak{bc}^{-1}$ with $\mathfrak{b}$ and $\mathfrak{c}$ integral ideals in I^S. The Chinese remainder theorem shows that there exists a nonzero $c \in \mathfrak{c} \cap K_{\mathfrak{m}_0,1}$, and the strong approximation theorem shows that c can be chosen to be > 0 at the real primes. Now $c\mathfrak{a}$ is integral and represents the same class as $\mathfrak{a}$ in $C_\mathfrak{m}$. The second part of the statement follows from Lemma 1.5. □

Thus, for example, the usual ideal class group can be identified with the set of integral ideals modulo the equivalence relation: $\mathfrak{a} \sim \mathfrak{b}$ if and only if $a\mathfrak{a} = b\mathfrak{b}$ for some nonzero $a, b \in \mathcal{O}_K$.

THEOREM 1.7 *For every modulus* $\mathfrak{m}$ *of* K*, there is an exact sequence*

$$0 \to U/U_{\mathfrak{m},1} \to K_{\mathfrak{m}}/K_{\mathfrak{m},1} \to C_{\mathfrak{m}} \to C \to 0$$

and canonical isomorphisms

$$K_{\mathfrak{m}}/K_{\mathfrak{m},1} \simeq \prod_{\substack{\mathfrak{p}\ \textit{real}\\ \mathfrak{p}|\mathfrak{m}}} \{\pm\} \times \prod_{\substack{\mathfrak{p}\ \textit{finite}\\ \mathfrak{p}|\mathfrak{m}}} (\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^\times \simeq \prod_{\substack{\mathfrak{p}\ \textit{real}\\ \mathfrak{p}|\mathfrak{m}}} \{\pm\} \times (\mathcal{O}_K/\mathfrak{m}_0)^\times,$$

where

$$\begin{aligned} K_{\mathfrak{m}} &= K^{S(\mathfrak{m})} = \{\alpha \in K^\times \mid \operatorname{ord}_{\mathfrak{p}}(\alpha) = 0 \textit{ for all } \mathfrak{p}|\mathfrak{m}_0\} \\ U &= \mathcal{O}_K^\times \textit{ , the group of units in } K, \\ U_{\mathfrak{m},1} &= U \cap K_{\mathfrak{m},1}. \end{aligned}$$

Therefore, $C_{\mathfrak{m}}$ *is a finite group of order*

$$h_{\mathfrak{m}} = h \cdot (U : U_{\mathfrak{m},1})^{-1} \cdot 2^{r_0} \cdot \mathbb{N}(\mathfrak{m}_0) \cdot \prod_{\mathfrak{p}|\mathfrak{m}_0} \left(1 - \frac{1}{\mathbb{N}\mathfrak{p}}\right),$$

where r_0 *is the number of real primes dividing* $\mathfrak{m}$ *and* h *is the class number of* K *(order of* C*).*

PROOF. The inclusion $I^{S(\mathfrak{m})} \to I$ defines a homomorphism $C_{\mathfrak{m}} \to C$. Consider the pair of maps

$$K_{\mathfrak{m},1} \xrightarrow{f} K_{\mathfrak{m}} \xrightarrow{g} I^{S(\mathfrak{m})}.$$

According to the Lemma 1.1, the kernel and cokernel of g are U and C respectively. The cokernel of $g \circ f$ is $C_{\mathfrak{m}}$ (by definition) and its kernel is $K_{\mathfrak{m},1} \cap U = U_{\mathfrak{m},1}$. Finally, f is injective. Therefore, the kernel-cokernel sequence (see II, A.2) of the pair of maps is

$$0 \to U_{\mathfrak{m},1} \to U \to K_{\mathfrak{m}}/K_{\mathfrak{m},1} \to C_{\mathfrak{m}} \to C \to 0.$$

We next prove that $K_{\mathfrak{m}}$ is canonically isomorphic to the given groups. Let $\mathfrak{p}$ be a prime dividing $\mathfrak{m}$. If $\mathfrak{p}$ is real, we map $\alpha \in K_{\mathfrak{m}}$ to the sign of $\alpha_{\mathfrak{p}}$ (recall that a real prime is an embedding $K \hookrightarrow \mathbb{R}$, and that $\alpha_{\mathfrak{p}}$ denotes the image of α under the embedding). If $\mathfrak{p}$ is finite, i.e., it is a prime ideal in $\mathcal{O}_K$, then we map $\alpha \in K_{\mathfrak{m}}$ to $[a][b]^{-1} \in (\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^\times$, where a, b are as in the lemma. As a and b are relatively prime to $\mathfrak{p}$, their classes $[a]$ and $[b]$ in $\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})}$ are invertible, and so this makes sense. The weak approximation theorem (ANT, 7.20) shows that the map $K_{\mathfrak{m}} \to \prod\{\pm\} \times \prod(\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^\times$ is surjective, and its kernel is obviously $K_{\mathfrak{m},1}$.

The Chinese Remainder Theorem shows that there is an isomorphism of rings

$$\mathcal{O}_K/\mathfrak{m}_0 \simeq \prod_{\mathfrak{p}|\mathfrak{m}} \mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})},$$

and hence an isomorphism of groups

$$(\mathcal{O}_K/\mathfrak{m}_0)^\times \simeq \prod(\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^\times.$$

This completes proof of the isomorphisms.

It remains to compute the orders of the groups. Note that $\mathcal{O}_K/\mathfrak{p}^m$ is a local ring with maximal ideal $\mathfrak{p}/\mathfrak{p}^m$ (because its ideals correspond to the ideals of $\mathcal{O}_K$ containing $\mathfrak{p}^m$), and so its units are the elements not in $\mathfrak{p}/\mathfrak{p}^m$. The filtration

$$(\mathcal{O}_K/\mathfrak{p}^m)^\times \supset (1+\mathfrak{p})/\mathfrak{p}^m \supset \cdots \supset (1+\mathfrak{p}^{m-1})/\mathfrak{p}^m \supset 0$$

has quotients isomorphic to

$$k^\times, k, \dots, k, \quad k \stackrel{\text{def}}{=} \mathcal{O}_K/\mathfrak{p},$$

and so $(\mathcal{O}_K/\mathfrak{p}^m)^\times$ has order $(q-1)q^{m-1}$, $q = (\mathcal{O}_K : \mathfrak{p}) \stackrel{\text{def}}{=} \mathbb{N}\mathfrak{p}$. This shows that

$$(C_\mathfrak{m} : 1) = (C : 1) \cdot (K_\mathfrak{m} : K_{\mathfrak{m},1}) \cdot (U_\mathfrak{m} : U_{\mathfrak{m},1})^{-1}$$

is equal to the expression in the statement of the theorem. □

EXAMPLE 1.8 (a) If $\mathfrak{m} = 1$, then $C_\mathfrak{m} = C$.

(b) When $\mathfrak{m}$ is the product of the real primes, $C_\mathfrak{m}$ is the narrow-class group and there is an exact sequence

$$0 \to U/U_+ \to K^\times/K_+ \to C_\mathfrak{m} \to C \to 1,$$

where K_+ is the group of totally positive elements (i.e., positive under all real embeddings) and U_+ is the group of all totally positive units. Moreover, $K^\times/K_+ \simeq \prod_{\mathfrak{p}\text{ real}}\{\pm\}$, and so the kernel of $C_\mathfrak{m} \to C$ is the set of possible signs modulo those arising from units.

For $\mathbb{Q}$, the narrow-class group is trivial. For $\mathbb{Q}[\sqrt{d}]$, $d > 0$, there are two real primes, and $U = \{\pm\varepsilon^m \mid m \in \mathbb{Z}\} \approx (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}$, where ε is a fundamental unit. Let $\bar{\varepsilon}$ be the conjugate of ε. Then $h_\mathfrak{m} = 2h$ or h according as ε and $\bar{\varepsilon}$ have the same or different signs. Note that $\mathrm{Nm}(\varepsilon) = +1$ if the signs are the same and -1 if they differ. For small values of d we have

d	h	ε	$\mathrm{Nm}(\varepsilon)$
2	1	$1+\sqrt{2}$	-1
3	1	$2+\sqrt{3}$	1
5	1	$(1+\sqrt{5})/2$	-1
6	1	$5+2\sqrt{6}$	1

Therefore, $\mathbb{Q}[\sqrt{3}]$ and $\mathbb{Q}[\sqrt{6}]$ have class number 1 but narrow-class number 2, whereas for $\mathbb{Q}[\sqrt{2}]$ $\mathbb{Q}[\sqrt{3}]$ and $\mathbb{Q}[\sqrt{5}]$ both class numbers are 1.

(c) For the field $\mathbb{Q}$ and the modulus (m), the sequence becomes

$$0 \to \{\pm 1\} \to (\mathbb{Z}/m\mathbb{Z})^\times \to C_\mathfrak{m} \to 0.$$

For the modulus $\infty(m)$, the sequence becomes

$$0 \to \{\pm 1\} \to \{\pm\} \times (\mathbb{Z}/m\mathbb{Z})^\times \to C_\mathfrak{m} \to 0.$$

Here -1 maps to $(-, [-1])$, and the subgroup $(\mathbb{Z}/m\mathbb{Z})^\times$ of the product maps isomorphically onto the quotient $C_\mathfrak{m}$.

The Frobenius element

We review the theory of the Frobenius element (ANT, Chapter 8). Let K be a number field, and let L be a finite Galois extension of K with group G. Let $\mathfrak{p}$ be an ideal of K, and let $\mathfrak{P}$ be an ideal of L lying over it. The decomposition group $D(\mathfrak{P})$ (or $G(\mathfrak{P})$) is defined to be

$$\{\tau \in G \mid \tau\mathfrak{P} = \mathfrak{P}\}.$$

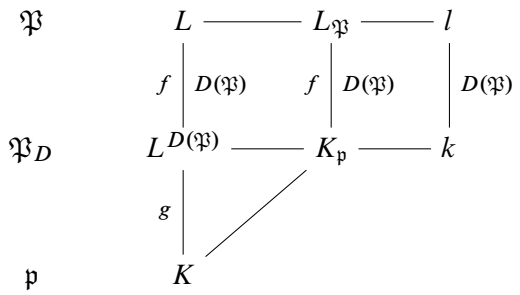
Equivalently, it is the set of elements of G that act continuously for the $\mathfrak{P}$-adic topology, and so extend to the completion $L_\mathfrak{P}$. In this way we obtain an isomorphism

$$D(\mathfrak{P}) \to \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p}).$$

Assume $\mathfrak{P}$ is unramified over $\mathfrak{p}$. Then the action of $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ on $\mathcal{O}_L$ induces an isomorphism

$$\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \to \mathrm{Gal}(l/k),$$

where l and k are the residue fields. Pictorially:



The group $\mathrm{Gal}(l/k)$ is cyclic with a canonical generator, namely, the Frobenius element $x \mapsto x^q$, where q is the number of elements of k. Hence $D(\mathfrak{P})$ is cyclic, and the generator of $D(\mathfrak{P})$ corresponding to the Frobenius element in $\mathrm{Gal}(l/k)$ is called the **Frobenius ele- ment** $(\mathfrak{P}, L/K)$ at $\mathfrak{P}$. It is the unique element σ of $\mathrm{Gal}(L/K)$ satisfying the following two conditions:

(a) $\sigma \in D(\mathfrak{P})$, i.e., $\sigma\mathfrak{P} = \mathfrak{P}$;

(b) for all $\alpha \in \mathcal{O}_L$, $\sigma\alpha \equiv \alpha^q \bmod \mathfrak{P}$, where q is the number of elements the residue field $\mathcal{O}_K/\mathfrak{p}$, $\mathfrak{p} = \mathfrak{P} \cap K$.

We now list the basic properties of $(\mathfrak{P}, L/K)$.

1.9 *Let $\tau\mathfrak{P}$ be a second prime dividing $\mathfrak{p}$. Then $D(\tau\mathfrak{P}) = \tau D(\mathfrak{P})\tau^{-1}$, and*

$$(\tau\mathfrak{P}, L/K) = \tau(\mathfrak{P}, L/K)\tau^{-1}.$$

PROOF. If $\rho \in D(\mathfrak{P})$, then

$$\rho\tau^{-1}(\tau\mathfrak{P}) = \tau\rho\mathfrak{P} = \tau\mathfrak{P},$$

and so $\tau\rho\tau^{-1} \in D(\tau\mathfrak{P})$. Thus $\tau D(\mathfrak{P})\tau^{-1} \subset D(\tau\mathfrak{P})$, and since they have the same order, they must be equal.

Let $\alpha \in \mathcal{O}_L$ and let $\sigma = (\mathfrak{P}, L/K)$; then

$$\sigma\tau^{-1}(\alpha) = \tau\left((\tau^{-1}\alpha)^q + a\right) \text{ , some } a \in \mathfrak{P} \text{ , and}$$

$$\tau\left((\tau^{-1}\alpha)^q + a\right) = \alpha^q + \tau a \equiv \alpha^q \bmod \tau\mathfrak{P}. \qquad \square$$

As G acts transitively on the primes dividing $\mathfrak{p}$, this implies that

$$\{(\mathfrak{P}, L/K) \mid \mathfrak{P}|\mathfrak{p}\}$$

is a conjugacy class in G, which we denote $(\mathfrak{p}, L/K)$. When L/K is abelian, $(\mathfrak{p}, L/K)$ contains a single element, and we regard it as an element of $\mathrm{Gal}(L/K)$ (rather than a set consisting of a single element).

1.10 *Consider a tower of fields*

$$\begin{array}{cc} M & \mathfrak{Q} \\ | & \\ L & \mathfrak{P} \\ | & \\ K & \mathfrak{p} \end{array}$$

and assume that $\mathfrak{Q}$ is unramified over $\mathfrak{p}$; then

$$(\mathfrak{Q}, M/L) = (\mathfrak{Q}, M/K)^{f(\mathfrak{P}/\mathfrak{p})}.$$

PROOF. Let $k(\mathfrak{Q}) \supset k(\mathfrak{P}) \supset k(\mathfrak{p})$ be the tower of residue fields. Then $f(\mathfrak{P}/\mathfrak{p}) \stackrel{\text{def}}{=} [k(\mathfrak{P}) : k(\mathfrak{p})]$, and the Frobenius element in $\mathrm{Gal}(k(\mathfrak{Q})/k(\mathfrak{P}))$ is the $f(\mathfrak{P}/\mathfrak{p})$th power of the Frobenius element in $\mathrm{Gal}(k(\mathfrak{Q})/k(\mathfrak{p}))$. The rest is straightforward. □

1.11 *In 1.10, assume that L is Galois over K; then*

$$(\mathfrak{Q}, M/K)|L = (\mathfrak{P}, L/K).$$

PROOF. Clearly $(\mathfrak{Q}, M/K)|L$ satisfies the conditions characterizing $(\mathfrak{P}, L/K)$. □

Let L_1 and L_2 be Galois extensions of K contained in some field Ω, and let $M = L_1 \cdot L_2$. Then M is Galois over K, and there is an injective homomorphism

$$\sigma \mapsto (\sigma|L_1, \sigma|L_2) \colon \mathrm{Gal}(M/K) \to \mathrm{Gal}(L_1/K)) \times \mathrm{Gal}(L_2/K).$$

1.12 *Let $\mathfrak{Q}$ be a prime ideal of $\mathcal{O}_M$, and let $\mathfrak{P}_i = \mathfrak{Q} \cap \mathcal{O}_{L_i}$. Under the above map,*

$$(\mathfrak{Q}, M/K) \mapsto (\mathfrak{P}_1, L_1/K) \times (\mathfrak{P}_2, L_2/K).$$

PROOF. Apply 1.11. □

Note that $\mathfrak{p}$ splits completely in L if and only if $(\mathfrak{P}, L/K) = 1$ for one (hence all) primes $\mathfrak{P}$ lying over it. Hence, in the situation of 1.12, $\mathfrak{p}$ splits completely in M if and only if it splits completely in L_1 and L_2.

2 L-series

Progressions

We begin by briefly reviewing the elementary theory of Dirichlet L-series (see, for example, Serre 1970, Chapter VI).

Let m be an integer. A **Dirichlet character modulo** m is a homomorphism $\chi \colon (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$. Because $(\mathbb{Z}/m\mathbb{Z})^\times$ is finite, $\chi([n])$ is a root of 1 for all n. A Dirichlet character modulo m can be regarded as a multiplicative function on the set of integers prime to m whose value at n depends only on n modulo m. Often one extends to a function on all the integers by setting $\chi(n) = 0$ when $\gcd(m, n) \neq 1$. The trivial Dirichlet character modulo m, taking the value 1 for all integers prime to m, is called the **principal Dirichlet character** χ_0.

To a Dirichlet character modulo m, one attaches a Dirichlet series

$$L(s, \chi) = \prod_{p \nmid m} \frac{1}{1 - \chi(p)p^{-s}} = \sum_{n>0} \chi(n)/n^s.$$

Both expressions converge for s a complex number with $\Re(s) > 1$—their equality is the analytic expression of the unique factorization. Note that $L(s, \chi_0)$ differs from the Riemann zeta function $\zeta(s)$ only in that it is missing the factors $\frac{1}{1-p^{-s}}$ for p dividing m.

THEOREM 2.1 *(a) The zeta function $\zeta(s)$ extends to a meromorphic function on the half- plane $\Re(s) > 0$, and*

$$\zeta(s) = \frac{1}{s-1} + \varphi(s),$$

where $\varphi(s)$ is holomorphic for $\Re(s) > 0$.

(b) If $\chi \neq \chi_0$, then the series for $L(s, \chi)$ converges for $\Re(s) > 0$ and $L(1, \chi) \neq 0$.

PROOF. Serre 1970, Chapter VI, Propositions 10, 12, Theó'reme 1. □

Applying log to the equality in (a) and using $-\log(1-x) \sim x$ gives

$$\sum_p p^{-s} \sim \log \frac{1}{1-s} \qquad (s \downarrow 1).$$

This means that $\left(\sum_p p^{-s}\right)/\log(1/(1-s))$ tends to 1 as s approaches 1 through real numbers $s > 1$. Accordingly, a set T of primes has *Dirichlet (or analytic) density* δ if

$$\lim_{s\downarrow 1} \frac{\sum_{p\in T} p^{-s}}{\log(1/(1-s))} = \delta.$$

Define $f_\chi(s) = \sum_{p\nmid m} \chi(p)/p^s$. Then (2.1b) shows that, for $\chi \neq \chi_0$, $f_\chi(s)$ is bounded near $s = 1$. An elementary argument (Serre 1970, Chapter VI, Lemme 9) shows that, for every a prime to m,

$$\sum_{p\equiv a \bmod m} 1/p^s = \frac{1}{\varphi(m)} \sum_\chi \chi(a)^{-1} f_\chi(s),$$

def $_\times$ where $\varphi(m) \overset{\text{def}}{=} |(\mathbb{Z}/m\mathbb{Z})^\times|$ and the sum is over all Dirichlet characters modulo m.

THEOREM 2.2 *For every a prime to m, the primes in the arithmetic progression*

$$\ldots, a-2m, a-m, a, a+m, a+2m, \ldots$$

have Dirichlet density $1/\varphi(m)$.

PROOF. For $\chi \neq \chi_0$, $f_\chi(s)$ remains bounded near $s = 1$, and so

$$\sum_{p\equiv a \bmod m} 1/p^s \sim \frac{1}{\varphi(m)} \chi_0(a)^{-1} f_{\chi_0}(s) \sim \frac{1}{\varphi(m)} \log \frac{1}{1-s} \text{ as } s \downarrow 1.$$

□

COROLLARY 2.3 *For every m, the set of primes splitting in the cyclotomic field $\mathbb{Q}[\zeta_m]$ has Dirichlet density $1/\varphi(m)$.*

PROOF. A prime ideal (p) splits in $\mathbb{Q}[\zeta_m]$ if and only if $p \equiv 1 \mod m$. □

We now explain how the above results generalize from $\mathbb{Q}$ to arbitrary number fields. Proofs will be given in Chapter VI.

Let K be a number field, and let $\mathfrak{m}$ be modulus for K. A **(Dirichlet or Weber) character modulo $\mathfrak{m}$** is a homomorphism $\chi: C_\mathfrak{m} \to \mathbb{C}^\times$—again, its values are roots of 1. Alternatively, such a character is a multiplicative function $I^S \to \mathbb{C}^\times$ that is zero on $i(K_{\mathfrak{m},1})$ for some modulus $\mathfrak{m}$ with $S(\mathfrak{m}) = S$. The **principal character** modulo $\mathfrak{m}$ is the function $\chi_0: C_\mathfrak{m} \to \mathbb{C}^\times$ taking only the value 1.

To a character modulo $\mathfrak{m}$, one attaches a Dirichlet series

$$L(s,\chi) = \prod_{\mathfrak{p}\nmid\mathfrak{m}} \frac{1}{1-\chi(\mathfrak{p})\mathbb{N}\mathfrak{p}^{-s}} = \sum_{(\mathfrak{a},\mathfrak{m}_0)=\mathcal{O}_K} \chi(\mathfrak{a})/\mathbb{N}\mathfrak{a}^s.$$

The product is over the prime ideals relatively prime to $\mathfrak{m}_0$, and the sum is over the integral ideals relatively prime to $\mathfrak{m}_0$. Again, both expressions converge for $\Re(s) > 1$, and their equality is the analytic expression of the unique factorization of ideals. The L-series $L(s,\chi_0)$ differs by only a finite number of factors from the **Dedekind zeta function**

$$\zeta_K(s) \overset{\text{def}}{=} \prod_\mathfrak{p} \frac{1}{1-\mathbb{N}\mathfrak{p}^{-s}} = \sum_{\mathfrak{a}\subset\mathcal{O}_K} \mathbb{N}\mathfrak{a}^{-s}.$$

THEOREM 2.4 *(a) The zeta function $\zeta_K(s)$ extends to a meromorphic function on the half- plane $\Re(s) > 0$, and*

$$\zeta_K(s) \sim \frac{2^{r_1}(2\pi)^{r_2}\ Reg(K)}{w_K|\Delta_{K/\mathbb{Q}}|^{1/2}} h_K \frac{1}{s-1} \text{ as } s \downarrow 1,$$

where r_1 and r_2 are the numbers of real and complex primes of K respectively, $Reg(K)$ is the regulator of K (see ANT, Chapter 5), w_K is the number of roots of 1 in K, $\Delta_{K/\mathbb{Q}}$ is the discriminant of $K/\mathbb{Q}$, and h_K is the class number.

(b) If $\chi \neq \chi_0$, then the series for $L(s,\chi)$ converges for $\Re(s) > 0$ and $L(1,\chi) \neq 0$.

The proof of (b) uses the Existence Theorem (see 3.6). Again, on applying log to the equality in (a), one finds that

$$\sum_{\mathfrak{p}} 1/\mathbb{N}\mathfrak{p}^s \sim \log \frac{1}{s-1} \text{ as } s \downarrow 1,$$

and one says that a set T of prime ideals in K has **Dirichlet (or natural) density** δ if

$$\sum_{\mathfrak{p}\in T} 1/\mathbb{N}\mathfrak{p}^s \sim \delta \log \frac{1}{s-1} \text{ as } s \downarrow 1.$$

A similar argument to that in the previous case proves:

THEOREM 2.5 *For every ideal $\mathfrak{a}$ relatively prime to $\mathfrak{m}_0$, the prime ideals in $\mathcal{O}_K$ whose class in $C_\mathfrak{m}$ is $[\mathfrak{a}]$ have Dirichlet density $1/h_\mathfrak{m}$.*

The analysis in the proofs of Theorems 2.4 and 2.5 is the same as in the case $K = \mathbb{Q}$, but the number theory is much more difficult.

3 The Main Theorems in Terms of Ideals

The Artin map

Let L/K be a finite abelian extension Galois group G. Recall that, for a prime ideal $\mathfrak{p}$ of K that is unramified in L, there is a Frobenius automorphism $\sigma = (\mathfrak{p}, L/K)$ of L uniquely determined by the following condition: for every prime ideal $\mathfrak{P}$ of L lying over $\mathfrak{p}$, $\sigma\mathfrak{P} = \mathfrak{P}$, and $\sigma\alpha \equiv \alpha^{\mathbb{N}\mathfrak{p}} \bmod \mathfrak{P}$.

For every finite set S of primes of K containing all primes that ramify in L, we have a homomorphism

$$(\ ,L/K): I^S \to \mathrm{Gal}(L/K), \quad \mathfrak{p}_1^{n_1}\cdots\mathfrak{p}_t^{n_t} \mapsto \prod(\mathfrak{p}_i, L/K)^{n_i}$$

called the **global Artin map (or reciprocity map)**.

EXAMPLE 3.1 Let $K = \mathbb{Q}[\sqrt{m}]$, where m is a square-free integer. The set S of finite primes ramifying in K consists of the primes dividing m if $m \equiv 1 \bmod 4$ and the primes dividing m together with 2 otherwise. Identify $\mathrm{Gal}(K/\mathbb{Q})$ with $\{\pm 1\}$. The Artin map is the homomorphism determined by

$$p \mapsto \left(\frac{m}{p}\right) : I^S \to \mathrm{Gal}(K/\mathbb{Q}),$$

where $(\frac{m}{p})$ is the quadratic residue (Legendre) symbol.

EXAMPLE 3.2 Let $L = \mathbb{Q}[\zeta_m]$, where ζ_m is a primitive mth root of 1. Assume that m is odd or divisible by 4 (so that the primes ramifying in L are precisely the primes dividing m). The

map sending an integer n prime to m to the automorphism $\zeta \mapsto \zeta^n$ of L defines an isomorphism $(\mathbb{Z}/m\mathbb{Z})^\times \to \mathrm{Gal}(L/\mathbb{Q})$. For p not dividing n, $(p, L/K) = [p]$. If r and s are positive integers prime to m, then r/s defines a class $[r/s] = [r][s]^{-1} \in (\mathbb{Z}/m\mathbb{Z})^\times$, and the Artin map is the composite of

$$I^S \xrightarrow{(r/s)\mapsto[r/s]} (\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{[n]\mapsto(\zeta\mapsto\zeta^n)} \mathrm{Gal}(L/\mathbb{Q}).$$

Recall (ANT, p. 68) that for any finite extension of number fields L/K, the norm map $\mathrm{Nm}_{L/K}\colon I_L \to I_K$ from the group of fractional ideals of L to the similar group for K, is the unique homomorphism such that for any prime ideal $\mathfrak{P}$ of L, $\mathrm{Nm}_{L/K}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}$, where $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. For any $\alpha \in L$, $\mathrm{Nm}_{L/K}((\alpha)) = (\mathrm{Nm}_{L/K}\,\alpha)$.

PROPOSITION 3.3 *Let L be an abelian extension of K, and let K' be an intermediate field: $L \supset K' \supset K$. Then the following diagram commutes:*

$$\begin{array}{ccc} I_{K'}^S & \xrightarrow{\psi_{L/K'}} & \mathrm{Gal}(L/K') \\ \downarrow{\scriptstyle \mathrm{Nm}} & & \downarrow \\ I_K^S & \xrightarrow{\psi_{L/K}} & \mathrm{Gal}(L/K). \end{array}$$

Here S is any finite set of prime ideals of K containing all those that ramify in L, and also the set of primes of K' lying over a prime in S.

PROOF. Let $\mathfrak{p}'$ be any prime ideal of K' lying over a prime ideal $\mathfrak{p}$ of K not in S. Then $\mathrm{Nm}_{K'/K}(\mathfrak{p}') = \mathfrak{p}^{f(\mathfrak{p}'/\mathfrak{p})}$, and we have to show that $\psi_{L/K'}(\mathfrak{p}') = \psi_{L/K}(\mathfrak{p}^{f(\mathfrak{p}'/\mathfrak{p})})$, i.e., that $(\mathfrak{P}, L/K') = (\mathfrak{P}, L/K)^{f(\mathfrak{p}'/\mathfrak{p})}$ for every prime ideal $\mathfrak{P}$ of L lying over $\mathfrak{p}$. But this was proved in 1.10. □

COROLLARY 3.4 *For every finite abelian extension L of K, $\mathrm{Nm}_{L/K}(I_L^S)$ is contained in the kernel of $\psi_{L/K}\colon I^S \to \mathrm{Gal}(L/K)$.*

PROOF. Take $K' = L$ in the above diagram. □

Thus the Artin map induces a homomorphism

$$\psi_{L/K}\colon I_K^S/\mathrm{Nm}(I_L^S) \to \mathrm{Gal}(L/K)$$

whenever L/K is a finite abelian extension. The group $I^S/\mathrm{Nm}(I_L^S)$ is infinite (because infinitely many primes don't split), and so $\psi_{L/K}$ can not be injective.

The main theorems of global class field theory

Let S be a finite set of primes of K. We shall say that a homomorphism $\colon I^S \to G$ **admits a modulus** if there exists a modulus $\mathfrak{m}$ with $S(\mathfrak{m}) \supset S$ such that $(i(K_{\mathfrak{m},1})) = 0$. Thus admits a modulus if and only if it factors through $C_{\mathfrak{m}}$ for some $\mathfrak{m}$ with $S(\mathfrak{m}) \supset S$.

THEOREM 3.5 (RECIPROCITY LAW) *Let L be a finite abelian extension of K, and let S be the set of primes of K ramifying in L. Then the Artin map $\colon I^S \to \mathrm{Gal}(L/K)$ admits a modulus $\mathfrak{m}$ with $S(\mathfrak{m}) = S$, and it defines an isomorphism*

$$I_K^{S(\mathfrak{m})}/i(K_{\mathfrak{m},1}) \cdot \mathrm{Nm}(I_L^{S(\mathfrak{m})}) \to \mathrm{Gal}(L/K).$$

A modulus as in the statement of the theorem is called a **defining modulus for** L. Note that the theorem does not imply that K has even a single nontrivial abelian extension. Write $I_K^{\mathfrak{m}}$ for the group of $S(\mathfrak{m})$-ideals in K, and $I_L^{\mathfrak{m}}$ for the group of $S(\mathfrak{m})'$-ideals in L, where $S(\mathfrak{m})'$ contains

the primes of L lying over a prime in $S(\mathfrak{m})$. Call a subgroup H of $I_K^{\mathfrak{m}}$ a **congruence subgroup modulo** $\mathfrak{m}$ if

$$I_K^{\mathfrak{m}} \supset H \supset i(K_{\mathfrak{m},1}).$$

THEOREM 3.6 (EXISTENCE THEOREM) *For every congruence subgroup H modulo $\mathfrak{m}$, there exists a finite abelian extension L/K, unramified at the primes not dividing $\mathfrak{m}$ such that $H = i(K_{\mathfrak{m},1}) \cdot \mathrm{Nm}_{L/K}(I_L^{\mathfrak{m}})$.*

Note that, for H and L as in the theorem, the Artin map $\ _{L/K}$ induces an isomorphism

$$I^{S(\mathfrak{m})}/H \to \mathrm{Gal}(L/K).$$

In particular, for each modulus $\mathfrak{m}$ there is a field $L_{\mathfrak{m}}$, called the **ray class field modulo** $\mathfrak{m}$ such that the Artin map defines an isomorphism $C_{\mathfrak{m}} \to \mathrm{Gal}(L_{\mathfrak{m}}/K)$. For a field $L \subset L_{\mathfrak{m}}$, set

$$\mathrm{Nm}(C_{L,\mathfrak{m}}) = i(K_{\mathfrak{m},1}) \cdot \mathrm{Nm}(I_L^{\mathfrak{m}}) \mod i(K_{\mathfrak{m},1}).$$

COROLLARY 3.7 *Fix a modulus $\mathfrak{m}$. Then the map $L \mapsto \mathrm{Nm}(C_{L,\mathfrak{m}})$ is a bijection from the set of abelian extensions of K contained in $L_{\mathfrak{m}}$ to the set of subgroups of $C_{\mathfrak{m}}$. Moreover,*

$$\begin{aligned} L_1 \subset L_2 &\iff \mathrm{Nm}(C_{L_1,\mathfrak{m}}) \supset \mathrm{Nm}(C_{L_2,\mathfrak{m}}); \\ \mathrm{Nm}(C_{L_1 \cdot L_2,\mathfrak{m}}) &= \mathrm{Nm}(C_{L_1,\mathfrak{m}}) \cap \mathrm{Nm}(C_{L_2,\mathfrak{m}}); \\ \mathrm{Nm}(C_{L_1 \cap L_2,\mathfrak{m}}) &= \mathrm{Nm}(C_{L_1,\mathfrak{m}}) \cdot \mathrm{Nm}(C_{L_2,\mathfrak{m}}). \end{aligned}$$

REMARK 3.8 Let L/K be an abelian extension with Galois group G. According to the Reciprocity Law, there is a modulus $\mathfrak{m}$ with support the set of primes of K ramifying in L such that the Artin map $\ _{L/K}\colon I^{S(\mathfrak{m})} \to G$ takes the value 1 on $i(K_{\mathfrak{m},1})$. Consider the map in Theorem 1.7

$$(\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^\times \hookrightarrow K_{\mathfrak{m}}/K_{\mathfrak{m},1} \xrightarrow{i} C_{\mathfrak{m}} \xrightarrow{\psi_{L/K}} G.$$

Clearly, there will be a smallest integer $f(\mathfrak{p}) \le m(\mathfrak{p})$ such that this map factors through $(\mathcal{O}_K/\mathfrak{p}^{f(\mathfrak{p})})^\times$. The modulus $\mathfrak{f}(L/K) = \mathfrak{m}_\infty \prod \mathfrak{p}^{f(\mathfrak{p})}$ is then the smallest modulus such that $\ _{L/K}$ factors through $C_{\mathfrak{f}}$—it is called the **conductor**[2] of L/K. The conductor $\mathfrak{f}(L/K)$ is divisible exactly by the primes ramifying in L.

The subfields of the ray class field $L_{\mathfrak{m}}$ containing K are those with conductor $\mathfrak{f}|\mathfrak{m}$.[3] Every abelian extension of K is contained in $L_{\mathfrak{m}}$ for some $\mathfrak{m}$.

---

[2] Fu¨hrer in German—in Germany in the 1930s, conversations in public on class field theory could be hazardous.

[3] Let L be an abelian extension of K whose conductor divides $\mathfrak{m}$. Then the primes that split in $L_{\mathfrak{m}}$ also split in L. Now the Chebotarev density theorem shows that $L \subset L_{\mathfrak{m}}$ (see 3.25 below).

In Section 5 below, we shall restate Theorems 3.5 and 3.6 in terms of ide'les, and in Chapter VII we prove the restated theorems.

As we discuss below, there is a rather simple analytic proof that the Artin map is surjective. Thus the difficulty in proving the Reciprocity Law is in showing that the Artin map admits a conductor and that

$$\left(I^{S(\mathfrak{m})} : i(K_{\mathfrak{m},1}) \cdot \mathrm{Nm}(I_L^{S(\mathfrak{m})})\right) \le [L : K].$$

To prove the Existence Theorem we must construct a ray class field for each modulus. Unfortunately, we don't know how to construct the ray class field directly. Rather we construct enough extensions to force the theorem to be true.

EXAMPLE 3.9 The ray class group for the modulus $\mathfrak{m} = 1$ is the ideal class group, and the corresponding ray class field is the Hilbert class field; it is the maximal abelian extension of K that is unramified at all primes including the real primes (which means that real primes stay real). For example, the Hilbert class field of $\mathbb{Q}$ is $\mathbb{Q}$ itself (because $\mathbb{Q}$ has class number 1). The Hilbert class field of $\mathbb{Q}[\sqrt{-5}]$ is $\mathbb{Q}[\sqrt{-1}, \sqrt{5}]$—both 2 and 5 ramify in $\mathbb{Q}[\sqrt{-5}]$, but only 2 ramifies in $\mathbb{Q}[\sqrt{-1}]$ and only 5 ramifies in $\mathbb{Q}[\sqrt{5}]$, from which it follows that the primes of $\mathbb{Q}[\sqrt{-5}]$ dividing 2 and 5 do not ramify $\mathbb{Q}[\sqrt{-1}, \sqrt{5}]$.

EXAMPLE 3.10 Let m be a positive integer which is odd or divisible by 4. The ray class field for (m) is $\mathbb{Q}[\zeta_m + \bar{\zeta}_m]$, and the ray class field for $\infty(m)$ is $\mathbb{Q}[\zeta_m]$.[4] Thus the Reciprocity Law implies the Kronecker-Weber theorem: every abelian extension of $\mathbb{Q}$ has conductor dividing $\infty(m)$ for some m, and therefore is contained in a cyclotomic field.

EXAMPLE 3.11 Let d be a square-free integer. We compute the conductor of $K = \mathbb{Q}[\sqrt{d}]$ over $\mathbb{Q}$ by finding the smallest integer m such that $\mathbb{Q}[\sqrt{d}] \subset \mathbb{Q}[\zeta_m]$.

First, consider an odd prime p. Then $\mathrm{Gal}(\mathbb{Q}[\zeta_p]/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p-1$, and so has a unique quotient group of order 2. Therefore, $\mathbb{Q}[\zeta_p]$ contains a unique quadratic field, which because it can only be ramified at p, must equal $\mathbb{Q}[\sqrt{p^*}]$, where $p^* = (-1)^{\frac{p-1}{2}} p$ (the sign is chosen so that $p^* \equiv 1 \mod 4$).

Second, note that $\zeta_8 = (1+i)/\sqrt{2}$, and so $\zeta_8 + \bar{\zeta}_8 = \sqrt{2}$. Therefore $\mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}[\zeta_8]$ (in fact, $\mathbb{Q}[\sqrt{2}]$ is the largest real subfield of $\mathbb{Q}[\zeta_8]$, and $\mathbb{Q}[\zeta_8] = \mathbb{Q}[i, \sqrt{2}]$).

Let n be the product of the odd primes dividing d (so $d = \pm n$ or $\pm 2n$). I claim that

$$\begin{array}{lll} \mathbb{Q}[\sqrt{d}] & \subset & \mathbb{Q}[\zeta_n] \text{ if } d \equiv 1 \mod 4, \\ \mathbb{Q}[\sqrt{d}] & \subset & \mathbb{Q}[\zeta_{4n}] \text{ if } d \equiv 3 \mod 4, \\ \mathbb{Q}[\sqrt{d}] & \subset & \mathbb{Q}[\zeta_{8n}] \text{ if } d \equiv 2 \mod 4 \end{array}$$

and that, in each case, this is the smallest cyclotomic field containing $\mathbb{Q}[\sqrt{d}]$. For example, note that $d = p_1 \dots p_r$, $d \equiv 1 \mod 4$, implies that $d = p_1^* \cdots p_r^*$, and so $\mathbb{Q}[\sqrt{d}] \subset \mathbb{Q}[\zeta_n]$. Also note that if d is even, then $\mathbb{Q}[\sqrt{d}]$ is not contained in $\mathbb{Q}[\zeta_{4n}]$ because otherwise $\mathbb{Q}[\zeta_{4n}]$ would contain i, $\sqrt{d}$, $d/2$, and hence would contain i, $\sqrt{2}$, and ζ_8.

We conclude that the conductor of $\mathbb{Q}[\sqrt{d}]$ is $|\Delta_{K/\mathbb{Q}}|$ or $\infty|\Delta_{K/\mathbb{Q}}|$ depending on whether $d > 0$ or $d < 0$—here $\Delta_{K/\mathbb{Q}}$ is the discriminant of $K/\mathbb{Q}$.

---

[4] This follows from the description of the ray class group in 1.8(c) of the notes and the description of the Frobenius element in ANT, 8.18.

REMARK 3.12 For a finite abelian extension L/K and modulus $\mathfrak{m}$ with $S(\mathfrak{m})$ equal to the set of primes of K ramifying in L, let

$$T(L/K, \mathfrak{m}) = i(K_{\mathfrak{m},1}) \cdot \mathrm{Nm}_{L/K}(I_L^{S(\mathfrak{m})}) \subset I_K.$$

Takagi showed that for $\mathfrak{m}$ sufficiently divisible (in fact, for all $\mathfrak{m}$ divisible by the conductor $\mathfrak{f}$ of L/K), the group $T(L/K, \mathfrak{m})$ is independent of $\mathfrak{m}$ and $I_K^{S(\mathfrak{m})}/T(L/K, \mathfrak{m}) \approx \mathrm{Gal}(L/K)$. For this reason, $T(L/K, \mathfrak{m})$ is often called the **Takagi group** of L/K when $\mathfrak{f}|\mathfrak{m}$. Artin showed that the Takagi group is the kernel of the map $\mathfrak{a} \mapsto (\mathfrak{a}, L/K)$: $I_K^{S(\mathfrak{m})} \to \mathrm{Gal}(L/K)$.

EXERCISE 3.13 Compute the conductor of $\mathbb{Q}[\sqrt{d}]/\mathbb{Q}$ by applying the quadratic reciprocity law to find the smallest $\mathfrak{m}$ such that $i(\mathbb{Q}_{\mathfrak{m},1})$ is in the kernel of the Artin map (cf. Exercise 0.11).

The field L corresponding to a congruence subgroup H is called the **class field** of H, whence the name of the subject. Note that for a prime $\mathfrak{p}$ of K not dividing the conductor of L/K, the residue class degree $f(\mathfrak{P}/\mathfrak{p})$ for a prime lying over $\mathfrak{p}$ is the order of $\mathfrak{p}$ in $I^{\mathfrak{m}}/H$ (because this is the order of the Frobenius element in $\mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$). Thus we have obtained a classification of the abelian extensions of K in terms of the ideal structure of K, and for each abelian extension we know the decomposition laws of the primes in K.

Exercise 3.14. Verify the last row in the following table:

Discriminant	-15	-20	-23	-24	-31
Class number	2	2	3	2	3
Hilbert class field	X^2+3	X^2+1	X^3-X-1	X^2+3	X^3+X-1

The first row lists the discriminants of the first five imaginary quadratic fields with class number not equal to 1, the second row lists their class numbers, and the final row lists the minimal polynomial of a generator of the Hilbert class field. (Note that for a totally imaginary field, the class number and the narrow-class number coincide.)

[For example, the quadratic field with discriminant -24 is $\mathbb{Q}[\sqrt{-6}]$, and its Hilbert class field is $L=\mathbb{Q}[\sqrt{-6},\sqrt{-3}]=\mathbb{Q}[\sqrt{2},\sqrt{-3}]$. Thus $L=\mathbb{Q}[\alpha]$ with $\alpha=\sqrt{2}+\sqrt{-3}$, which has minimum polynomial X^4+2X^2+5. However, $\mathbb{Z}[\alpha]$ is not equal to the ring of integers in L; cf. mo122765.]

EXERCISE 3.15 This exercise explains what happens when we ignore a finite set S of prime ideals of K. Let $\mathfrak{m}$ be a modulus of K with $S(\mathfrak{m})\cap S=\emptyset$, and let H be a subgroup of $I^{S\cup S(\mathfrak{m})}$ containing $i(K_{\mathfrak{m},1})$. Define an extension L of K to be an S-class field for H if

(a) L is a finite abelian extension of K, and the prime ideals in S split completely in L;

(b) $\mathfrak{m}(\mathfrak{p})=0\Rightarrow\mathfrak{p}$ does not ramify in L;

(c) the prime ideals not in $S\cup S(\mathfrak{m})$ that split in L are precisely those in H.

Prove that an S-class field L exists for each group H as above, that it is unique, and that $I^{S\cup S(\mathfrak{m})}/H\simeq\mathrm{Gal}(L/K)$; moreover, every field L satisfying (a) is the S-class field for some H.

Hint: Show $I^{S\cup S(\mathfrak{m})}/i(K_{\mathfrak{m},1})\simeq I^{S(\mathfrak{m})}/\langle S\rangle\cdot i(K_{\mathfrak{m},1})$, where $\langle S\rangle$ is the subgroup of $I^{S(\mathfrak{m})}$ generated by the primes in S. *The norm limitation theorem*

In our classification of the abelian extensions of K, we attach to L the group $H=i(K_{\mathfrak{m},1})\cdot\mathrm{Nm}(I_L^{S(\mathfrak{m})})$ for $\mathfrak{m}$ a modulus sufficiently large to be a defining modulus (and then $(I^{S(\mathfrak{m})}:H)=[L:K]$). One might hope that something similar works for nonabelian extensions, but the following theorem shows that it does not.

THEOREM 3.16 (NORM LIMITATION THEOREM) *Let L be a finite extension of K, and let L'/K be the maximal abelian subextension of L/K. For every defining modulus $\mathfrak{m}$ for L'/K,*

$$i(K_{\mathfrak{m},1})\cdot\mathrm{Nm}_{L/K}(I_L^{S(\mathfrak{m})})=i(K_{\mathfrak{m},1})\cdot\mathrm{Nm}_{L'/K}(I_{L'}^{S(\mathfrak{m})}).$$

For example, if L is a cubic extension of K that is not Galois over K, then $L'=K$, and so

$$i(K_{\mathfrak{m},1})\cdot\mathrm{Nm}_{L/K}(I_L^{S(\mathfrak{m})})=I_K^{S(\mathfrak{m})}.$$

The norm limitation theorem indicates that, for a nonabelian extension L/K, $\mathrm{Spl}(L/K)$ is not described by congruence conditions. For a proof of the norm limitation theorem, see, e.g., Grant and Leitzel 1969.

The principal ideal theorem

> *... à ma honte, je ne suis par arrivé à retrouver ce "corollaire" que tous les idéaux de K deviennent principaux dans la plus grande extension abélienne non ramifiée dans le fini. Si ça s'explique en deux mots, je t'en serais fort reconnaissant.*
> Grothendieck, letter to Serre, 19.9.1956.[5]

The following theorem was conjectured by Hilbert about 1900.

THEOREM 3.17 (PRINCIPAL IDEAL THEOREM) *Every ideal in K becomes principal in the Hilbert class field of K.*

I explain the idea of the proof. Recall that for a group G, the **commutator** (or **derived**) subgroup G' of G is the subgroup generated by the commutators $ghg^{-1}h^{-1}$, $g, h \in G$. The quotient $G^{\mathrm{ab}} = G/G'$ is abelian, and it is the largest abelian quotient of G. If L is a Galois extension of K with Galois group G, then $L^{G'}$ is an abelian extension of K with Galois group G^{ab}, and it is the largest abelian extension of K contained in L.

---

[5]. . . to my shame, I have been unable to find the "corollary" stating that all ideals of K become principal in the largest abelian extension unramified at the finite primes. If it can be explained in two words, I would be very grateful to you.

Serre responded: Enclosed is a little paper on the "Hauptidealsatz" explaining how the theorem can be reduced to an (actually very mysterious) theorem in group theory. This, in fact, is the reduction given by Artin himself in his paper on the subject (Abh. Hamburg, around volume 7–10); if you could find a beautiful cohomological proof of the theorem it would be so much better, but everyone has got stuck on it up to now. See also the endnote to Serre's letter (Grothendieck and Serre 2001).

Suppose we have fields

$$L \supset K' \supset K$$

with L Galois over K (not necessarily abelian). For every finite set of primes S of K, $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_{K'}$ is a homomorphism $I_K^S \to I_{K'}^S$. Consider:

$$\begin{array}{ccc} I_K^S & \xrightarrow{\psi_{L/K}} & \mathrm{Gal}(L/K)^{\mathrm{ab}} \\ \downarrow \text{canonical} & & \downarrow ? \\ I_{K'}^S & \xrightarrow{\psi_{L/K'}} & \mathrm{Gal}(L/K')^{\mathrm{ab}}. \end{array}$$

What is the map "?" making the diagram commute?

Before describing it, I need to explain a construction in group theory. Let H be a group of finite index in a group G, and write G as a disjoint union of cosets,

$$G = Hg_1 \cup Hg_2 \cup \ldots \cup Hg_n.$$

For $g \in G$, set $\varphi(g) = g_i$ if $g \in Hg_i$, and define

$$V(g) = \prod_{i=1}^{n} g_i g \varphi(g_i g)^{-1} \mod H',$$

where H' is the commutator subgroup of H.

PROPOSITION 3.18 *The map $g \mapsto V(g)$ is a homomorphism $G \to H/H'$, and it is inde- pendent of the choice of the coset representatives g_i.*

PROOF. The verification is straightforward—see, for example, Hall 1959, 14.2.1. □

Thus, whenever we have a group G and a subgroup H of finite index, we have a welldefined homomorphism

$$V : G^{\mathrm{ab}} \to H^{\mathrm{ab}},$$

called the **Verlagerung** (or **transfer**) map. Roughly speaking, we are trying to define a "norm" from G to H, which doesn't work because the groups are not abelian, but does work when we pass to the associated abelian groups.

In the situation of the above diagram, $\mathrm{Gal}(L/K')$ is a subgroup of $\mathrm{Gal}(L/K)$, and hence the Verlagerung is a homomorphism

$$V\colon \mathrm{Gal}(L/K)^{\mathrm{ab}} \to \mathrm{Gal}(L/K')^{\mathrm{ab}}.$$

Emil Artin showed that this is the map making the above diagram commute (cf. II, 3.2b).

Consider the fields

$$K'' \supset K' \supset K,$$

where K' is the Hilbert class field of K, and K'' is the Hilbert class field of K'. Then

(a) K'' is normal over K (because any conjugate of K'' is again an abelian unramified extension of K', and hence is contained in K'');

(b) K' is the largest abelian extension of K contained in K'' (because every abelian extension of K contained in K'' is unramified over K, and hence is contained in K'). From (b) we find that $\mathrm{Gal}(K''/K)^{\mathrm{ab}} = \mathrm{Gal}(K'/K)$. Therefore, when $L = K''$, the previous diagram becomes

$$\begin{array}{ccc} C_K & \xrightarrow{\simeq} & \mathrm{Gal}(K'/K) \\ \downarrow{\scriptstyle \text{canonical}} & & \downarrow{\scriptstyle \text{Ver}} \\ C_{K'} & \xrightarrow{\simeq} & \mathrm{Gal}(K''/K'), \end{array}$$

where C_K and $C_{K'}$ are the class groups of K and K'. Let $G = \mathrm{Gal}(K''/K)$ and let $H = \mathrm{Gal}(K''/K')$. Because of (b), H is the commutator subgroup of G. The next theorem (which was conjectured by Emil Artin) shows that V is zero in this situation, and hence that the canonical map $C_K \to C_{K'}$ is zero, i.e., that every ideal of K becomes principal in K'.

THEOREM 3.19 *Let G be a finite group, and let H be its commutator subgroup; then*

$$V\colon G^{\mathrm{ab}} \to H^{\mathrm{ab}}$$

is zero.

PROOF. This is a theorem in group theory, also called the Principal Ideal Theorem. It was proved by Furtwa¨ngler in 1930. For a simple proof, see: Witt, Proc. International Congress of Mathematicians, Amsterdam, 1954, Vol 2, pp. 71–73. Also Zassehaus, Theory of Groups, V, Theorem 12, or Artin and Tate 1961, Chapter XII. □

REMARK 3.20 It is in fact easy to see that there exists an extension L of K of degree dividing the class number h of K such that every ideal in K becomes principal in L: write the class group of K as a direct sum of cyclic groups; choose a generator $\mathfrak{a}_i$ for each summand, and let h_i be the order of $\mathfrak{a}_i$ in the class group; write $\mathfrak{a}_i^{h_i} = (a_i)$, and define L to be the field obtained from K by adjoining an h_ith root of a_i for each i.

However, a field constructed in this fashion will not usually be the Hilbert class field of K—it need not even be Galois over K. There may exist fields of degree $< h$ over K in which every ideal in K becomes principal.

REMARK 3.21 Note that the principal ideal theorem says that "ideal" factorizations of elements in K become actual factorizations in the Hilbert class field L: let $a \in K$, and let $(a) = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_s^{r_s}$; then $\mathfrak{p}_i \mathcal{O}_L = (\pi_i)$ for some $\pi_i \in \mathcal{O}_L$, and so $a = u\pi_1^{r_1} \cdots \pi_s^{r_s}$ in $\mathcal{O}_L$.

REMARK 3.22 The principal ideal theorem does not, of course, imply that every ideal in the Hilbert class field K' of K is principal, because not every ideal of K' is in the image of the homomorphism $I_K \to I_{K'}$. One can form the Hilbert class field K'' of K', and so on, to obtain a tower

$$K \subset K' \subset K'' \subset \cdots \subset K^{(n)} \subset \cdots$$

in which $K^{(n+1)}$ is the Hilbert class field of $K^{(n)}$. For every automorphism of K^{al}, $\tau K^{(n+1)}$ is obviously the largest abelian unramified extension of $\tau K^{(n)}$, which implies that $\tau K' = K$, $\tau K'' = K''$, etc., and so on. In particular, $K^{(n)}$ is Galois over K. The class field tower problem (stated by Hasse in 1925) asks whether this tower is always finite, and so terminates in a field with class number one. The answer was shown to be negative by Golod and Shafarevich in 1964 (see Roquette 1967). For example, $\mathbb{Q}[\sqrt{-2.3.5.7.11.13}]$ has infinite class field. In fact, $\mathbb{Q}[\sqrt{d}]$ has an infinite class field tower whenever d has more than 8 prime factors. *The Chebotarev Density Theorem*

Let L be a Galois extension of K with Galois group G. Recall that, for every prime ideal $\mathfrak{p}$ of K unramified in L,

$$(\mathfrak{p}, L/K) \stackrel{\text{def}}{=} \{(\mathfrak{P}, L/K) \mid \mathfrak{P}|\mathfrak{p}\}$$

is a conjugacy class in G.

THEOREM 3.23 (CHEBOTAREV DENSITY THEOREM) *Let L/K be a finite extension of number fields with Galois group G, and let C be a conjugacy class in G. Then the set of prime ideals of K such that $(\mathfrak{p}, L/K) = C$ has density $|C|/|G|$ in the set of all prime ideals of K. In particular, if G is abelian, then, for a fixed $\tau \in G$, the set of prime ideals $\mathfrak{p}$ of K with $(\mathfrak{p}, L/K) = \tau$ has density $1/(G:1)$.*

PROOF. For an abelian extension L/K this follows from Theorem 2.5 and Theorem 3.5: the latter says that the map $\mathfrak{p} \mapsto (\mathfrak{p}, L/K)$ induces a surjective homomorphism $C_{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ for some modulus $\mathfrak{m}$, and the former says that the primes are equidistributed among the classes in $C_{\mathfrak{m}}$. The nonabelian case is derived from the abelian case by an ingenious argument—see Chapter VIII □

COROLLARY 3.24 *If a polynomial $f(X) \in K[X]$ splits into linear factors modulo $\mathfrak{p}$ for all but finitely prime ideals $\mathfrak{p}$ in K, then it splits in $K[X]$.*

PROOF. Apply the theorem to the splitting field of $f(X)$. □

For a finite extension L/K of number fields and a finite set S of primes of K, let $\mathrm{Spl}_S(L/K)$ be the set of primes of K not in S that split in L.

THEOREM 3.25 *If L and M are Galois extensions of K, then*

$$L \subset M \iff \mathrm{Spl}_S(L/K) \supset \mathrm{Spl}_S(M/K).$$

Hence

$$L = M \iff \mathrm{Spl}_S(L/K) = \mathrm{Spl}_S(M/K).$$

PROOF. As a consequence of (1.12),

$$\mathrm{Spl}_S(LM/K) = \mathrm{Spl}_S(L/K) \cap \mathrm{Spl}_S(M/K).$$

Hence

$\mathrm{Spl}_S(L/K) \supset \mathrm{Spl}_S(M/K) \Rightarrow \mathrm{Spl}_S(LM/K) = \mathrm{Spl}_S(M/K)$,

which, by the Chebotarev density theorem, implies

$$[LM : K] = [M : K],$$

and so $L \subset M$. The reverse implication is obvious. □

REMARK 3.26 (a) Theorem 3.25 is not true without the Galois assumption (see Cassels and Fro¨hlich 1967, p. 363).

(b) In the statement of Theorem 3.25, S can be replaced by any set of primes of density 0.

(c) Let $f(X)$ be an irreducible polynomial in $K[X]$. If $f(X)$ has a root modulo $\mathfrak{p}$ for almost all prime ideals $\mathfrak{p}$, then $f(X)$ has a root in K (Cassels and Fro¨hlich 1967, p. 363, 6.2).

(d) Chebotarev proved his theorem using Dirichlet (analytic) densities. Artin noted that it should hold for natural densities (see later), and, in fact, it does.

(e) Given a finite Galois extension K of $\mathbb{Q}$ and a conjugacy class C, Chebotarev's theorem says that there exists a prime ideal $\mathfrak{p}$ of K, unramified over $\mathbb{Q}$, such that $(\mathfrak{p}, L/K) = C$. It is interesting to know how big $\mathbb{N}\mathfrak{p}$ has to be. For a recent paper on this question, see Ahn, Jeoung-Hwan; Kwon, Soun-Hi. An explicit upper bound for the least prime ideal in the Chebotarev density theorem. Ann. Inst. Fourier (Grenoble) 69 (2019), no. 3, 1411–1458.

The conductor-discriminant formula

Two **Dirichlet characters** $\chi\colon I^S \to \mathbb{C}^\times$ and $\chi'\colon I^{S'} \to \mathbb{C}^\times$ are said to be **cotrained** if they agree on $I^{S''}$ for some $S'' \supset S \bigcup S'$. This is an equivalence relation. In each equivalence class, there is a unique with smallest S—such a is said to be **primitive.**

Let χ_1 be the primitive character equivalent to . The smallest modulus $\mathfrak{m}$ such that χ_1 is zero on $i(K_{\mathfrak{m},1})$ is called the **conductor** of $\mathfrak{f}(\chi)$ of . Set $\mathfrak{f}(\chi) = \mathfrak{f}_\infty(\chi)\mathfrak{f}_0(\chi)$, where $\mathfrak{f}_\infty$ and $\mathfrak{f}_0$ are respectively divisible only by infinite primes and finite primes.

THEOREM 3.27 (F U¨HRERDISKRIMINANTENPRODUKTFORMEL) *For every finite abelian extension L/K of number fields with Galois group G,*

$$\mathrm{disc}(L/K) = \prod_{\chi \in G^\vee} \mathfrak{f}_0(\chi \circ \psi_{L/K}), \quad G^\vee \stackrel{\text{def}}{=} \mathrm{Hom}(G, \mathbb{C}^\times);$$
$$\mathfrak{f}(L/K) = \mathrm{lcm}_\chi \left(\mathfrak{f}(\chi \circ \psi_{L/K})\right).$$

Clearly $\bigcap \mathrm{Ker}(\chi\colon G \to \mathbb{C}^\times) = 0$, from which the second statement follows. We omit the proof of the first—it is really a statement about local fields.

REMARK 3.28 Let H be the kernel of the character . Then $\mathfrak{f}(\chi) = \mathfrak{f}(L^H/K)$. For example, if is injective, then $\mathfrak{f}(\chi) = \mathfrak{f}(L/K)$.

EXAMPLE 3.29 Let $L = \mathbb{Q}[\sqrt{d}]$. Then $G \simeq \mathbb{Z}/2\mathbb{Z}$, and there are only two characters $G \to \mathbb{C}^\times$, namely, the trivial character χ_0 an an injective character χ_1. Therefore, the theorem says that $\Delta_{K/\mathbb{Q}} = \mathfrak{f}_0(\chi_1) = \mathfrak{f}_0(K/\mathbb{Q})$, as we showed in Example 3.11.

EXAMPLE 3.30 Let $L = \mathbb{Q}[\zeta_p]$, p an odd prime. Then $G \simeq (\mathbb{Z}/p\mathbb{Z})^\times$, which is cyclic of order $p-1$. It therefore has $p-2$ nontrivial characters. If is nontrivial, then $\mathfrak{f}(\chi)|\infty(p)$, but $\mathfrak{f}(\chi) = 1$ or ∞ is impossible (because it would imply is trivial). Therefore, $\mathfrak{f}(\chi) = (p)$ or $\infty(p)$ if is nontrivial, and so the conductor-discriminant formula shows (correctly) that $\Delta_{L/\mathbb{Q}} = \pm p^{p-2}$.

EXERCISE 3.31 Verify the conductor-discriminant formula for the extension $\mathbb{Q}[\zeta_{p^2}]/\mathbb{Q}$.

REMARK 3.32 Let L/K be a finite extension of number fields with Galois group G (not necessarily abelian). To a representation $\rho\colon G \to \mathrm{GL}(V)$ of G on a finite-dimensional vector space V , Artin

attaches a Dirichlet L-series $L(s,\rho)$ (see the introduction). The analytic properties of these **Artin L-series** are still not fully understood.

When G is commutative, the Artin map $I^S \to G$ identifies characters of G with Dirichlet/Weber characters, and hence Artin L-series with Dirichlet L-series. This was Artin's motivation for seeking the map (not, as seems natural today, in order to construct a *canonical* isomorphism between the groups $C_{\mathfrak{m}}$ and G, already known to be abstractly isomorphic).

A part of Langlands's philosophy is a vast generalization of this correspondence between Dirichlet L-series and abelian Artin L-series.

The reciprocity law and power reciprocity

Assume K contains a primitive nth root of 1, and let $a \in K$. If $\sqrt[n]{a}$ is one root of $X^n - a$, then the remaining roots are of the form $\zeta\sqrt[n]{a}$, where ζ is an nth root of 1. Therefore

then the remaining roots are of the form $\zeta\sqrt[n]{a}$,

def $L \overset{\text{def}}{=} K[\sqrt[n]{a}]$ is Galois over K, and $\sigma\sqrt[n]{a} = \zeta\sqrt[n]{a}$ for some nth root ζ of 1.

If $\mathfrak{p}$ is a prime ideal of K that is relatively prime to n and a, then $\mathfrak{p}$ is unramified in L, and we can define an nth root $(\frac{a}{\mathfrak{p}})_n$ of 1 by the formula

$$(\mathfrak{p}, L/K)(\sqrt[n]{a}) = \left(\frac{a}{\mathfrak{p}}\right)_n \sqrt[n]{a}.$$

One can show that

$$\left(\frac{a}{\mathfrak{p}}\right)_n = 1 \iff a \text{ is an } n\text{th power modulo } \mathfrak{p},$$

Thus $\left(\frac{a}{\mathfrak{p}}\right)_n$ generalizes the quadratic residue symbol and is called the *nth power residue symbol*. Artin's reciprocity law implies all known reciprocity laws for these symbols. As Artin pointed out, it can therefore be viewed as a generalization of them to fields without roots of unity. We shall explain this in Chapter VIII of the source.

An elementary unsolved problem

Let K be a number field, let S be a nonempty finite set of prime ideals of K, and let p be a prime number not divisible by any prime in S. Does there exist a sequence of fields $\dots, L_n, L_{n+1}, \dots$ such that

(a) L_n is unramified outside the primes of S;

(b) $p^n | [L_n : K]$?

A key case, for which the answer is unknown, is $K = \mathbb{Q}$ and $S = \{l\}$. More explicitly (and slightly harder), fix primes $p \neq l$ in $\mathbb{Q}$. Does there exist a sequence of monic irreducible polynomials $f_n(X) \in \mathbb{Z}[X]$ such that

(a) $\operatorname{disc}(f_n(X))$ is not divisible by any prime other than l;

(b) $p^n | \deg f_n(X)$.

See Milne 2006, pp. 48–49, to find where this problem turned up. It is certainly very difficult.[6]

[6]Let K be a number field, let S be a set of primes of K, and let K_S be the largest extension of K unramified outside S. Let P be the set of prime numbers ℓ such that $\ell^\infty | [K_S : K]$. It is now known that P contains *all* prime numbers provided that S contains all the prime ideals of K lying over at least two primes in $\mathbb{Q}$. See Chenevier and Clozel, JAMS 22 (2009), 467–519, Cor. 5.2.

Explicit global class field theory: Kronecker's Jugentraum and Hilbert's twelfth problem

Unlike local class field theory, global class field theory does not (in general) provide an explicit construction of the abelian extensions of a number field K.

Gauss knew that the cyclotomic extensions of $\mathbb{Q}$ are abelian. Towards the end of the 1840s Kronecker had the idea that the cyclotomic fields, and their subfields, exhaust the abelian extensions of $\mathbb{Q}$, and furthermore, that every abelian extension of an imaginary quadratic number field E is contained in the extension given by adjoining to E roots of 1 and certain special values of the modular function j. Many years later he was to refer to this idea as the most cherished dream of his youth (mein liebster Jugendtraum).

More precisely, Kronecker's dream[7] is that every abelian extension of $\mathbb{Q}$ is contained in the field obtained by adjoining to $\mathbb{Q}$ all values of the function $e^{2\pi iz}$ for $z \in \mathbb{Q}^\times$, and that every abelian extension of an imaginary quadratic field K is contained in the field obtained by adjoining to K all values of the function $j(z)$ for $z \in K^\times$.

Later Hilbert took this up as the twelfth of his famous problems: for any number field K, find functions that play the same role for K that the exponential function plays for $\mathbb{Q}$ and the modular function j plays for an imaginary quadratic field[8]. The first part of Kronecker's dream, that every abelian extension of $\mathbb{Q}$ is a subfield of a cyclotomic extension, was proved by Weber (1886, 1899, 1907, 1911) and Hilbert (1896).

The statement above of "Kronecker's dream" is not quite correct. Let K be an imaginary quadratic field. We can write $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\tau$ with $\Im(\tau) > 0$. It is known that $K[j(\tau)]$ is the Hilbert class field of K. Now adjoin to K all roots of unity and all values $j(\tau)$ with $\tau \in K$, $\Im(\tau) > 0$. The resulting field K' is abelian over K, and $[K^{\mathrm{ab}} : K']$ is product of groups of order 2. To get the whole of K^{ab}, it is necessary to adjoin special values of other elliptic functions. These statements were partially proved Weber (1908) and Feuter (1914), and completely proved by Takagi (1920).

From the modern point of view, special values of elliptic modular functions are related to the arithmetic of elliptic curves with complex multiplication, and it is results about the latter that allow one to prove that the former generate abelian extension of an imaginary quadratic field.

Beginning with the work of Taniyama, Shimura, and Weil in the late fifties, the theory of elliptic curves and elliptic modular curves has been successfully generalized to higher dimensions. In this theory, an elliptic curve with complex multiplication by an imaginary quadratic field is replaced by an abelian variety with complex multiplication by a CM field, that is, a quadratic totally imaginary extension K of a totally real field F , and an elliptic modular function by an automorphic function.

Philosophically, one expects that, with the exception of $\mathbb{Q}$, one can not obtain abelian extensions of totally real fields by adjoining special values of automorphic functions. However, it is known that, roughly speaking, one does obtain the largest possible abelian extension of a CM-field K consistent with this restriction.

More precisely, let K be a CM-field and let F be the largest totally real subfield of def $^{\mathrm{al}}/K)$ is a subgroup of index 2 in G' def $_{\mathrm{al}}$ K. Then $G \overset{\mathrm{def}}{=} \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/K)$ is a subgroup of index 2 in $G' \overset{\mathrm{def}}{=} \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/F)$, and the corresponding Verlagerung is a homomorphism $V : G'^{\mathrm{ab}} \to G^{\mathrm{ab}}$. In this case, V has a very simple description.

---

[7]For a careful account of Kronecker's idea and work on it, see Schappacher 1998 [8]See pp. 18-20 of Mathematical Developments arising from Hilbert's Problems, Proc. Symp. Pure Math. XXVIII, Part 1, AMS, 1976.

THEOREM 3.33 *Let K be a CM-field, and let F be the totally real subfield of K with $[K : F] = 2$. Let H be the image of the Verlagerung map*

$$\mathrm{Gal}(F^{\mathrm{al}}/F)^{\mathrm{ab}} \to \mathrm{Gal}(K^{\mathrm{al}}/K)^{\mathrm{ab}}.$$

Then the extension of K obtained by adjoining the special values of all automorphic func- tions defined on canonical models of Shimura varieties with rational weight is $(K^{\mathrm{ab}})^{H}\cdot\mathbb{Q}^{\mathrm{ab}}$.

PROOF. See Wei 1993, Wei 1994. □

Notes

The relation between congruence groups and abelian extensions of K was known before Artin defined his map. It emerged only slowly over roughly the period 1870–1920. The main contributors were Kronecker, Weber, Hilbert, and Takagi. Chebotarev proved his theorem in (1926) (a less precise result had been proved much earlier by Frobenius), and Artin defined his map and proved it gave an isomorphism in 1927. (Earlier, it had been known that $I^{\mathfrak{m}}/H \approx \mathrm{Gal}(L/K)$, but no *canonical* isomorphism was known.) The fact that analysis, in the form of Chebotarev's (or Frobenius's) theorem was required to prove the main theorems, which are purely algebraic in form, was regarded as a defect, and in 1940, after much effort, Chevalley succeeded in giving a purely algebraic proof of the main

theorems. (The difficult point is proving that if L/K is an abelian extension of number fields of prime degree p, then *at least one* prime of K does not split or ramify in L.[9]) He also introduced ide'les, which make it possible to state class field theory directly for infinite extensions. Group cohomology (at least 2-cocycles etc.) had been used implicitly in class field theory from the 1920s, but it was used systematically by Nakayama, Hochschild, and Tate in the 1950s. In 1951/52 in a very influential seminar, Artin and Tate gave a purely algebraic and very cohomological treatment of class field theory. Since then there have been important improvements in our understanding of local class field theory (mainly due to Lubin and Tate). Nonabelian class field theory is a part of Langlands's program, which is a vast interlocking series of conjectures, and some progress has been made, especially in the local case and the function field case. A fairly satisfactory abelian class field theory for more general fields (fields of finite transcendence degree over $\mathbb{Q}$ or $\mathbb{F}_p$) has been created by Bloch, Kato, Saito, and others. It uses algebraic K-theory (see Raskind 1995 for a survey and Wiesend 2007 for a recent result).

4 Idèles

Theorems 3.5 and 3.6 show that, for any number field K, there is a canonical isomorphism $\varprojlim_{\mathfrak{m}} C_{\mathfrak{m}} \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$. Rather than studying $\varprojlim_{\mathfrak{m}} C_{\mathfrak{m}}$ directly, it turns out to be more natural to introduce another group that has it as a quotient—this is the ide'le class group.

---

[9] Class field theory holds also for fields that are finite extensions of $k(X)$ with k finite, and local class field theory holds for local fields whose residue fields k are only quasi-finite, i.e., perfect with $\mathrm{Gal}(k^{\mathrm{al}}/k) \simeq \hat{\mathbb{Z}}$. When one tries to do global class field theory for finite extensions of $k(X)$ with k *quasi-finite*, one finds that everything works except that, for some k, there *do* exist nontrivial abelian extensions in which every prime splits. See my book, Arithmetic Duality Theorems, Appendix to Chapter I.

Topological groups

A group G with a topology is called a **topological group** if the maps

$$g, g' \mapsto gg' : G\times G \to G, \quad g \mapsto g^{-1} : G \to G$$

are continuous. The translation map

$$g \mapsto ag : G \to G$$

is then a homeomorphism.

In general, to determine a topology on a set we have to give a fundamental system of neighbourhoods of each point, i.e., a set of neighbourhoods of the point such that every neighbourhood

contains one in the set. Because the translation map is a homeomorphism, the topology on a topological group is determined by a fundamental system of neighbourhoods of 1.

We shall need to make use of various generalities concerning topological groups, which can be found in many books. Fortunately, we shall only need quite elementary things.

Le t $(X_i)_i$ be a (possibly infinite) family of top ological spaces. The product topology on $\prod X_i$ is that for which the sets of the form $\prod U_i$, U_i open in X for all i and equal to X_i for all but finitely many i, form a basis. Tychonoff's theorem says that a product of compact spaces is compact. However, an infinite product of locally compact spaces will not in general be locally compact: if V_i is a compact neighbourhood of x_i in X_i for all i, then $\prod V_i$ will be compact, but it will not be a neigbourhood of (x_i) unless $V_i = X_i$ for all but finitely many i.

Ide'les

We now often write v for a prime of K. Then:

$|\cdot|_v$ = the normalized absolute value for v (for which the product formula holds), K_v = the completion of K at v, $\mathfrak{p}_v$ = the corresponding prime ideal in $\mathcal{O}_K$, (when v is finite), $\mathcal{O}_v$ = the ring of integers in K_v,

$$U_v = \mathcal{O}_v^\times$$

$\hat{\mathfrak{p}}_v$ = the completion of $\mathfrak{p}_v$ = maximal ideal in $\mathcal{O}_v$.

Recall that, for all v, K_v is locally compact—in fact, $\mathcal{O}_v$ is a compact neighbourhood of 0. Similarly $K_v^\times$ is locally compact; in fact

$$1 + \hat{\mathfrak{p}}_v \supset 1 + \hat{\mathfrak{p}}_v^2 \supset 1 + \hat{\mathfrak{p}}_v^3 \supset \cdots$$

is a fundamental system of neighbourhoods of 1 consisting of open compact subg roups.

We want to combine all the groups $K_v^\times$ into one big topological space, but $\prod K_v^\times$ is not locally compact. Instead we define the **group of ide'les** to be[10]

$$\mathbb{I}_K = \{(a_v) \in \prod K_v^\times \mid a_v \in \mathcal{O}_v^\times \text{ for all but finitely many } v\}.$$

[10]Other notations for the ide'les: $\mathbb{A}_K^\times$, $\mathrm{GL}_1(\mathbb{A}_K)$. In the following, an unadorned $\mathbb{I}$ means $\mathbb{I}_K$.

For every finite set S of primes that includes all infinite primes, let

$$\mathbb{I}_S = \prod_{v \in S} K_v^\times \times \prod_{v \notin S} \mathcal{O}_v^\times$$

with the product topology. The first factor is a finite product of locally compact spaces, and so is locally compact, and the second factor is a product of compact spaces, and so is compact (by Tychonoff). Hence $\mathbb{I}_S$ is locally compact. Note that

$$\mathbb{I} = \bigcup \mathbb{I}_S.$$

We want to endow $\mathbb{I}$ with a topology such that each $\mathbb{I}_S$ is open in $\mathbb{I}$ and inherits the product topology. We do this by decreeing that a basis for the open sets consists of the sets of the form $\prod_v V_v$ with V_v open in $K_v^\times$ for all v and $V_v = \mathcal{O}_v^\times$ for almost all[11] v. An intersection of two sets of this form contains a set of this form, and so they do form a basis for a topology. It is clear that the topology does have the property we want, and moreover that it endows $\mathbb{I}$ with the structure of a topological group. The following sets form a fundamental system of neighbourhoods of 1: for each finite set of primes $S \supset S_\infty$ and $\varepsilon > 0$, define

$$U(S, \varepsilon) = \{(a_v) \mid |a_v - 1|_v < \varepsilon, \quad v \in S, \quad |a_v|_v = 1, \quad \text{all } v \notin S\}.$$

4.1 There is a canonical surjective homomorphism id

$$(a_v) \mapsto \prod_{v \text{ finite}} p_v^{\operatorname{ord}_p(a_v)} : \mathbb{I}_K \to I_K$$

whose kernel is $\mathbb{I}_{S_\infty}$.

We can think of the ide'les as a thickening of the ideals: it includes factors for the infinite primes, and it includes the units at the finite primes. Note that $\mathbb{I}/\mathbb{I}_{S_\infty}$ is a direct sum of countably many copies of $\mathbb{Z}$ with the discrete topology, but that $\prod \tilde{K_v^\times}/\mathbb{I}_{S_\infty}$ is a direct *product* of countably many copies of $\mathbb{Z}$, which is itself uncountable.

4.2 There is a canonical injective (diagonal) homomorphism

$$a \mapsto (a, a, a, \ldots) : K^\times \to \mathbb{I}_K.$$

I claim that the image is discrete. Because we have groups, it suffices to prove that $1 \in K^\times$ is open in the induced topology. Let $U = U(S, \varepsilon)$ with S any finite set containing S_∞ and $1 > \varepsilon > 0$. For every $a \in K^\times \cap U$,

$$\begin{cases} |a-1|_v < \varepsilon & \text{for all } v \in S \\ |a|_v = 1 & \text{for all } v \notin S. \end{cases}$$

The second condition implies that

$$|a-1|_v \leq \max(|a|_v, |-1|_v) \leq 1.$$

Therefore, if $a \in K^\times \cap U$, then $\prod_v |a-1|_v < \varepsilon^{|S|} < 1$, which contradicts the product formula unless $a = 1$.

---

[11] Here "almost all" means "for all but possibly finitely many".

The quotient $\boldsymbol{C} = \mathbb{I}/K^\times$ is called the **ide'le class group** of K. It maps onto the ideal class group of K. It is not compact (see (4.4) below).

4.3 There is a canonical injective homomorphism

$$a \mapsto (1, \ldots, 1, a, 1, \ldots 1) : K_v^\times \to \mathbb{I}_K$$

(a in the vth place). The topology induced on $K_v^\times$ is its natural topology, because

$$U(S, \varepsilon) \cap K_v^\times = \begin{cases} \{a \mid |a-1|_v < \varepsilon\} & v \in S \\ \{a \mid |a|_v = 1\} & v \notin S \end{cases}$$

and such sets form a fundamental system of neighbourhoods of 1 in $K_v^\times$.

4.4 There is canonical surjective homomorphism

$$\mathbf{a} = (a_v) \mapsto c(\mathbf{a}) = \prod |a_v|_v : \mathbb{I} \to \mathbb{R}_{>0}.$$

The image of $\mathbf{a}$ is called the **content** of $\mathbf{a}$. Define

$$\mathbb{I}^1 = \operatorname{Ker}(c) = \{\mathbf{a} \in \mathbb{I} \mid c(\mathbf{a}) = 1\}.$$

Note that, because of the product formula, $K^\times \subset \mathbb{I}^1$. The quotient $\mathbb{I}/K^\times$ can't be compact because it maps surjectively onto $\mathbb{R}_{>0}$, but one can prove that $\mathbb{I}^1/K^\times$ is compact.

ASIDE 4.5 Define $\mathbb{I}_f$ the same way as $\mathbb{I}$, except using only the finite primes. We call $\mathbb{I}_f$ the **group of finite ideʻles.** We have

$$\prod_{v \text{ finite}} \mathcal{O}_v^\times \subset \mathbb{I}_f \subset \prod_{v \text{ finite}} K_v^\times.$$

The subgroup $\prod \mathcal{O}_v^\times$ is open and compact in $\mathbb{I}_f$, and $\mathbb{I}_f / \prod \mathcal{O}_v^\times = I$ (the group of ideals of K).

Again there is a diagonal embedding of $K^\times$ into $\mathbb{I}_f$, but this time the induced topology on $K^\times$ has the following description: $U_K \overset{\text{def}}{=} \mathcal{O}_K^\times$ is open, and a fundamental system of neighbourhoods of 1 is formed by the subgroups of U_K of finite index (nontrivial theorem).[12] In particular, $K^\times$ is a discrete subgroup of $\mathbb{I}_f \iff U_K$ is finite $\iff K = \mathbb{Q}$ or an imaginary quadratic field.

NOTES The adeʻlic topology does not induce the ideʻlic topology on the ideʻles (because $\prod_{v|\infty} K_v^\times \times \prod_{v \text{ finite}} \mathcal{O}_v^\times$ is not open in the adeʻles). As an exercise, show that the ideʻles are not even a topological

finite v group under the induced topology. (Consider first the case of $\mathbb{Q}$, and forget about the infinite prime. (a) Make sure you understand what the standard basis for the neighbourhoods of 0 in the adeʻles is. (b) Translate the neighbourhoods in (a) by adding 1, and intersect with the ideʻles to get a base for the neighbourhoods of 1 in the ideʻles for the adelic topology. (c) Check that the pre-image of one of the neighbourhoods in (b) under the map $x \mapsto x^{-1}$ is not open.)

---

[12] Copied from sx140729. For the first claim: The subset of the finite ideʻles given by $\prod_v \mathcal{O}_{K_v}^\times$ is open by the definition of the topology on the restricted direct product, and an element in $K^\times$ is in this subset if and only if it is a unit in each completion, which is true if and only if it is in $\mathcal{O}_K^\times$.

The proof of the second claim is just a generalization of this first argument. A basis of open neighborhoods of 1 in the finite idèles is given by choosing any open subgroup you wish in $K_v^\times$ for finitely many primes v and choosing $\mathcal{O}_v^\times$ for the remaining v. If we just want a basis of open subsets, we may as well only look at really small ones, so we can assume that, for the finitely many primes v where we did not choose $\mathcal{O}_v^\times$, we chose some small open subset of $\mathcal{O}_v^\times$. Note that subgroups of $\mathcal{O}_v^\times$ are all finite index and generated by a power of a prime element. Note also that all these open subsets of the ideʻles are subsets of the one we discussed in checking the first claim.

What happens when we intersect such a neighbourhood with the diagonal image of $K^\times$? We get the subgroup of elements in $\mathcal{O}_K^\times$ which are in all the open subgroups of $\mathcal{O}_v^\times$ that we chose at the special places v. The index is just the product of the indices of those subgroups, so that's a finite index subgroup. Conversely, any finite index subgroup of $\mathcal{O}_K^\times$ is determined by its images in each completion.

NOTES Let $(V_v, U_v)_v$ be a family of topological spaces V_v, each equipped with a subspace U_v. The **restricted product** of the family, $\prod(V_v, U_v)$, is the subset of $\prod V_v$ consisting o f the families (a_v) such that $a_v \in U_v$ for almost all v.It is equipped with the topology for which $\prod U_v$ is open and has the product topology. Sometimes the restricted product is written $\prod' V_v$. Now $\mathbb{A}_K = \prod_v (K_v, U_v)$, where $U_v = \mathcal{O}_v$ if v is finite and $U_v = K_v$ otherwise. Similarly, $\mathbb{A}_K^\times = \prod_v (K_v^\times, U_v^\times)$, where $U_v = \mathcal{O}_v^\times$ if v is finite and $U_v = K_v^\times$ otherwise.

NOTES Give more examples. Let K be a field with class number 1. Let $x = (x_v)$ be an ideʻle. Then the ideal of x is principal, say, equal to (a). Now $x/a \in \prod_{\text{finite}} \mathcal{O}_v^\times \times K_\infty^\times$. Hence $\mathbb{A}_K^\times =$

$$\prod \mathcal{O}_v^\times \times K_\infty^\times. \text{ However, } K^\times \cap \Big(\prod$$

$K^\times \cdot \prod_{\text{finite}} \mathcal{O}_v^\times \times K_\infty^\times$. However, $K^\times \cap (\prod_{\text{finite}} \mathcal{O}_v^\times \times K_\infty^\times) = U_K$.

NOTES Copied from sx80763. Question from Princeton's generals: What results do the major compactness theorems about adeles and ideles imply? Answer: The finiteness of the ideal class group and the units theorem (proven with classical methods) prove the compactness of the norm one ideʻle class group, and the compactness of the norm-one ideʻle class group, proven using measure theoretic methods proves finiteness of the ideal class group and the units theorem. (See Cassels 1967.) On the other hand, the compactness result does generalize to division algebras,

where there is not an obvious version of the ideal class group, etc. (See Weil's Basic Number Theory.)

Realizing ray class groups as quotients of $\mathbb{I}$

We have seen that the class group $C_K = I/i(K^\times)$ can be realized as the quotient of $\mathbb{I}$. We want to show the same for $C_\mathfrak{m}$.

Let $\mathfrak{m}$ be a modulus. For $\mathfrak{p}|\mathfrak{m}$, set

$$W_\mathfrak{m}(\mathfrak{p}) = \begin{cases} \mathbb{R}_{>0} & \mathfrak{p} \text{ real} \\ 1 + \hat{\mathfrak{p}}^{m(\mathfrak{p})} & \mathfrak{p} \text{ finite.} \end{cases}$$

Thus, in each case, $W_\mathfrak{m}(\mathfrak{p})$ is a neighbourhood of 1 in $K_\mathfrak{p}^\times$.

Define $\mathbb{I}_\mathfrak{m}$ to be the set of ide'les $(a_\mathfrak{p})_\mathfrak{p}$ such that $a_\mathfrak{p} \in^r W_\mathfrak{m}(\mathfrak{p})$ for all $\mathfrak{p}|\mathfrak{m}$:

$$\mathbb{I}_\mathfrak{m} = \left(\prod_{\mathfrak{p}\nmid\mathfrak{m}} K_\mathfrak{p}^\times \times \prod_{\mathfrak{p}|\mathfrak{m}} W_\mathfrak{m}(\mathfrak{p}) \right) \bigcap \mathbb{I}.$$

In other words, $\mathbb{I}_\mathfrak{m}$ consists of the families $(a_\mathfrak{p})_\mathfrak{p}$ indexed by the primes of K such that

$$\begin{cases} a_\mathfrak{p} \in K_\mathfrak{p}^\times & \text{for all } \mathfrak{p} \\ a_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^\times & \text{for almost all } \mathfrak{p} \\ a_\mathfrak{p} \in W_\mathfrak{m}(\mathfrak{p}) & \text{for all } \mathfrak{p}|\mathfrak{m}. \end{cases}$$

Define $W_\mathfrak{m}$ to be the set of ide'les $(a_\mathfrak{p})_\mathfrak{p}$ in $\mathbb{I}_\mathfrak{m}$ such that $a_\mathfrak{p}$ is a unit for all finite $\mathfrak{p}$ not dividing $\mathfrak{m}$:

$$W_\mathfrak{m} = \coprod_{\substack{\mathfrak{p}\nmid\mathfrak{m} \\ \mathfrak{p} \text{ infinite}}} K_\mathfrak{p}^\times \times \coprod_{\mathfrak{p}|\mathfrak{m}} W_\mathfrak{m}(\mathfrak{p}) \times \coprod_{\substack{\mathfrak{p}\nmid\mathfrak{m} \\ \mathfrak{p} \text{ finite}}} U_\mathfrak{p}.$$

In other words, $W_\mathfrak{m}$ consists of the families $(a_\mathfrak{p})_\mathfrak{p}$ indexed by the primes of K such that

$$\begin{cases} a_\mathfrak{p} \in K_\mathfrak{p}^\times & \text{for all infinite } \mathfrak{p} \\ a_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^\times & \text{for all finite } \mathfrak{p} \\ a_\mathfrak{p} \in W_\mathfrak{m}(\mathfrak{p}) & \text{for all } \mathfrak{p}|\mathfrak{m}. \end{cases}$$

Note that

$$K_{\mathfrak{m},1} = K^\times \cap \prod_{\mathfrak{p}|\mathfrak{m}} W_\mathfrak{m}(\mathfrak{p}) \qquad \text{(intersection inside } \prod_{\mathfrak{p}|\mathfrak{m}} K_\mathfrak{p}^\times),$$

and that

$$K_{\mathfrak{m},1} = K^\times \cap \mathbb{I}_\mathfrak{m} \qquad \text{(intersection inside } \mathbb{I}).$$

PROPOSITION 4.6 *Let* $\mathfrak{m}$ *be a modulus of* K.

(a) *The map* $\mathrm{id}\colon \mathbb{I}_\mathfrak{m} \to I^{S(\mathfrak{m})}$ *defines an isomorphism*

$$\mathbb{I}_\mathfrak{m}/K_{\mathfrak{m},1} \cdot W_\mathfrak{m} \xrightarrow{\simeq} C_\mathfrak{m}.$$

(b) *The inclusion* $\mathbb{I}_\mathfrak{m} \hookrightarrow \mathbb{I}$ *defines an isomorphism:*

$$\mathbb{I}_\mathfrak{m}/K_{\mathfrak{m},1} \to \mathbb{I}/K^\times.$$

PROOF. (a) Consider the pair of maps

$$K_{\mathfrak{m},1} \to \mathbb{I}_\mathfrak{m} \xrightarrow{\mathrm{id}} I^{S(\mathfrak{m})}.$$

The first map is injective, and the second is surjective with kernel $W_{\mathfrak{m}}$, and so the kernelcokernel sequence (II, A.2) of the pair of maps is

$$W_{\mathfrak{m}} \to \mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \to C_{\mathfrak{m}} \to 1.$$

The proves (a) of the proposition.

(b) The kernel of $\mathbb{I}_{\mathfrak{m}} \to \mathbb{I}/K^{\times}$ is $K^{\times} \cap \mathbb{I}_{\mathfrak{m}}$ (intersection in $\mathbb{I}$) which, we just saw, is $K_{\mathfrak{m},1}$. Hence the inclusion defines an injection

$$\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \hookrightarrow \mathbb{I}/K^{\times}.$$

For the surjectivity, we apply the weak approximation theorem (ANT, 7.20). Let $S = S(\mathfrak{m})$ and let $\mathbf{a} = (a_v) \in \mathbb{I}$. If we choose $b \in K$ to be very close to a_v in $K_v^{\times}$ for all $v \in S$, then a_v/b will be close to 1 in $K_v^{\times}$ for all $v \in S$; in fact, we can choose b so that $a_v/b \in W_{\mathfrak{m}}(\mathfrak{p})$ for all $v \in S$. For example, for a real prime v in S, we need only choose b to have the same sign as a_v in K_v. Then $\mathbf{a}/b \in \mathbb{I}_{\mathfrak{m}}$, and it maps to $\mathbf{a}$ in $\mathbb{I}/K^{\times}$. □

Characters of ideals and of ide'les

Let $S \supset S_{\infty}$ be a finite set of primes of K, and let G be a finite abelian group. A homomorphism

$$: I^S \to G$$

is said to **admit a modulus** if there exists a modulus $\mathfrak{m}$ with support in S such that $(i(K_{\mathfrak{m},1})) = 1$. For example, for every abelian extension L/K, Artin showed that the Artin map

$$I^S \to \mathrm{Gal}(L/K)$$

admits a modulus.

PROPOSITION 4.7 *If* $: I^S \to G$ *admits a modulus, then there exists a unique homomor- phism* $\phi: \mathbb{I} \to G$ *such that*

(a) *is continuous (G with the discrete topology)*

(b) $\phi(K^{\times}) = 1$*;*

(c) $\phi(\mathbf{a}) = (\mathrm{id}(\mathbf{a}))$, *all* $\mathbf{a} \in \mathbb{I}^S \overset{\text{def}}{=} \{\mathbf{a} \mid a_v = 1 \text{ all } v \in S\}$.

Moreover, every continuous homomorphism $\phi: \mathbb{I} \to G$ *satisfying (b) arises from a .*

PROOF. Because admits a modulus $\mathfrak{m}$, it factors through $I^{\mathfrak{m}}/i(K_{\mathfrak{m},1}) = C_{\mathfrak{m}}$. Hence we have the diagram:

$$\begin{array}{ccccc} I^{\mathfrak{m}} & \longrightarrow & C_{\mathfrak{m}} & \xrightarrow{\psi} & G \\ & & \simeq\uparrow & & \\ \mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} & \longrightarrow & \mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1}W_{\mathfrak{m}} & & \\ \downarrow\simeq & & & & \\ \mathbb{I} & \longrightarrow & \mathbb{I}/K^{\times}. & & \end{array} \tag{43}$$

The isomorphisms are those in Proposition 4.6, and the remaining unnamed maps are quotient maps. Define to be the composite $\mathbb{I} \to G$. It certainly has properties (a) and (b), and it also has the property that

$$(\mathbf{a}) = \psi(\mathrm{id}(\mathbf{a})) \text{ for all } \mathbf{a} \in \mathbb{I}_{\mathfrak{m}},$$

and so, *a fortiori,* it has property (c).

To prove that the map is uniquely determined by (a), (b), and (c), it suffices to prove that $\mathbb{I}^S K^{\times}$ is dense in $\mathbb{I}$, but this follows from the weak approximation theorem (ANT, 7.20): let $\mathbf{a} \in \mathbb{I}$; choose

$b \in K^\times$ to be very close to a_v for $v \in S$, and let $\mathbf{a}'$ be the element of $\mathbb{I}^S$ such that $a'_v b = a_v$ for all $v \notin S$. Then $\mathbf{a}'b \in \mathbb{I}^S \cdot K$ and is close to $\mathbf{a}$ in $\mathbb{I}$.

For the converse, let $\phi\colon \mathbb{I} \to G$ be a continuous map. The kernel contains an open neighbourhood of 1, and so $U(S,\varepsilon) \subset \mathrm{Ker}(\phi)$ for some S and ε. Consider an infinite prime v. The restriction of to $K_v^\times$ is a continuous map $\mathbb{R}^\times \to G$ or $\mathbb{C}^\times \to G$. Clearly, the connected component of $K_v^\times$ containing 1, namely, $\mathbb{R}_{>0}$ or $\mathbb{C}^\times$, maps to 1, and so is in the kernel. On combining these remarks, we see that the kernel of contains $W_\mathfrak{m}$ for some $\mathfrak{m}$.

Now we can use the diagram at the start of the proof again. We are given a homomorphism $\phi\colon \mathbb{I}/K^\times \to G$, which we can "restrict" to a homomorphism $\mathbb{I}_\mathfrak{m}/K_{\mathfrak{m},1} \to G$. This homomorphism is trivial on $W_\mathfrak{m}$, and hence factors through $\mathbb{I}_\mathfrak{m}/K_{\mathfrak{m},1}W_\mathfrak{m}$. The homomorphism can now be transferred to $C_\mathfrak{m}$, and composed with $\mathbb{I} \twoheadrightarrow C_\mathfrak{m}$. This is the we are looking for. □

REMARK 4.8 Let G be a commutative topological group. Define a homomorphism $: I^S \to G$ to be **admissible** if for every neighbourhood N of 1 in G, there exists a modulus $\mathfrak{m}$ such that $(i(K_{\mathfrak{m},1})) \subset N$. Then every admissible homomorphism defines a homomorphism $\phi\colon \mathbb{I} \to G$ satisfying conditions (a), (b), (c) of the proposition. Moreover, if G is complete and has "no small subgroups" i.e., there exists a neighbourhood of 1 containing no nontrivial subgroup, then every continuous homomorphism $\phi\colon \mathbb{I} \to G$ satisfying (b) arises from an admissible . The proof is the same as that of the proposition (see Proposition 4.1 of Tate 1967).

The circle group $G = \{z \in \mathbb{C} \mid |z| = 1\}$ is complete and has no small subgroups. The admissible $: I^S \to G$, and the corresponding , are called **Hecke characters.**

REMARK 4.9 Given we chose an $\mathfrak{m}$, and then showed how to construct . In practice, it is more usually more convenient to identify directly from knowing that it satisifies the conditions (a), (b), (c). For this, the following observations are useful.

(a)Let $\mathbf{a} = (a_v)$ be an ide'le such that $a_v = 1$ for all finite primes and $a_v > 0$ for all real primes; then $\phi(\mathbf{a}) = 1$. To see this, note that the topology induced on $\prod_{v|\infty} K_v^\times$ as a subgroup of $\mathbb{I}$ is its natural topology. Therefore, the restriction of to it is trivial on the connected component containing 1.

(b)Let $\mathbf{a} = (a_v)$ be an ide'le such that $a_v = 1$ for all $v \in S$ and a_v is a unit for all $v \notin S$; then $\phi(\mathbf{a}) = 1$. In fact, this follows directly from condition (c).

(c) If $\mathbf{a}$ is "close to 1", $\phi(\mathbf{a}) = 1$. In fact, this follows directly from condition (a) in view of the fact that G has the discrete topology.

(d) On combining (a), (b), (c), we find that if $\mathbf{a} = (a_v)$ is such that

$$\begin{cases} a_v > 0 \text{ when } v \text{ is real;} \\ a_v \text{ is "close to 1 " when } v \in S \text{ is finite;} \\ a_v \text{ is a unit when } v \notin S \end{cases}$$

the $\phi(\mathbf{a}) = 1$. In fact, (a) and (b) say that we can multiply $\mathbf{a}$ with ide'les of certain types without changing the value $\phi(\mathbf{a})$. Clearly, if a_v is close to 1 for the finite v in S, we can multiply it by such ide'les to make it close to 1.

EXAMPLE 4.10 Let $L = \mathbb{Q}[\zeta_p]$, and let be the Artin map

$$I^S \to (\mathbb{Z}/p\mathbb{Z})^\times \to \mathrm{Gal}(L/\mathbb{Q}), \quad S = \{p, \infty\}.$$

Recall that first map sends the ideal (uniquely) represented by (r/s), $r,s > 0$, $(p,r) = 1 = (p,s)$, to $[r][s]^{-1}$, and that the second sends $[m]$ to the automorphism $\zeta \mapsto \zeta^m$. Overall, for any prime number $l \neq p$, the map sends (l) to the Frobenius automorphism at l, $\zeta \mapsto \zeta^l$. Let

$\phi: \mathbb{I} \to \mathrm{Gal}(L/\mathbb{Q})$ be the homomorphism corresponding to as in the theorem. We wish to determine explicitly.

Let $\mathbf{a} = (a_\infty, a_2, \dots, a_p, \dots, a_l, \dots)$ b e an ide'le of $\mathbb{O}$. If $a_\infty = 1 = a_p$, then $\phi(\mathbf{a}) = (\mathrm{id}(\mathbf{a}))$. Thus $\phi(\mathbf{a}) = \zeta_p^m$, where $m = \prod l^{\mathrm{ord}_l(a_l)}$.

Consider $\mathbf{p} = (1, \dots, \overset{r}{1}, p, 1, \dots)$ (p in the p-position). Then

$$\mathbf{p}/p = (p^{-1}, \dots, p^{-1}, 1, p^{-1}, \dots).$$

According to (d) of the above Remark, $\phi(\mathbf{p}/p) = 1$, and so

$$(\mathbf{p}) = \phi(\mathbf{p}/p)\phi(p) = 1.$$

In this, p denotes both the element $p \in \mathbb{Q}_p$ and the principal ide'le $(p, p, \dots)$.

Consider $\mathbf{a} = (1, \dots, 1, u, 1, \dots)$, $u \in \mathbb{Z}_p^\times$, u in the p-position. Write

$$u^{-1} = a_0 + a_1 p + \cdots + a_s p^s + \cdots, \quad 0 \le a_i < p, \quad a_i \in \mathbb{Z},$$

and let $c = a_0 + \cdots + a_s p^s \in \mathbb{Z}$. Note that $c > 0$. Then $uc \in 1 + p^{s+1}\mathbb{Z}_p$, i.e., for large s it is "close to 1". Write

$$\mathbf{a}c = (c, c, \dots, c, \overset{l|c}{1}, c, \dots, \overset{p}{uc}, c, \dots)(1, \dots, 1, \overset{l|c}{c}, 1, \dots).$$

The first factor is $\mathbf{a}c$ except that we have moved the components at the primes l dividing c to the second factor. For large s, $\phi($ first factor$) = 1$ by (d) of the above remark. The second factor lies in $\mathbb{I}^S$, and the description we have of $\phi|\mathbb{I}^S$ shows that $\phi($ second factor$)$ maps ζ to ζ^c. In conclusion,

$$(\mathbf{a})(\zeta) = \zeta^c = \zeta^{u^{-1}}. \tag{44}$$

Consider $\mathbf{a} = (-1, 1, \dots, 1)$. Then

$$-\mathbf{a} = (1, -1, \dots, -1, \overset{p}{1}, -1, \dots)(1, \dots, 1, \overset{p}{-1}, 1, \dots),$$

and

$$(\mathbf{a}) = \phi(-\mathbf{a}) = \phi(1, \dots, 1, -1, 1, \dots).$$

According (44), $\phi(\mathbf{a})(\zeta) = \zeta^{-1}$.

Because is a homomorphism, this completes the explicit description of it.

REMARK 4.11 From (43), we get a canonical homomorphism $\pi_\mathfrak{m}: \mathbb{I} \to C_\mathfrak{m}$. This is the unique continuous homomorphism $\pi_\mathfrak{m}: \mathbb{I} \to C_\mathfrak{m}$ such that

(a) $\pi_\mathfrak{m}(K^\times) = 1$;

(b) $\pi_\mathfrak{m}(\mathbf{a}) = \mathrm{id}(\mathbf{a})$ for all $\mathbf{a} \in \mathbb{I}^{S(\mathfrak{m})}$.

(Take to be $I^S \to C_\mathfrak{m}$ in Proposition 4.7.).

If $\mathfrak{m}|\mathfrak{m}'$, then the composite of $\pi_{\mathfrak{m}'}$ with the canonical homomorphism $C_{\mathfrak{m}'} \to C_\mathfrak{m}$ satisfies the conditions characterizing $\pi_\mathfrak{m}$. Therefore, the $\pi_\mathfrak{m}$ combine to give a continuous homomorphism $\pi: \mathbb{I} \to \varprojlim C_\mathfrak{m}$. We wish to determine the kernel and image of this map.

Because each map $\pi_\mathfrak{m}: \mathbb{I} \to C_\mathfrak{m}$ is onto, the image is dense. In fact, $\mathbb{I}^1 \to C_\mathfrak{m}$ is onto, and so $\pi_\mathfrak{m}(\mathbb{I}^1)$ is dense. But $\pi_\mathfrak{m}(\mathbb{I}^1)$ is compact, because $\pi_\mathfrak{m}$ factors through the compact group $\mathbb{I}^1/K^\times$, and therefore is complete. This shows that π is onto.

Let $\mathbb{I}_\infty^+$ be the set of ideʻles $\mathbf{a}$ such that $a_v = 1$ if v is finite and $a_v > 0$ if v is real. Thus $\mathbb{I}_\infty^+$ is isomorphic to the identity component of $(K \otimes_{\mathbb{Q}} \mathbb{R})^\times = \prod_{v|\infty} K_v^\times$. The kernel of $\mathbb{I} \to \varprojlim C_{\mathfrak{m}}$ contains $\mathbb{I}_\infty^+ \cdot K^\times$, and hence its closure. In fact, it equals it. [In a future version, these things will be examined in more detail.]

Norms of ideʻles

Let L be a finite extension of the number field K, let v be a prime of K. Recall from (ANT, 8.2) that there is a canonical isomorphism

$$L \otimes_K K_v \to \prod_{w|v} L_w.$$

It follows (ibid. 8.3) that for any $\alpha \in L$,

$$\mathrm{Nm}_{L/K}\,\alpha = \prod_{w|v} \mathrm{Nm}_{L_w/K_v}\,\alpha \qquad \text{(equality in } K_v\text{)}.$$

For an ideʻle $\mathbf{a} = (a_w) \in \mathbb{I}_L$, define $\mathrm{Nm}_{L/K}(\mathbf{a})$ to be the ideʻle $\mathbf{b} \in \mathbb{I}_K$ with $b_v = \prod_{w|v} \mathrm{Nm}_{L_w/K_v}\, a_w$. The preceding remark shows that the left hand square in the following diagram commutes, and it is easy to see that the right hand square commutes:

$$\begin{array}{ccccc} L^\times & \longrightarrow & \mathbb{I}_L & \xrightarrow{\text{id}} & I_L \\ \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} \\ K^\times & \longrightarrow & \mathbb{I}_K & \xrightarrow{\text{id}} & I_K. \end{array}$$

Thus we get a commutative diagram:

$$\begin{array}{ccc} \boldsymbol{C}_L & \longrightarrow & C_L \\ \downarrow{\scriptstyle \mathrm{Nm}\, L/K} & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} \\ \boldsymbol{C}_K & \longrightarrow & C_K \end{array}$$

($\boldsymbol{C}_K$ = ideʻle class group $\mathbb{I}/K^\times$; C_K =ideal class group $I/i(K^\times)$).

PROPOSITION 4.12 *If L/K is a finite extension of local fields of characteristic zero, then*

(a) $\mathrm{Nm}_{L/K}(L^\times) = \mathbb{R}_{>0}$ *(case $K = \mathbb{R}$, $L = \mathbb{C}$);*

(b) $\mathrm{Nm}_{L/K}(L^\times) \supset 1 + \mathfrak{p}_K^m$ *for some m (case K is nonarchimedean);*

(c) $\mathrm{Nm}_{L/K}(L^\times) \supset \mathcal{O}_K^\times$ *(case K is nonarchimedean and L/K is unramified).*

PROOF. Statement (a) is obvious. For (b), see (I 1.3), and for (c), see (III, 1.2). □

COROLLARY 4.13 *Let L/K be a finite extension of number fields. Then $\mathrm{Nm}_{L/K}\,\mathbb{I}_L \supset W_{\mathfrak{m}}$ for some modulus $\mathfrak{m}$.*

5 The Main Theorems in Terms of Idèles

The statement of the main theorems of class field theory in terms of ideals is very explicit and, for many purposes, it is the most useful one. However, it has some disadvantages. One has to fix a modulus $\mathfrak{m}$, and then the theory describes only the abelian extensions whose conductor divides $\mathfrak{m}$. In particular, it provides no description of the infinite abelian extensions of K. The statement of the main theorems in terms of ideʻles allows one to consider infinite abelian extensions, or, what amounts to the same thing, all finite abelian extensions simultaneously. It also makes transparent the relation between the local and global Artin maps.

Let L be a finite abelian extension of K. Let v be a prime of K, and let w be a prime of L lying over v. Recall that the decomposition group $D(w)$ of w is the subgroup

$$D(w) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma w = w\}.$$

Its elements extend uniquely to automorphisms of L_w/K_v, and $D(w) \simeq \mathrm{Gal}(L_w/K_v)$. Local class field theory (I, 1.1) provides us with a homomorphism (the local Artin map)

$$'_v\colon K_v^\times \to D(w) \subset G.$$

LEMMA 5.1 *The subgroup $D(w)$ of G and the map φ_v are independent of the choice of the prime $w|v$.* PROOF. Any other prime lying over v is of the form σw for some $\sigma \in G$, and $\sigma\colon L \to L$ extends by continuity to a homomorphism $\sigma\colon L_w \to L_{\sigma w}$ fixing K_v. We have

$$D(\sigma w) = \sigma D(w)\sigma^{-1},$$

which equals $D(w)$ because G is commutative.

Let Ω and Ω' be maximal abelian extensions of K_v containing L_w and $L_{\sigma w}$ respectively. From Chapter III, we obtain local Artin maps $\phi_v\colon K^\times \to \mathrm{Gal}(\Omega/K_v)$ and $\phi'_v\colon K^\times \to \mathrm{Gal}(\Omega'/K_v)$. The choice of an isomorphism $\tilde{\sigma}\colon \Omega \to \Omega'$ determines an isomorphism

$$\rho \mapsto \tilde{\sigma} \circ \rho \circ \tilde{\sigma}^{-1}\colon \mathrm{Gal}(\Omega/K_v) \to \mathrm{Gal}(\Omega'/K_v)$$

which is independent of $\tilde{\sigma}$. Moreover, its composite with φ_v is ϕ'_v (because it satisfies the conditions characterizing ϕ'_v). □

PROPOSITION 5.2 *There exists a unique continuous homomorphism $\phi_K\colon \mathbb{I} \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ with the following property: for any $L \subset K^{\mathrm{ab}}$ finite over K and any prime w of L lying over a prime v of K, the diagram*

$$\begin{array}{ccc} K_v^\times & \xrightarrow{\phi_v} & \mathrm{Gal}(L_w/K_v) \\ \downarrow & & \downarrow \\ \mathbb{I}_K & \xrightarrow{\mathbf{a}\mapsto\phi_K(\mathbf{a})|L} & \mathrm{Gal}(L/K) \end{array}$$

commutes.

PROOF. Let $\mathbf{a} \in \mathbb{I}$, and let $L \subset K^{\mathrm{ab}}$ be finite over K. If $a_v \in U_v$ and L_w/K_v is unramified, the $\phi_v(a_v) = 1$ (see III, 1). Therefore, $\phi_v(a_v) = 1$ except for finitely many v's, and so we can define

$$'_{L/K}(\mathbf{a}) = \prod_v \prod \phi_v(a_v).$$

(product inside $\mathrm{Gal}(L/K)$). Clearly, $\varphi_{L/K}$ is the unique homomorphism making the above diagram commute.

If $L' \supset L$, then the properties of the local Artin maps show that $\phi_{L'/K}(\mathbf{a})|L = \phi_{L/K}(\mathbf{a})$. Therefore there exists a unique homomorphism $\phi\colon \mathbb{I} \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ such that

$$(\mathbf{a})|L = \phi_{L/K}(\mathbf{a}) \text{ for all } L \subset K^{\mathrm{ab}}, L \text{ finite over } K.$$

Again, the properties of the local Artin maps show that, for any fields $K \subset K' \subset L \subset K^{\mathrm{ab}}$ with L finite over K,

$$\begin{array}{ccc} \mathbb{I}_{K'}^S & \xrightarrow{\phi_{L/K'}} & \mathrm{Gal}(L/K') \\ \downarrow \mathrm{Nm} & & \downarrow \\ \mathbb{I}_K^S & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K) \end{array}$$

commutes. On taking $K' = L$, we find that $\mathrm{Nm}_{L/K}(\mathbb{I}_L^S)$ is contained in the kernel of $\varphi_{L/K}$. In particular, the kernel of $\varphi_{L/K}$ contains an open subgroup of $\mathbb{I}_K^S$ (Corollary 4.13), and this implies that φ_K is continuous. □

THEOREM 5.3 (RECIPROCITY LAW) *The homomorphism $\phi_K\colon \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ has the following properties:*

(a) $\phi_K(K^\times) = 1$;

(b) *for every finite abelian extension L of K, φ_K defines an isomorphism*

$$'_{L/K}\colon \mathbb{I}_K/(K^\times \cdot \mathrm{Nm}(\mathbb{I}_L)) \to \mathrm{Gal}(L/K).$$

We saw in the proof of the proposition that $\phi_{L/K}(\mathrm{Nm}(\mathbb{I}_L)) = 1$, and so (assuming (a) of the theorem) we see that $\varphi_{L/K}$ does factor through $\mathbb{I}_K/K^\times \cdot \mathrm{Nm}(\mathbb{I}_L)$. Part (b) can also be stated as: defines an isomorphism

$$'_{L/K}\colon \boldsymbol{C}_K/\mathrm{Nm}(\boldsymbol{C}_L) \to \mathrm{Gal}(L/K).$$

EXAMPLE 5.4 Statement (a) of the theorem says that, for every $b \in K^\times$, $\prod \phi_v(b) = 1$. On applying this to the extension $K[a^{\frac{1}{n}}]/K$ under the assumption that K contains a primitive nth root of 1, one obtains the product formula for the Hilbert symbol:

$$\prod_v (a,b)_v = 1.$$

See (III, 4.8).

THEOREM 5.5 (EXISTENCE THEOREM) *Fix an algebraic closure K^{al} of K; for every open subgroup $N \subset \boldsymbol{C}_K$ of finite index, there exists a unique abelian extension L of K contained in K^{al} such that $\mathrm{Nm}_{L/K}\boldsymbol{C}_L = N$.*

A subgroup of $\boldsymbol{C}_K$ is a **norm group** if it is of the form $\mathrm{Nm}(\boldsymbol{C}_L)$ for some finite abelian extension L of K. The existence theorem shows that the norm groups are exactly the open subgroups of finite index in $\boldsymbol{C}_K$. If N is such a group, then the finite abelian extension L of K such that $\mathrm{Nm}(\boldsymbol{C}_L) = N$, i.e., such that $N = \mathrm{Ker}(\phi_{L/K})$, is called the **class field of K belonging to N.**

As stated, the Existence Theorem is valid for all global fields.

COROLLARY 5.6 *The map $L \mapsto \mathrm{Nm}(\boldsymbol{C}_L)$ is a bijection from the set of finite abelian extensions of K to the set of open subgroups of finite index in $\boldsymbol{C}_K$. Moreover,*

$$\begin{array}{rcl} L_1 \subset L_2 & \iff & \mathrm{Nm}(\boldsymbol{C}_{L_1}) \supset \mathrm{Nm}(\boldsymbol{C}_{L_2}); \\ \mathrm{Nm}(\boldsymbol{C}_{L_1 \cdot L_2}) & = & \mathrm{Nm}(\boldsymbol{C}_{L_1}) \cap \mathrm{Nm}(\boldsymbol{C}_{L_2}); \\ \mathrm{Nm}(\boldsymbol{C}_{L_1 \cap L_2}) & = & \mathrm{Nm}(\boldsymbol{C}_{L_1}) \cdot \mathrm{Nm}(\boldsymbol{C}_{L_2}). \end{array}$$

REMARK 5.7 (a) In the number field case, the map

$$'_K\colon \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

is surjective. For an infinite prime v of K, write K_v^+ for the connected component of $K_v^\times$ containing 1; thus K_v^+ is isomorphic to $\mathbb{C}^\times$ or $\mathbb{R}_{>0}^\times$ according as v is complex or real. Clearly $\prod_{v|\infty} K_v^+ \subset \mathrm{Ker}(\phi_K)$. By definition $K^\times \subset \mathrm{Ker}(\phi_K)$, and so $K^\times \cdot (\prod_{v|\infty} K_v^+) \subset \mathrm{Ker}(\phi_K)$. But φ_K is a continuous homomorphism and $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ is Hausdorff, and so the kernel is a *closed* subgroup. Thus $\mathrm{Ker}(\phi_K)$ contains the closure of $K^\times \cdot (\prod_{v|\infty} K_v^+)$. It is a theorem that this is precisely the kernel. The image of the closure of $K^\times \cdot (\prod_{v|\infty} K_v^+)$ in $\boldsymbol{C}_K$ is the connected component of $\boldsymbol{C}_K$ containing 1.

For every finite abelian extension L/K, the Artin map defines an isomorphism

$$C_K/N_{L/K}(C_L) \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

Passing to the inverse limit over L gives an isomorphism with $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ on the right. The problem is therefore to compute the inverse limit of the system $\big(C_K/N_{L/K}(C_L)\big)_L$. The existence theorem says that the norm groups $N_{L/K}(C_L)$ are exactly the open subgroups of finite index, so this is a problem in topology.

(b) In the function field case, the Artin map $\phi_K\colon \mathbb{I}_K/K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ is injective, but it is not surjective (its image is dense).

REMARK 5.8 Assume that the global Artin map $\phi\colon \mathbb{I} \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ contains $K^\times$ in its kernel. Then, for every finite abelian extension L/K, $\phi_{L/K}\colon \mathbb{I} \to \mathrm{Gal}(L/K)$ arises (as in Proposition 4.7) from a homomorphism $: I^S \to \mathrm{Gal}(L/K)$ admitting a modulus. Moreover, because is the product of the local Artin maps, must be the ideal-theoretic global Artin map (which therefore admits a modulus). It is a straightforward exercise to derive Theorems 3.5 and 3.6 from their ideʻlic counterparts, Theorems 5.3 and 5.5. We shall prove Theorems 5.3 and 5.5 in Chapter VII

NOTES In his 1951 report Sur la theórie du corps de classes, Weil wrote:[13]

La recherche d'une interpre´tation de C_k si k est un corps de nombres, analogue en quelque manieʻre aʻ l'interpre´tation par un groupe de Galois quand k est un corps de fonctions, me semble constituer l'un des probleʻmes fondamentaux de la theórie des nombres aʻ l'heure actuelle; il se peut qu'une telle interpre´tation renferme la clef de l'hypotheʻse de Riemann...

For a discussion of this, see mo41296.

Example

LEMMA 5.9 *The map*

$$(r, t, (u_p)) \mapsto (rt, ru_2, ru_3, ru_5, \ldots)\colon \mathbb{Q}^\times \times \mathbb{R}_{>0} \times \prod \mathbb{Z}_p^\times \to \mathbb{I}_\mathbb{Q}$$

is an isomorphism of topological groups ($\mathbb{Q}^\times$ with the discrete topology).

PROOF. Any ideʻle $\mathbf{a} = (a_\infty, a_2, \ldots, a_p, \ldots)$ can be written

$$\mathbf{a} = a(t, u_2, u_3, u_5, \ldots), \quad a \in \mathbb{Q}^\times, \quad t \in \mathbb{R}_{>0}, \quad u_p \in \mathbb{Z}_p^\times;$$

—take $a = (\ \mathrm{sign}(a_\infty)) \prod p^{\mathrm{ord}_p(a_p)}$, $t = a_\infty/a$, $u_p = a_p/a$. Moreover, the expression is unique because the only positive rational number that is a p-adic unit for all p is 1.

The subsets

$$\{1\} \times U \times \coprod_{p \text{ finite}} U_p$$

with U, U_p open neighbourhoods of 1 in $\mathbb{R}^\times, \mathbb{Q}_p^\times$, and $U_p^\times = \mathbb{Z}_p^\times$ for all but finitely many p's, form a fundamental system of neighbourhoods 1 on the left, and also on the right. □

Thus there is a canonical isomorphism of topological groups

$$\boldsymbol{C}_\mathbb{Q} \to \mathbb{R}_{>0} \times \prod_{p \text{ finite}} \mathbb{Z}_p^\times = \mathbb{R}_{>0} \times \hat{\mathbb{Z}}^\times.$$

[13]The search for an interpretation of C_k when k is a number field, in some way analogous to its interpretation as a Galois group when k is a function field, seems to me to be one of the

fundamental problems of number theory at present; perhaps such an interpretation contains the key to the Riemann hypothesis... Let

$$\mathbb{Q}^{\mathrm{cyc}} = \bigcup \mathbb{Q}[\zeta_n].$$

In this case, the global reciprocity map is the reciprocal of

$$: \mathbb{I}_{\mathbb{Q}} \to \hat{\mathbb{Z}}^{\times} \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q}),$$

where $\mathbb{I}_{\mathbb{Q}} \to \hat{\mathbb{Z}}^{\times}$ is the above projection map, and $\hat{\mathbb{Z}}^{\times} \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q})$ is the canonical isomorphism (see I A.5c).

SUMMARY 5.10 Let K be an algebraic number field. There exists a continuous surjective homomorphism (the reciprocity or Artin map)

$$'_K : \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

such that, for every finite extension L of K contained in K^{ab}, φ_K gives rise to a commutative diagram

$$\begin{array}{ccc} \mathbb{I}_K/K^{\times} & \xrightarrow{\phi_K} & \mathrm{Gal}(K^{\mathrm{ab}}/K) \\ \downarrow & & \downarrow{\scriptstyle \tau \mapsto \tau|L} \\ \mathbb{I}_K/\left(K^{\times} \cdot \mathrm{Nm}(\mathbb{I}_L)\right) & \xrightarrow[\simeq]{\phi_{L/K}} & \mathrm{Gal}(L/K). \end{array}$$

It is determined by the following two properties:

(a) $\phi_{L/K}(u) = 1$ for every $u = (u_v) \in \mathbb{I}_K$ such that

i) if v is unramified in L, then u_v is a unit, ii) if v is ramified in L, then u_v is sufficiently close to 1 (depending only on L/K), and iii) if v is real but becomes complex in L, then $u_v > 0$.

(b) For every prime v of K unramified in L, the ide'le

$$\alpha = (1, \ldots, 1, \underset{v}{\pi}, 1, \ldots), \quad \pi \text{ a prime element of } \mathcal{O}_v,$$

maps to the Frobenius element $(\mathfrak{p}_v, L/K)$ in $\mathrm{Gal}(L/K)$. To see that there is at most one map satisfying these conditions, let $\alpha \in \mathbb{I}_K$, and use the weak approximation theorem to choose an $a \in K^{\times}$ that is close to α_v for all primes v that ramify in L or become complex. Then $\alpha = au\beta$ with u an ide'le as in (a) and β a finite product of ide'les as in (b). Now $\phi_{L/K}(\alpha) = \phi_{L/K}(\beta)$, which can be computed using (b).

For $K = \mathbb{Q}$, the Artin map factors through $\{\pm\} \times \mathbb{I}_f/\mathbb{Q}^{\times}$, and every element of this quotient is uniquely represented by an element of $\hat{\mathbb{Z}}^{\times} \subset \mathbb{I}_f$. In this case, we get the diagram

$$\begin{array}{ccccc} \hat{\mathbb{Z}}^{\times} & \xrightarrow[\simeq]{\phi_{\mathbb{Q}}} & \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) & = & \bigcup_m \mathbb{Q}[\zeta_m] \\ \downarrow & & \downarrow{\scriptstyle \text{restrict}} & & \\ (\mathbb{Z}/m\mathbb{Z})^{\times} & \xrightarrow[\simeq]{[n] \mapsto (\zeta_m \mapsto \zeta_m^n)} & \mathrm{Gal}(\mathbb{Q}[\zeta_m]/\mathbb{Q}). & & \end{array}$$

which *commutes with an inverse.* This can be checked by writing an ide'le α in the form $au\beta$ as above, but it is more instructive to look at an example. Let p be a prime not dividing m, and let

$$\alpha = p \cdot (1, \ldots, 1, \underset{p}{p^{-1}}, 1, \ldots) \in \mathbb{Z} \cdot \mathbb{I}_f = \mathbb{I}_f.$$

Then

$$\alpha = (p, \ldots, p, \underset{p}{1}, p, \ldots) \in \hat{\mathbb{Z}}^{\times}$$

has image $[p]$ in $(\mathbb{Z}/m\mathbb{Z})^\times$, which acts as $(p, \mathbb{Q}[\zeta_m]/\mathbb{Q})$ on $\mathbb{Q}[\zeta_m]$. On the other hand, $\phi_{\mathbb{Q}}(\alpha) = \phi_{\mathbb{Q}}((1, \ldots, 1, \underset{p}{p^{-1}}, 1, \ldots))$, which acts as $(p, \mathbb{Q}[\zeta_m]/\mathbb{Q})^{-1}$.

EXERCISE 5.11 Show that, even when K is a number field, the ideʻle class group of K has subgroups of finite index that are not open.

5. GLOBAL CLASS FIELD THEORY: PROOFS

J. S. Milne, Class Field Theory (v4.03)

> *J'ai revu un peu la théorie du corps de classes, dont j'ai enfin l'impression d'avoir compris les énoncés essentiels (bien entendu, pas les démonstrations!)*
> Grothendieck, letter to Serre, 19.9.56.[1]

In this chapter we prove the main theorems of global class field theory, namely, the Reciprocity Law and the Existence Theorem (Theorems 5.3 and 5.5 of Chapter V), following the method of Tate 1967 (see also Artin and Tate 1961). Throughout, we work with ideles rather than ideals.

This chapter is independent of Chapter VI, except that Theorem 4.9 of Chapter VI can be used to replace Section 6. We shall need to refer to Chapter V only for the definitions of the idele class group and the the definition of the global Artin map $\phi\colon \mathbb{I} \to \mathrm{Gal}(L/K)$ as the "product" of the local Artin maps (Section 5). On the other hand, we shall make frequent use of the results in Chapters II and III.

We use the notation from Chapter V (especially p. 169). In particular, $|\cdot|_v$ denotes the normalized absolute value for v (for which the product formula holds).

1 Outline

Let L/K be a finite Galois extension of number fields with Galois group G. The idele class group $\boldsymbol{C}_L \overset{\text{def}}{=} \mathbb{I}_L/L^\times$ plays the same role for global class field theory that the multiplicative group $\tilde{L}^\times$ plays for local class field theory. In particular, when L/K is abelian, we shall prove that there is a isomorphism

$$: \boldsymbol{C}_K/\operatorname{Nm}_{L/K}(\boldsymbol{C}_L) \to G$$

[1]I have been reviewing a little class field theory, of which I finally have the impression that I understand the main results (but not the proofs, of course!) whose local components are the local Artin maps, i.e., such that for any prime v of K and prime w of L lying over it, the following diagram commutes,

$$\begin{array}{ccc} K_v^\times & \xrightarrow{\phi_v} & \mathrm{Gal}(L_w/K_v) \\ \downarrow & & \downarrow \\ \mathbb{I}_K & \xrightarrow{\phi} & \mathrm{Gal}(L/K), \end{array}$$

where φ_v is the local Artin map of Chapters I and III.

According to Tate's theorem (3.11, Chapter II), to obtain such an isomorphism, it suffices to prove that, for every finite Galois extension L/K with Galois group G,

(a) $H^1(G, \boldsymbol{C}_L) = 0$;

(b) $H^2(G, \boldsymbol{C}_L)$ is cyclic of order $[L : K]$ with a canonical generator $u_{L/K}$;

(c) if $E \supset L \supset K$ are two finite Galois extensions of K, then $\mathrm{Res}(u_{E/K}) = u_{E/L}$. The isomorphism $\varphi_{L/K}$ is then the inverse of that defined by $u_{L/K}$,

$$H_T^{-2}(G, \mathbb{Z}) \to H_T^0(G, \boldsymbol{C}_L).$$

Once the fundamental class $u_{L/K}$ has been shown to be compatible with the local fundamental classes, $\varphi_{L/K}$ will be a product of the local Artin maps.

In fact, we adopt a slightly different approach. We shall *define* the global Artin map $\boldsymbol{C}_K \to \mathrm{Gal}(L/K)$ to be the "product" of the local Artin maps, and we shall use results slightly weaker than (a) and (b) to deduce that it has the correct properties.

In Section 2, we express the cohomology of the ide'les in terms of the cohomology of the local fields,

$$H^0(G, \mathbb{I}_L) = \mathbb{I}_K;$$
$$H_T^r(G, \mathbb{I}_L) \simeq \bigoplus\nolimits_v H_T^r(G^v, L^{v\times})$$

(sum over the primes v of K; for some choice of a prime $w|v$, G^v is the decomposition group of w and $L^v = L_w$). After computing the Herbrand quotient of the group of S-units in Section 3, we prove the first inequality,

for any cyclic extension L/K, $(\boldsymbol{C}_K : \mathrm{Nm}_{L/K}\boldsymbol{C}_L) \geq [L : K]$, in Section 4. We also prove in Section 4 that, for any abelian extension, the Galois group is generated by the Frobenius elements. In Section 5 we state the theorem,

For every Galois extension L/K of number fields, (a) $(\boldsymbol{C}_K : \mathrm{Nm}_{L/K}\boldsymbol{C}_L) \leq [L : K]$ (second inequality); (b) $H^1(G, \boldsymbol{C}_L) = 1$; (c) $H^2(G, \boldsymbol{C}_L)$ has order

$$\leq [L : K].$$

and we prove it using Theorem 4.9 of Chapter VI. In the following section, we give a different proof of the theorem that avoids the use complex analysis.

After some preliminaries on Brauer groups, in Section 7 we complete the proof of the reciprocity law by showing that, for every abelian extension L/K, $K^\times$ is contained in the kernel of $\phi_{L/K} : \mathbb{I}_K \to \mathrm{Gal}(L/K)$. Because we already know that $\mathrm{Nm}_{L/K}(\mathbb{I}_L)$ is contained in the kernel of $\varphi_{L/K}$ and that $\varphi_{L/K}$ is surjective (because $\mathrm{Gal}(L/K)$ is generated by the Frobenius elements), the second inequality implies that $\varphi_{L/K}$ is an isomorphism.

We prove the Existence Theorem in Section 9 by showing the every (open) subgroup of finite index in $\boldsymbol{C}_K$ contains the norm group of some subextension of the extension obtained by first adjoining a root of unity to K and then making a Kummer extension.

To some extent, the cyclic cyclotomic extensions of K play the same role as the unramified extensions of a local field. For example, a key point in the last step of the proof of the Reciprocity Law is that every element of $\mathrm{Br}(K)$ is split by a cyclic cyclotomic extension.

2 The Cohomology of the Idèles

Let L/K be a finite Galois extension of number fields with Galois group G. Recall that $\sigma \in G$ acts on the primes w of L lying over a fixed prime v of K according to the rule $|\sigma a|_{\sigma w} = |a|_w$. Therefore σ is an isomorphism of valued fields

$$(L, |\ |_w) \to (L, |\ |_{\sigma w}),$$

and so extends to the completions: there is a commutative diagram

$$\begin{array}{ccc} L_w & \xrightarrow{\sigma} & L_{\sigma w} \\ \uparrow{\scriptstyle i_w} & & \uparrow{\scriptstyle i_{\sigma w}} \\ L & \xrightarrow{\sigma} & L. \end{array}$$

Fix a prime v of K, and let w_0 be a prime of L lying over v. The map $\sigma \mapsto \sigma w_0$ defines a bijection

$$G/G_{w_0} \to \{w|v\},$$

where G_{w_0} is the decomposition group of w_0.

We wish to extend the action of G on L to an action of G on $\prod_{w|v} L_w$. Recall (ANT, 8.2) that the map

$$a \otimes b \mapsto (i_w(a)b)_w : L \otimes_K K_v \to \prod\nolimits_{w|v} L_w$$

is an isomorphism. The group G acts on $L \otimes_K K_v$ through its action on L, and we use the isomorphism to transfer this action to $\prod_{w|v} L_w$. Thus,

(a) the elements of G acts continuously on $\prod_{w|v} L_w$;

(b) all elements of the form $(a, \dots, a)$, $a \in K_v$, are fixed by G;

(c) for every $a \in L$, $\sigma(\dots, i_w(a), \dots) = (\dots, i_w(\sigma a), \dots)$. These conditions determine the action uniquely (in fact, (a) and (c) determine it because K is dense in K_v).

LEMMA 2.1 *For $\sigma \in G$ and $\alpha = (\alpha(w)) \in \prod_{w|v} L_w$,*

$$(\sigma\alpha)(w) = \sigma(\alpha(\sigma^{-1}w)). \qquad (*)$$

PROOF. The rule $(*)$ does define a continuous action of G on $\prod L_w$, and so it suffices to check that it satisfies (b) and (c). Condition (b) is obvious. For (c), let $\alpha(w) = i_w(a)$, $a \in L$. Then (by $(*)$)

$$(\sigma\alpha)(w) = \sigma(i_{\sigma^{-1}w}(a)).$$

When we replace w with $\sigma^{-1}w$ in the commutative diagram above, we obtain the formula $\sigma \circ i_{\sigma^{-1}w} = i_w \circ \sigma$. Therefore

$$(\sigma\alpha)(w) = i_w(\sigma a),$$

as required. □

In more down-to-earth terms, $(\sigma\alpha)(\sigma w) = \sigma(\alpha(w))$: if α has the element a in the w-position, then $\sigma\alpha$ has the element σa in the σw-position.

Note that the action of G on $\prod_{w|v} L_w$ induces an action of G on the subsets $\prod_{w|v} L_w^\times$ and $\prod_{w|v} U_w$ of $\prod_{w|v} L_w$.

PROPOSITION 2.2 *Choose a $w_0|v$, and let G_{w_0} be its decomposition group. For $\alpha \in \prod_{w|v} L_w$ and $\sigma \in G$, define $f_\alpha(\sigma) = \sigma(\alpha(\sigma^{-1}w_0))$. Then $f_\alpha \in \operatorname{Ind}_{G_{w_0}}^G(L_{w_0})$, and the map*

$$\alpha \mapsto f_\alpha : \prod_{w|v} L_w \to \operatorname{Ind}_{G_{w_0}}^G(L_{w_0})$$

is an isomorphism of G-modules. Similar statements hold with L_w replaced with $L_w^\times$ and with U_w.

PROOF. Recall (II 1) that

$$\operatorname{Ind}_{G_{w_0}}^G(L_{w_0}) = \{f : G \to L_{w_0} \mid f(\rho\sigma) = \rho f(\sigma), \text{ all } \rho \in G_{w_0}\}$$

and that $\tau \in G$ acts on $f \in \operatorname{Ind}_{G_{w_0}}^G(L_{w_0})$ according to the rule $(\tau f)(\sigma) = f(\sigma\tau)$. For $\rho \in G_{w_0}$,

$$f_\alpha(\rho\sigma) = \rho\sigma(\alpha(\sigma^{-1}\rho^{-1}w_0)) = \rho\sigma(\alpha(\sigma^{-1}w_0)) = \rho f_\alpha(\sigma),$$

and so $f_\alpha \in \mathrm{Ind}_{G_{w_0}}^{G}(L_{w_0})$. Moreover,

$$(\tau f_\alpha)(\sigma) = f_\alpha(\sigma\tau) = \sigma\tau(\alpha(\tau^{-1}\sigma^{-1}w_0)) = \sigma(\tau\alpha)(\sigma^{-1}w_0) = f_{\tau\alpha}(\sigma),$$

and so $\alpha \mapsto f_\alpha$ is a homomorphism of G-modules $\prod_{w|v} L_w \to \mathrm{Ind}_{G_{w_0}}^{G}(L_{w_0})$. Given

$f \in \mathrm{Ind}_{G_{w_0}}^{G}(L_{w_0})$, set

$$\alpha_f(w) = \sigma(f(\sigma^{-1})), \quad w = \sigma w_0.$$

Then $f \mapsto \alpha_f$ is an inverse to $\alpha \mapsto f_\alpha$. □

PROPOSITION 2.3 *For all r,*

$$H^r(G, \textstyle\prod_{w|v} L_w^\times) \simeq H^r(G_{w_0}, L_{w_0}^\times).$$

In particular,

$$H^0(G, \textstyle\prod_{w|v} L_w^\times) \simeq K_v^\times.$$

Similar statements hold with $L_w^\times$ replaced with U_w.

PROOF. We have

$$H^r(G, \textstyle\prod_{w|v} L_w^\times) = H^r(G, \mathrm{Ind}_{G_{w_0}}^{G} L_{w_0}^\times) = H^r(G_{w_0}, L_{w_0}^\times)$$

by Shapiro's lemma (II, 1.11). □

REMARK 2.4 The group $H^r(G_{w_0}, L_{w_0}^\times)$ is independent of the prime w_0 dividing v up to a *canonical* isomorphism, for let w be a second such prime. Then we can write $w = \sigma w_0$, and we have a compatible pair of isomorphisms

$$\mapsto \sigma\tau\sigma^{-1}\colon G_{w_0} \to G_w, \qquad x \mapsto \sigma^{-1}x\colon L_w \to L_{w_0},$$

and hence isomorphisms

$$H^r(G_w, L_w^\times) \to H^r(G_{w_0}, L_{w_0}^\times)$$

for each r (see II, §1).

If $w = \sigma' w_0$, then $\sigma' = \sigma\tau$ with $\tau \in G_{w_0}$. The maps defined by σ and σ' differ by the automorphism of $H^r(G_{w_0}, L_{w_0}^\times)$ defined by , which is the identity map (II, 1.27d). Therefore $H^r(G_{w_0}, L_{w_0}^\times)$ and $H^r(G_w, L_w^\times)$ are *canonically* isomorphic. This suggests the following notation: choose a prime $w|v$ and set,

$$G^v = G_w, \quad L^v = L_w, \quad U^v = U_w.$$

These objects are defined only up to noncanonical isomorphisms, but $H^r(G^v, L^{v\times})$ and $H^r(G^v, U^v)$ are defined up to *canonical* isomorphisms.

We endow $\mathbb{I}_L$ with the action of G such that the inclusions

$$\prod_{w|v} L_w^\times \to \mathbb{I}_L$$

are G-homomorphisms. Thus if α has a_w in the w-position, then $\sigma\alpha$ has σa_w in the σwposition.

PROPOSITION 2.5(a) *The map $\mathbb{I}_K \hookrightarrow \mathbb{I}_L$ induces an isomorphism $\mathbb{I}_K \to \mathbb{I}_L^G$.*

(b) *For all* $r \geq 0$,

$$H_T^r(G, \mathbb{I}_L) = \bigoplus\nolimits_v H_T^r(G^v, L^{v\times}).$$

PROOF. (a) Clearly $\alpha = (a_w)$ is fixed by G if and only if each subfamily $(a_w)_{w|v}$ is fixed by G. But $(a_w)_{w|v}$ is fixed by G only if a_w is independent of w and lies in $\dot{K}_v^\times$.

(b) For each finite set S of primes of K, let

$$\mathbb{I}_{L,S} = \prod_{v\in S}(\prod_{w|v} L_w^\times) \times \prod_{v\notin S}(\prod_{w|v} U_w).$$

Then $\mathbb{I}_{L,S}$ is stable under the action of G, and $\mathbb{I}_L$ is the directed union of the $\mathbb{I}_{L,S}$ as S runs over the finite sets of primes of K containing all infinite primes and all primes that ramify in L. Hence (see II, 4.4),

$$H^r(G, \mathbb{I}_L) = \varinjlim H^r(G, \mathbb{I}_{L,S}).$$

On applying (II, 1.25) and (2.3), we find that

$$\begin{aligned} H^r(G, \mathbb{I}_{L,S}) &= \prod_{v\in S} H^r(G, \textstyle\prod_{w|v} L_w^\times) \times \prod_{v\notin S} H^r(G, \prod_{w|v} U_w) \\ &= \prod_{v\in S} H^r(G^v, L^{v\times}) \times \prod_{v\notin S} H^r(G^v, U^v). \end{aligned}$$

Because of (III, 1.1), the second factor is zero when $r > 0$, and so

$$\begin{aligned} H^r(G, \mathbb{I}_L) &= \varinjlim\nolimits_S H^r(G, \mathbb{I}_{L,S}) \\ &= \varinjlim\nolimits_S \bigoplus\nolimits_{v\in S} H^r(G^v, L^{v\times}) \\ &= \bigoplus\nolimits_{\text{all } v} H^r(G^v, L^{v\times}). \end{aligned}$$

The same argument works for $r \leq 0$ when one uses the Tate groups. □

COROLLARY 2.6(a) $H^1(G, \mathbb{I}_L) = 0$;

(b) $H^2(G, \mathbb{I}_L) \simeq \bigoplus_v \left(\frac{1}{n_v}\mathbb{Z}/\mathbb{Z}\right)$, *where* $n_v = [L^v : K_v]$.

PROOF. (a) Apply Hilbert's theorem 90 (II, 1.22).

(b) From Theorem 2.1 of Chapter III, we know that the invariant map gives an isomorphism

$$H^2(G^v, L^{v\times}) \to \frac{1}{n_v}\mathbb{Z}/\mathbb{Z}.$$

□

PROPOSITION 2.7 *Let S be a finite set of primes of K, and let T be the set of primes of L lying over primes in S. If L/K is cyclic, then the Herbrand quotient*

$$h(\mathbb{I}_{L,T}) = \prod_{v\in S} n_v, \quad n_v = [L^v : K_v].$$

PROOF. We have

$$\mathbb{I}_{L,T} = \Big(\prod_{v\in S}(\prod_{w|v} L_w^\times)\Big) \times \Big(\prod_{v\notin S}(\prod_{w|v} U_w)\Big).$$

The Herbrand quotient of the second factor is 1 (apply III, 2.5), and so

$$\begin{aligned} h(G, \mathbb{I}_{L,T}) &= \prod_{v \in S} h(G, \textstyle\prod_{w|v} L_w^\times) \\ &= \prod_{v \in S} h(G^v, L^{v\times}) \\ &= \prod_{v \in S} \left|H^2(G^v, L^{v\times})\right| \\ &= \prod_{v \in S} n_v. \end{aligned}$$

□

The norm map on ide´les

Let L/K be a finite Galois extension of number fields. As for any G-module, there is a norm map

$$x \mapsto \prod_{\sigma \in G} \sigma x \colon \mathbb{I}_L \to \mathbb{I}_L^G = \mathbb{I}_K.$$

We need to examine this map. Recall (ANT, 8.4) that there is a commutative diagram:

$$\begin{array}{ccc} L^\times & \longrightarrow & \prod_{w|v} L_w^\times \\ \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle (a_w) \mapsto \prod \mathrm{Nm}_{L_w/K_v} a_w} \\ K^\times & \longrightarrow & K_v^\times. \end{array}$$

For every w, $\mathrm{Nm}\, L_w^\times$ is open in $K_v^\times$ (because it is of finite index; see I, 1.3), and for any unramified w, the norm map sends U_w onto U_v (see III, 1.2). The image of the right hand vertical map in the diagram is equal to $\mathrm{Nm}\, L_w^\times$ for any $w|v$ (because any two L_w's are K_v-isomorphic). We denote it by $\mathrm{Nm}\, L^{v\times}$.

Let $S \supset S_\infty$ be a finite set of primes of K containing those that ramify, and let T be the set of primes lying over a prime of S. The above remarks show that

$$\mathrm{Nm}_{L/K}\, \mathbb{I}_{L,T} = \prod_{v \in S} V_v \times \prod_{v \notin S} U_v,$$

where V_v is an open subgroup of finite index $K_v^\times$. This is an open subgroup in $\mathbb{I}_{K,S}$ and $\mathbb{I}_{K,S}$ is open in $\mathbb{I}_K$. We have proved the following result.

PROPOSITION 2.8 *For every finite Galois extension L/K of number fields, $\mathrm{Nm}_{L/K}\, \mathbb{I}_L$ contains an open subgroup of $\mathbb{I}_K$ and therefore is itself open.*

In fact, we showed earlier (V, 4.13) that every norm group contains $W_\mathfrak{m}$ for some modulus $\mathfrak{m}$, and $W_\mathfrak{m}$ is open.

We next consider the norm map on ide'le classes. Consider

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L^\times & \longrightarrow & \mathbb{I}_L & \longrightarrow & \boldsymbol{C}_L & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & & & \\ 0 & \longrightarrow & K^\times & \longrightarrow & \mathbb{I}_K & \longrightarrow & \boldsymbol{C}_K & \longrightarrow & 0. \end{array}$$

The left hand square commutes, and so the norm map $\mathbb{I}_L \to \mathbb{I}_K$ induces a norm map $\mathrm{Nm}_{L/K} \colon \boldsymbol{C}_L \to \boldsymbol{C}_K$. From the snake lemma, we find that the quotient map $\mathbb{I}_K \to \boldsymbol{C}_K$ induces an isomorphism

$$\mathbb{I}_K / K^\times \cdot \mathrm{Nm}(\mathbb{I}_L) \to \boldsymbol{C}_K / \mathrm{Nm}(\boldsymbol{C}_L).$$

3 The Cohomology of the Units

Let L/K be a finite extension of number fields with Galois group G. Let $S \supset S_\infty$ be a finite set of primes of K, and let T be the set of primes of L lying over a prime of K in S. Because T is stable under the action of G, the group of T -units

$$U(T) \stackrel{\text{def}}{=} \{\alpha \in L \mid \text{ord}_w(\alpha) = 0 \text{ all } w \notin T\}$$

is also stable under G.

PROPOSITION 3.1 *In the above situation, assume that G is cyclic. Then the Herbrand quotient $h(U(T))$ is defined, and satisfies*

$$n \cdot h(U(T)) = \prod_{v \in S} n_v,$$

where $n = [L : K]$ and $n_v = [L^v : K_v]$.

We first show that any two G-stable full lattices[2] in the same real vector space have the same Herbrand quotient. Then we construct two suc h lattices, one with Herbrand quotient $n \cdot h(U(T))$ and the other with Herbrand quotient $\prod n_v$.

LEMMA 3.2 *Let G be a finite group, and let k be an infinite field. Let M and N be $k[G]$- modules that are of finite dimension when regarded as k-vector spaces. If $M \otimes_k \Omega$ and $N \otimes_k \Omega$ are isomorphic as $\Omega[G]$ modules for some field $\Omega \supset k$, then they are already isomorphic as $k[G]$-modules.*

PROOF. First note that if V is the space of solutions for a system of homogeneous linear equations over k, then the solution space for the same system of equations over Ω admits a basis with coordinates in k. In fact, the standard algorithm for finding a basis for the solution space yields the same result when carried out over k or Ω.

A k-linear map $\alpha: M \to N$ is a G-homomorphism if $\alpha(\sigma m) = \sigma\alpha(m)$ all $m \in M, \sigma \in G$. Once bases have been chosen for M and N , giving a k-linear map $\alpha: M \to N$ is the same as giving a matrix A, and the condition that α be a G-homomorphism takes the form $A \cdot B(\sigma) = C(\sigma) \cdot A$ for certain matrices $B(\sigma)$ and $C(\sigma)$. This is a linear condition on the coefficients of A, and so the remark shows that there are $k[G]$-homomorphisms $\alpha_1, \dots, \alpha_r: M \to N$ that form an Ω-basis for the space of $\Omega[G]$-homomorphisms $M \otimes_k \Omega \to N \otimes_k \Omega$.

Because $M \otimes_k \Omega$ and $N \otimes_k \Omega$ are isomorphic as $\Omega[G]$-modules, there exist $a_1, \dots, a_r \in \Omega$ such that $\sum a_i\alpha_i$ is an isomorphism, and hence has nonzero determinant. But $\det(\sum a_i\alpha_i)$ is a polynomial in the a_i with coefficients in k, and the preceding sentence shows that not all of its coefficients are zero. As k is infinite, there exist a_i's in k such that $\sum a_i\alpha_i$ has nonzero determinant[3], and hence is a $k[G]$-isomorphism $M \to N$. □

REMARK 3.3 For those who find the above proof too simple, here is another. Assume that k has characteristic zero. The group H of automorphisms of M as a $k[G]$-module is a product of groups of the form $\text{GL}_d(D)$, D a division algebra over k. The functor of isomorphisms $M \to N$ is a principal homogeneous space for H (nonempty, because there exists an isomorphism over some field containing k), and hence defines an element of $H^1(k, H)$. Now a generalization of Hilbert's theorem 90 shows that $H^1(k, H) = 1$.

LEMMA 3.4 *Let G be a finite cyclic group, and let M and N be G-modules that are finitely generated as $\mathbb{Z}$-modules, and such that $M \otimes_{\mathbb{Z}} \mathbb{Q}$ and $N \otimes_{\mathbb{Z}} \mathbb{Q}$ are isomorphic as G-modules. If either $h(M)$ or $h(N)$ is defined, so also is the other, and the two are equal.*

[2]Recall that a subgroup M of a real vector space V is called a **full lattice** if M is the $\mathbb{Z}$-submodule generated by a basis for V ; equivalently, if it is finitely generated and the canonical map $\mathbb{R}\otimes_{\mathbb{Z}} M \to V$ is an isomorphism. The definition of a full lattice in a $\mathbb{Q}$-vector space is similar.

[3]We are using that a polynomial f with coefficients in an infinite field k is zero if $f(a_1,\dots,a_n)=0$ for all $(a_1,\dots)\in k^n$ (FT, proof of 5.18).

PROOF. After (II, 3.9), we may assume that M and N are torsion free. Choose an isomorphism

$$\alpha\colon M\otimes\mathbb{Q}\to N\otimes\mathbb{Q}.$$

Then $\alpha(M)$ and N are lattices in the same $\mathbb{Q}$-vector space, and so $\alpha(M)\subset n^{-1}N$ for some $n\in\mathbb{N}$ (express the elements of a basis for $\alpha(M)$ in terms of a bases for N , and let n be a common denominator for the coefficients). After replacing α with $n\alpha$, we have that $\alpha(M)\subset N$. Now we have an exact sequence

$$0\to M\xrightarrow{\alpha} N\to N/\alpha(M)\to 0$$

with $N/\alpha(M)$ finite, and we can apply (II, 3.9) again to deduce that $h(M)=h(N)$. □

LEMMA 3.5 *Let G be a finite cyclic group, and let V be a real vector space on which G acts linearly (i.e., V is an $\mathbb{R}[G]$-module). Let M and N be two G-stable full lattices in V . If either $h(M)$ or $h(N)$ is defined, then so is the other, and they are equal.*

PROOF. Because M and N are full lattices in V , the canonical maps

$$M\otimes_{\mathbb{Z}}\mathbb{R}\to V,\quad N\otimes_{\mathbb{Z}}\mathbb{R}\to V$$

are isomorphisms. These maps are G-homomorphisms, and therefore (3.2) $M\otimes_{\mathbb{Z}}\mathbb{Q}\approx N\otimes_{\mathbb{Z}}\mathbb{Q}$ as $\mathbb{Q}[G]$-modules, and we can apply Lemma 3.4. □

We now complete the proof of the Theorem. Let V be a product of copies of $\mathbb{R}$ indexed by the elements of T , i.e.,

$$V=\operatorname{Hom}(T,\mathbb{R}).$$

We let G act on V according to the rule:

$$(\sigma f)(w)=f(\sigma^{-1}w),\quad \sigma\in G,\quad w\in T.$$

The first lattice in V is $N\overset{\text{def}}{=}\operatorname{Hom}(T,\mathbb{Z})$. For each $v\in S$, choose a w lying over v, and let G^v be the decomposition group of w. The sets $G^v\cdot w$, $v\in S$, are the orbits of G acting on T . In particular, T is a disjoint union of these sets, and so

$$\operatorname{Hom}(T,\mathbb{Z})=\bigoplus\nolimits_v \operatorname{Hom}(G/G^v,\mathbb{Z}).$$

But $\operatorname{Hom}(G/G^v,\mathbb{Z})=\operatorname{Ind}_{G^v}^{G}(\mathbb{Z})$ ($\mathbb{Z}$ regarded as a trivial G^v-module). Therefore,

$$h(G,N)=\prod_v h(G,\operatorname{Ind}_{G^v}^{G}(\mathbb{Z}))=\prod h(G^v,\mathbb{Z})=\prod n_v.$$

We now define the second lattice. Let $\lambda\colon U(T)\to V$ be the map $a\mapsto(\dots,\log|a|_w,\dots)$, and let M^0 to be the image of λ. Note that λ commutes with the action of G. The kernel of λ consists of the elements a of $L^\times$ such that $|a|_w=1$ for all w (including the infinite primes). These are the roots of 1 in L, and so $h(U(T))=h(M^0)$. The product formula shows M^0 is contained in the subspace

$$V^0\colon\sum x_w=0,$$

of V , and the proof of the T -unit theorem shows that M^0 is a lattice in V^0 (cf. ANT, 5.8). The vector $e = (1, 1, \dots, 1)$ is stable under G, and we define $M = M^0 + \mathbb{Z}e$. Then $M \otimes_{\mathbb{Z}} \mathbb{R} = V^0 + \mathbb{R}e = V$, and so M is a lattice in V . Moreover,

$$h(M) = h(M^0) \cdot h(\mathbb{Z}) = h(M^0) \cdot n.$$

This completes the proof Proposition 3.1.

4 Cohomology of the Idèle Classes I: the First Inequality

Let L/K be a finite Galois extension of number fields with Galois group G. We have a commutative diagram of G-modules with exact rows,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K^\times & \longrightarrow & \mathbb{I}_K & \longrightarrow & \boldsymbol{C}_K & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & L^\times & \longrightarrow & \mathbb{I}_L & \longrightarrow & \boldsymbol{C}_L & \longrightarrow & 0, \end{array}$$

That the rows are exact is the definition of the ide'le class groups. The vertical arrows in the left hand square are the natural inclusions. The square therefore commutes, which shows that the right hand vertical arrow exists.

LEMMA 4.1 *The canonical map $\boldsymbol{C}_K \to \boldsymbol{C}_L$ induces an isomorphism*

$$\boldsymbol{C}_K \to \boldsymbol{C}_L^G = H^0(G, \boldsymbol{C}_L).$$

PROOF. From the bottom row of the above diagram, we obtain a cohomology sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^0(G, L^\times) & \longrightarrow & H^0(G, \mathbb{I}_L) & \longrightarrow & H^0(G, \boldsymbol{C}_L) & \longrightarrow & H^1(G, L^\times) \\ & & \| & & \| & & \| & & \| \\ & & L^{\times G} & & \mathbb{I}_L^{\times G} & & \boldsymbol{C}_L^G & & 0 \end{array}$$

which can be identified with

$$0 \to K^\times \to \mathbb{I}_K \to \boldsymbol{C}_K \to 0.$$

□

The ideal class group of a number field is finite, and it is generated by the classes of prime ideals. Therefore, it is generated by a finite number of prime ideals.

LEMMA 4.2 *Let K be a number field, and let $S \supset S_\infty$ be a finite set of primes of K containing a set of generators for the ideal class group of K. Then*

$$\mathbb{I}_K = K^\times \cdot \mathbb{I}_S.$$

PROOF. The condition that S contains a set of generators for the ideal class group of K means that every fractional ideal $\mathfrak{a}$ can be written

$$\mathfrak{a} = \mathfrak{b} \cdot (c)$$

with $\mathfrak{b}$ in the group generated by the prime ideals in S and $c \in K^\times$. Therefore, $\mathfrak{a} = (c)$ in the quotient group $I^S = I/\langle S \rangle$, and so $I^S/i(K^\times) = 0$.

For every finite set $S \supset S_\infty$ of primes of K, the natural map $\mathbb{I} \to I^S$ defines an isomorphism $\mathbb{I}/\mathbb{I}_S \to I^S$. On dividing out by $K^\times$ on both sides, we find that $\mathbb{I}/K^\times \cdot \mathbb{I}_S \simeq I^S/i(K^\times) \simeq 0$. □

Recall that we want to prove that for every abelian extension L/K, $\boldsymbol{C}_K/\operatorname{Nm}_{L/K}\boldsymbol{C}_L \simeq \operatorname{Gal}(L/K)$ and that for every Galois extension $H^1(G, C_L) = 1$. For a cyclic extension, the two statements imply that the Herbrand quotient

$$h(\boldsymbol{C}_L) \stackrel{\text{def}}{=} \frac{(\boldsymbol{C}_K : \operatorname{Nm}\boldsymbol{C}_L)}{\left|H^1(G, \boldsymbol{C}_L)\right|} = [L : K].$$

As a first step, we verify this equality.

THEOREM 4.3 *For every finite cyclic extension L/K of number fields, $h(\boldsymbol{C}_L) = [L : K]$.*

PROOF. Let S any finite set of primes of K such that:

(a) $S \supset S_\infty$, the set of infinite primes of K;

(b) S contains all primes that ramify in L;

(c) S contains the prime ideals $\mathfrak{P} \cap \mathcal{O}_K$ for a set of generators $\mathfrak{P}$ of the ideal class group of L.

Let T be the set of primes of L lying over a prime in S. Condition (c) implies that $\mathbb{I}_L = \mathbb{I}_{L,T} \cdot L^\times$, and so

$$\boldsymbol{C}_L \stackrel{\text{def}}{=} \mathbb{I}_L/L^\times = L^\times \cdot \mathbb{I}_{L,T}/L^\times \simeq \mathbb{I}_{L,T}/L^\times \cap \mathbb{I}_T.$$

Note that

$$L^\times \cap \mathbb{I}_T = \{\alpha \in L \mid \operatorname{ord}_w(\alpha) = 0\,, \forall w \notin T\} = U(T),$$

and so

$$h(\boldsymbol{C}_L) = h(\mathbb{I}_{L,T})/h(U(T)).$$

The theorem now follows from Proposition 2.7 and Proposition 3.1. □

COROLLARY 4.4 (FIRST INEQUALITY) *If L/K is cyclic of degree n, then*

$$(\mathbb{I}_K : K^\times \cdot \operatorname{Nm}(\mathbb{I}_L)) \geq n.$$

PROOF. Since $h(\boldsymbol{C}_L) = n$, its numerator must be $\geq n$. □

We now give some application of the First Inequality.

LEMMA 4.5 *Let L be a finite solvable extension of K (i.e., a finite Galois extension with solvable Galois group). If there exists a subgroup D of $\mathbb{I}_K$ such that*

(a) $D \subset \operatorname{Nm}_{L/K}\mathbb{I}_L$; *and*

(b) $K^\times \cdot D$ *is dense in $\mathbb{I}_K$ then $L = K$.*

PROOF. If $L \neq K$, then the exists a subfield K' of L that is cyclic over K and $\neq K$. Then

$$D \subset \operatorname{Nm}_{L/K}(\mathbb{I}_L) = \operatorname{Nm}_{K'/K}(\operatorname{Nm}_{L/K}\mathbb{I}_L)) \subset \operatorname{Nm}_{K'/K}(\mathbb{I}_{K'}).$$

Therefore, $K^\times \cdot \operatorname{Nm}_{K'/K}\mathbb{I}_{K'}$ is dense in $\mathbb{I}_K$. Because it is a union of translates of $\operatorname{Nm}_{K'/K}\mathbb{I}_{K'}$, it is open (2.8), and because it is a subgroup of $\mathbb{I}_K$, it is also closed. Therefore, $K^\times \cdot \operatorname{Nm}_{K'/K}\mathbb{I}_{K'} = \mathbb{I}_K$, and the first inequality implies that $K' = K$. □

PROPOSITION 4.6 *Let L be a finite solvable extension of K. If $L \neq K$, then there are infinitely many primes of K that do not split completely in L.*

PROOF. Suppose there are only finitely many, and let $S \supset S_\infty$ be a finite set of primes of K including all those that do not split completely. We shall apply the lemma with

$$D = \mathbb{I}^S \stackrel{\text{def}}{=} \{(a_v) \mid a_v = 1 \text{ for all } v \in S\}.$$

For $w|v \notin S$, $L_w = K_v$, and so clearly $D \subset \mathrm{Nm}(\mathbb{I}_L)$. Let $\mathbf{a} = (a_v) \in \mathbb{I}$. By the Weak Approximation Theorem (ANT, 7.20), there is an element $b \in K^\times$ that is very close to a_v in K_v for all $v \in S$. Choose $\mathbf{a}'$ to be the element of $\mathbb{I}^S$ such that the v component of $b\mathbf{a}'$ is equal to a_v for all $v \notin S$. Then $b\mathbf{a}'$ is close to $\mathbf{a}$ in $\mathbb{I}_K$. Hence $K^\times \cdot D$ is dense in $\mathbb{I}_K$. □

PROPOSITION 4.7 *Let L/K be a finite solvable extension with Galois group G, and let T be a finite set of prime ideals containing those that ramify in L. Then the Frobenius elements $(\mathfrak{P}, L/K)$ for $\mathfrak{P} \notin T$ generate G.*

PROOF. After possibly replacing T with a larger set, we may suppose that it is stable under G. Then the subgroup H of G generated by the Frobenius elements at the $\mathfrak{P} \notin T$ is normal. Let $E = L^H$. Recall (V, 1.11) that

$$(\mathfrak{P} \cap E, E/K) = (\mathfrak{P}, L/K)|_E,$$

which is the identity map. Therefore all primes $\mathfrak{p}$ of K not lying under a prime of T split in E, which shows that $E = K$. By the main theorem of Galois theory, this implies that $H = G$. □

COROLLARY 4.8 *For every abelian extension L/K and finite set of primes $S \supset S_\infty$ of K including the primes that ramify in L, the map*

$$\mathfrak{p} \mapsto (\mathfrak{p}, L/K)\colon I^S \to \mathrm{Gal}(L/K)$$

is surjective. (Recall that I^S is the group of fractional ideals generated by prime ideals not in S.)

PROOF. The image contains the Frobenius elements $(\mathfrak{P}, L/K)$ for all $\mathfrak{P}$ dividing a prime $\mathfrak{p}$ not in S, and these generate $\mathrm{Gal}(L/K)$. □

REMARK 4.9 Of course, Proposition 4.6 is much weaker than the result available using complex analysis—see Theorem VI.3.4—but it suffices for the proof of the Reciprocity Law.

5 Cohomology of the Idèle Classes II: The Second Inequality

THEOREM 5.1 *Let L/K be a Galois extension of number fields with Galois group G. Then*

(a) *(second inequality) the index $(\mathbb{I}_K : K^\times \cdot \mathrm{Nm}(\mathbb{I}_L))$ is finite, and divides $[L : K]$;*

(b) *the group $H^1(G, \boldsymbol{C}_L) = 0$;*

(c) *the group $H^2(G, \boldsymbol{C}_L)$ is finite, and its order divides $[L : K]$.*

LEMMA 5.2 *If G is cyclic, then statements (a), (b), and (c) of the theorem are equivalent (and $(\mathbb{I}_K : K^\times \cdot \mathrm{Nm}(\mathbb{I}_L)) = (H^2(G, \boldsymbol{C}_L) : 1) = [L : K]$).*

PROOF. Without restriction on G,

$$\mathbb{I}_K/K^\times \cdot \mathrm{Nm}_{L/K}(\mathbb{I}_L) \simeq \boldsymbol{C}_K/\mathrm{Nm}_{L/K}(\boldsymbol{C}_L) = H^0_T(G, \boldsymbol{C}_L).$$

If G is cyclic, its cohomology is periodic, and so $H^0_T(G, \boldsymbol{C}_L) \approx H^2(G, \boldsymbol{C}_L)$. This proves that (a) and (c) are equivalent. Theorem 4.3 states that the Herbrand quotient $h(\boldsymbol{C}_L) = [L : K]$, and so each of (a) and (c) is equivalent to (b). □

LEMMA 5.3 *It suffices to prove the theorem in the case that G is a p-group, p prime.* PROOF. Recall (II, 1.33), that if H is the Sylow p-subgroup of G then, for every G-module M, the maps

$$\mathrm{Res} : H^r_T(G, M) \to H^r_T(H, M)$$

are injective on the p-primary components. Therefore, if the theorem holds for L/L^H, then p does not divide the order of $H^1_T(G, \boldsymbol{C}_L)$ and the power of p dividing the orders $H^0_T(G, \boldsymbol{C}_L)$ and $H^2_T(G, \boldsymbol{C}_L)$ is less than the power of p dividing $[L : K]$. On applying this for all p, we obtain the lemma. □

LEMMA 5.4 *It suffices to prove the theorem in the case that G is a cyclic group of prime order p.*

PROOF. After the last lemma, we may assume that G is a p-group. We shall prove the theorem for G by induction on $(G:1)$. Because G is a p-group, it has a normal subgroup H of index p (see GT 4.17). Consider the exact sequence (II, 1.34)

$$0 \to H^1(G/H, \boldsymbol{C}_{K'}) \xrightarrow{\text{Inf}} H^1(G, \boldsymbol{C}_L) \xrightarrow{\text{Res}} H^1(H, \boldsymbol{C}_L),$$

where $K' = L^H$. By assumption $H^1(G/H, \boldsymbol{C}_{K'}) = 0$ and by induction $H^1(H, \boldsymbol{C}_L) = 0$. Therefore $H^1(G, \boldsymbol{C}_L) = 0$—statement (b) is true.

Because $H^1(H, \boldsymbol{C}_L) = 0$, the sequence

$$0 \to H^2(G/H, \boldsymbol{C}_{K'}) \to H^2(G, \boldsymbol{C}_L) \to H^2(H, \boldsymbol{C}_L)$$

is exact, from which it follows that statement (c) is true.

Finally, note that

$$(\boldsymbol{C}_K : \mathrm{Nm}_{L/K}(\boldsymbol{C}_L)) = (\boldsymbol{C}_K : \mathrm{Nm}_{K'/K}(\boldsymbol{C}_{K'}))(\mathrm{Nm}_{K'/K}(\boldsymbol{C}_{K'}) : \mathrm{Nm}_{L/K}(\boldsymbol{C}_L)),$$

which divides $p[L:K']$ because $\mathrm{Nm}_{K'/K}$ defines a surjection

$$\boldsymbol{C}_{K'}/\mathrm{Nm}_{L/K'}(\boldsymbol{C}_L) \to \mathrm{Nm}_{K'/K}(\boldsymbol{C}_{K'})/\mathrm{Nm}_{L/K}(\boldsymbol{C}_L). \qquad \square$$

To finish the proof of Theorem 5.1 using Lemma 5.2, it therefore remains to prove that the Second Inequality holds for a cyclic extension of degree p, but in VI 4.9 we proved that the Second Inequality holds for all finite Galois extensions. (For the translation between the idealic and the ide'lic form of the statement, see Proposition V 4.6). In the next section, we give an algebraic proof of the Second Inequality, independent of Chapter VI.

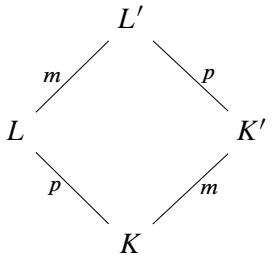
REMARK 5.5 To a finite Galois extension L/K of number fields, we have attached the group $\boldsymbol{C}_K/\mathrm{Nm}(\boldsymbol{C}_L)$ and $H^2(G, \boldsymbol{C}_L)$. When L/K is cyclic, they are canonically (up to a choice of a generator for G) isomorphic, but not otherwise. The first group is always isomorphic to G^{ab}, and the second is always cyclic of order $[L:K]$. Thus, when G is abelian but not cyclic, the two groups have the same order but are not isomorphic, and when G is nonabelian, they have different orders.

6 The Algebraic Proof of the Second Inequality

We shall prove the Second Inequality in the case that L/K is cyclic of prime degree p.

LEMMA 6.1 *It suffices to prove the Second Inequality in the case that K contains a pth root of 1.*

PROOF. Let ζ be a primitive pth root of 1 (in some fixed algebraic closure of K containing L), and let $K' = K[\zeta]$ and $L' = K' \cdot L = L[\zeta]$. Then $[K':K] = m | p-1$, and so is relatively prime to p. Hence $K' \cap L = K$, and we have the picture:



The map

$$\mathrm{Gal}(L'/K) \to \mathrm{Gal}(L/K) \times \mathrm{Gal}(K'/K)$$

is an isomorphism. Consider the diagram:

$$\begin{array}{ccccccc}
\boldsymbol{C}_L & \xrightarrow{\mathrm{Nm}_{L/K}} & \boldsymbol{C}_K & \longrightarrow & \boldsymbol{C}_K/\mathrm{Nm}\,\boldsymbol{C}_L & \longrightarrow & 0 \\
\downarrow{\scriptstyle i_L} & & \downarrow{\scriptstyle i_K} & & \downarrow & & \\
\boldsymbol{C}_{L'} & \xrightarrow{\mathrm{Nm}_{L'/K'}} & \boldsymbol{C}_{K'} & \longrightarrow & \boldsymbol{C}_{K'}/\mathrm{Nm}\,\boldsymbol{C}_{L'} & \longrightarrow & 0 \\
\downarrow{\scriptstyle \mathrm{Nm}_{L'/L}} & & \downarrow{\scriptstyle \mathrm{Nm}_{K'/K}} & & \downarrow & & \\
\boldsymbol{C}_L & \xrightarrow{\mathrm{Nm}_{L/K}} & \boldsymbol{C}_K & \longrightarrow & \boldsymbol{C}_K/\mathrm{Nm}\,\boldsymbol{C}_L & \longrightarrow & 0
\end{array}$$

Here i_L and i_K are the maps induced by the inclusions $\mathbb{I}_L \hookrightarrow \mathbb{I}_{L'}$ and $\mathbb{I}_K \hookrightarrow \mathbb{I}_{K'}$, $\mathrm{Nm}_{L/K}$ and $\mathrm{Nm}_{L'/K'}$ are the maps

$$x \mapsto \sum\nolimits_{\sigma} \sigma x, \quad \sigma \in \mathrm{Gal}(L/K) \simeq \mathrm{Gal}(L'/K'),$$

and $\mathrm{Nm}_{L'/L}$ and $\mathrm{Nm}_{K'/K}$ are the maps

$$x \mapsto \sum\nolimits_{\sigma} \sigma x, \quad \sigma \in \mathrm{Gal}(L'/L) \simeq \mathrm{Gal}(K'/K).$$

Clearly the squares at left commute, and this implies that the rest of the diagram exists. The composites

$$\mathrm{Nm}_{L'/L} \circ i_L \text{ and } \mathrm{Nm}_{K'/K} \circ i_K$$

are both multiplication by m. Therefore the composite

$$\boldsymbol{C}_K/\mathrm{Nm}\,\boldsymbol{C}_L \to \boldsymbol{C}_{K'}/\mathrm{Nm}\,\boldsymbol{C}_{L'} \to \boldsymbol{C}_K/\mathrm{Nm}\,\boldsymbol{C}_L$$

is also multiplication by m, and hence is an isomorphism (clearly, pth powers in $\boldsymbol{C}_K$ are norms, and so $\boldsymbol{C}_K/\mathrm{Nm}\,\boldsymbol{C}_L$ is killed by p). In particular, the second map is surjective, and so

$$(\boldsymbol{C}_K : \mathrm{Nm}\,\boldsymbol{C}_L) \text{ divides } (\boldsymbol{C}_{K'} : \mathrm{Nm}\,\boldsymbol{C}_{L'}),$$

which by assumption, divides p. □

We shall prove the Second Inequality in the case the K contains a primitive pth root of 1 and L is a finite abelian extension of K of exponent p with Galois group G. Let $[L : K] = p^r$, so that $G \approx (\mathbb{Z}/p\mathbb{Z})^r$. By Kummer theory (see the appendix to this chapter), there exist $a_1, \dots, a_r \in K$ such that

$$L = K[a_1^{\frac{1}{p}}, \dots, a_r^{\frac{1}{p}}].$$

Let S be a finite set of primes of K such that

(a) S contains the infinite primes;

(b) S contains all divisors of p;

(c) S is so large that all a_i are S-units.

(d) S contains a set of generators for the ideal class group of K, and so $\mathbb{I}_K = \mathbb{I}_{K,S} \cdot K^\times$ (see 4.2).

Note that, according to (A.5), conditions (b) and (c) imply that S contains all primes that ramify in L.

As usual, we write $U(S)$ for the group of S-units, i.e., the group of elements of $K^\times$ that are units for all primes outside S. Recall that the unit theorem says that

$$U(S) \approx \mathbb{Z}^{s-1} \times U(S)_{\mathrm{tors}}, \qquad s = |S|\,.$$

The group $U(S)$ tors is cyclic, and in our case its order is divisible by p (because it contains μ_p), and so

$$U(S)/U(S)^p \approx (\mathbb{Z}/p\mathbb{Z})^s.$$

Let $M = K[U(S)^{\frac{1}{p}}]$. This is the Kummer extension corresponding to the group

$$U(S)\cdot K^{\times p}/K^{\times p} \simeq U(S)/U(S)\cap K^{\times p} = U(S)/U(S)^p \approx (\mathbb{Z}/p\mathbb{Z})^s.$$

We therefore have extensions

$$M \overset{p^t}{\supset} L \overset{p^r}{\supset} K, \qquad r+t=s.$$

LEMMA 6.2 *There exists a finite set of primes T of K, disjoint from S, such that*

$$\{(\mathfrak{p}_v, M/K) \mid v \in T\}$$

is a basis for $\mathrm{Gal}(M/L)$ *(regarded as an $\mathbb{F}_p$-vector space).*

PROOF. Note S contains all primes of K ramified in M (by A.5). Therefore, for a prime w of M lying over a prime v not in S, the extension M_w/K_v is unramified, and hence is cyclic of exponent p. Therefore, it is either cyclic of order p or it is trivial. Thus, if $M_w \neq L_w$, then $L_w = K_v$ (here I'm using w both for the prime of M and the prime of L it divides).

According to (4.7), there exists a finite set T' of primes of M, none dividing a prime in S, such that the Frobenius elements $(\mathfrak{p}_w, M/L)$ for $w \in T'$ generate $\mathrm{Gal}(M/L)$. After replacing T' with a subset (if necessary), we may suppose that these Frobenius elements form a basis for $\mathrm{Gal}(M/L)$. Let $w \in T'$ divide the prime w_L of L and the prime w_K of K. Because $M_w \neq L_{w_L}$, we have $L_{w_L} = K_{w_K}$, and therefore $(\mathfrak{p}_w, M/L) = (\mathfrak{p}_w, M/K)$. Thus $T = \{w_K \mid w \in T'\}$ has the required property. □

Note that the order of T is t, where $p^t = [M : L]$, and that if w is a prime of M such that $w|v \in T$, then $L_w = K_v$.

LEMMA 6.3 *With the above notation, an element $a \in U(S)$ becomes a pth power in L if and only if it becomes a pth power in K_v for all $v \in T$.*

PROOF. $\Longrightarrow$: Let $a \in U(S)$. If a becomes pth power in L, then it becomes a pth power in $L_w^\times$ for all w. But if $w|v \in T$, then $L_w = K_v$, and so it becomes a pth power in K_v.

$\Longleftarrow$: Let $a \in U(S)$. Then $a^{\frac{1}{p}} \in M$. If $a^{\frac{1}{p}} \in K_v$ for all $v \in T$, then $a^{\frac{1}{p}}$ is fixed by $(\mathfrak{p}_v, M/K)$ for all $v \in T$, and hence by $\mathrm{Gal}(M/L)$. Thus, $a^{\frac{1}{p}}$ lies in L, and so $a \in L^p$. □

LEMMA 6.4 *The subgroup*

$$E = \prod_{v\in S} K_v^{\times p} \times \prod_{v\in T} K_v^\times \times \prod_{v\notin S\cup T} U_v$$

of $\mathbb{I}_K$ is contained in $\mathrm{Nm}_{L/K}(\mathbb{I}_L)$.

PROOF. Let $\mathbf{a} = (a_v) \in E$. We have to show that each component a_v of $\mathbf{a}$ is a norm.

$v \in S$: From local class field theory, we know that

$$K_v^\times/\operatorname{Nm} L_w^\times \xrightarrow{\simeq} \mathrm{Gal}(L_w/K_v).$$

Because the second group is killed by p, so also must be the first group, which means that $K_v^{\times p} \subset \operatorname{Nm} L_w^\times$.

$v \in T$: Here $L_w = K_v$, and so every element of K_v is a norm from L_w. $v \notin S \cup T$: Because L_w is unramified over K_v, the norm map $U_w \to U_v$ is surjective (see III, 1.2) □

Now

$$(\boldsymbol{C}_K : \operatorname{Nm} \boldsymbol{C}_L) = (\mathbb{I}_K : K^\times \cdot \operatorname{Nm} \mathbb{I}_L),$$

which divides $(\mathbb{I}_K : K^\times E)$, and so it remains to show that

$$\overline{(\mathbb{I}_K : K^\times E) | p^r}.$$

But $\mathbb{I}_K = K^\times \cdot \mathbb{I}_S = K^\times \cdot \mathbb{I}_S$, and so

$$(\mathbb{I}_K : K^\times E) = (K^\times \mathbb{I}_{S\cup T} : K^\times E).$$

LEMMA 6.5 *Let A, B, and C be subgroups of some abelian group, and assume that $A \supset B$. Then*

$$(AC : BC)(A \cap C : B \cap C) = (A : B)$$

in the sense that, if two of the indexes are finite, so is the third, and the equality holds.

PROOF. In the following commutative diagram, the columns and the top two rows are obviously exact, and it follows (from the snake lemma for example) that the bottom row is exact. This implies the statement.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & B \cap C & \longrightarrow & B & \longrightarrow & BC/C & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A \cap C & \longrightarrow & A & \longrightarrow & AC/C & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A \cap C/B \cap C & \longrightarrow & A/B & \longrightarrow & AC/BC & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

□

On applying the lemma with $A = \mathbb{I}_{S\cup T}$, $B = E$, and $\boldsymbol{C} = K^\times$ we find that

$$(\mathbb{I}_K : K^\times E) = \frac{(\mathbb{I}_{S\cup T} : E)}{(U(S \cup T) : K^\times \cap E)}.$$

LEMMA 6.6 *With the above notation:*

$$(\mathbb{I}_{S\cup T} : E) = p^{2s}.$$

LEMMA 6.7 *With the above notation:*

$$(U(S \cup T) : K^\times \cap E) = p^{s+t}.$$

Since $r + t = s$, this will prove the boxed formula.

PROOF (OF 6.6) Obviously $(\mathbb{I}_{S\cup T} : E) = \prod_{v\in S}(K_v^\times : K_v^{\times p})$. Since there are s primes in S and K contains p distinct pth roots of 1, the next proposition shows that

$$(\mathbb{I}_{S\cup T} : E) = \frac{p^{2s}}{\prod_{v\in S} |p|_v}.$$

By assumption, S contains all the primes for which $|p|_v \neq 1$, and so

$$\prod_{v\in S} |p|_v = \prod_{\text{all } v} |p|_v,$$

which equals 1 by the product formula. □

PROPOSITION 6.8 *Let K be a local field of characteristic zero, and let μ_n be the group of nth roots of 1 in $K^\times$. Then*

$$(K^\times : K^{\times n}) = n\frac{|\mu_n|}{|n|}.$$

If K is nonarchimedean and U is the group of units in K, then

$$(U : U^n) = \frac{|\mu_n|}{|n|}.$$

PROOF. If $K = \mathbb{C}$, the first equation becomes $1 = n\frac{n}{n^2}$, and if $K = \mathbb{R}$, it becomes $1 = n\frac{1}{n}$ when n is odd and $2 = n\frac{2}{n}$ when n is even. If K is nonarchimedean, $K^\times \approx U \times \mathbb{Z}$, and so

$$(K^\times : K^{\times n}) = (U : U^n)(\mathbb{Z} : n\mathbb{Z}) = (U : U^n)n.$$

Therefore, it remains to prove the second equation.

For an abelian group M, we write

$$h_n(M) = (M : nM)/(M_n : 1), \quad M_n = \{x \in M \mid nx = 0\}.$$

Then $h_n(M)$ is the Herbrand quotient of M regarded as a $\mathbb{Z}/n\mathbb{Z}$-module with trivial action, and so we may apply the results in II, §2.

As we saw in the proof of (III, 2.4), the exponential map defines an isomorphism from a subgroup of finite index in $\mathcal{O}_K$ onto a subgroup of finite index in U. Therefore

$$h_n(U) = h_n(\mathcal{O}_K) = (\mathcal{O}_K : n\mathcal{O}_K) \overset{\text{def}}{=} |n|^{-1}.$$

Hence

$$(U : U^n) = \frac{(U_n : 1)}{|n|}.$$

As $U_n = \mu_n$, this proves the second equation. □

PROOF (OF 6.7) Clearly $K^\times \cap E \supset U(S \cup T)^p$. It follows from the unit theorem (as before) that $(U(S \cup T) : U(S \cup T)^p) = p^{s+t}$, and so it remains to prove that

$$K^\times \cap E \subset U(S \cup T)^p.$$

This is accomplished by the next two lemmas (the first shows that the second may be applied to prove the inclusion). □

LEMMA 6.9 *With the above hypotheses, the obvious map*

$$U(S) \to \prod_{v \in T} U_v/U_v^p$$

is surjective.

PROOF. Let H be the kernel of the map. To prove that the map is surjective, we shall show that

$$(U(S) : H) = \coprod_{v \in T} (U_v : U_v^p).$$

Because T is disjoint from S, $|p|_v = 1$ for all $v \in T$, and so (6.8) shows that the right hand side is p^t. On the other hand, by Lemma 6.3, $H = U(S) \cap L^{\times p}$, and so

$$U(S)/H = U(S)/U(S) \cap L^{\times p} \simeq U(S) \cdot L^{\times p}/L^{\times p}.$$

This last group corresponds by Kummer theory (see A.3) to the extension M/L, and hence has order $[M : L] = p^t$. □

PROPOSITION 6.10 *Let K be a number field containing a primitive nth root of 1. Let S be a set primes containing the infinite primes, the divisors of n, and a set of representatives of the ideal class group of K. Let T be a set of primes disjoint from S and such that*

$$U(S) \to \prod_{v \in T} U_v/U_v^n$$

is surjective. Suppose that $b \in K^\times$ is an nth power in K_v for all $v \in S$ and a unit outside $S \cup T$. Then $b \in K^{\times n}$.

PROOF. Let $L = K[b^{\frac{1}{n}}]$—we have to show that $L = K$. Put

$$D = \prod_{v \in S} K_v^\times \times \prod_{v \in T} U_v^n \times \prod_{v \notin S \cup T} U_v.$$

By Lemma 4.5, in order to show that $L = K$, it suffices to shows that

(a) $D \subset \mathrm{Nm}_{L/K} \mathbb{I}_L$, and

(b) $D \cdot K^\times = \mathbb{I}_K$.

(a) Let $\mathbf{d} = (d_v) \in D$. We have to check that d_v is a norm from $K_v[b^{\frac{1}{n}}]$ for all v. $v \in S$: In this case $K_v[b^{\frac{1}{n}}] = K_v$, and so every element of K_v is a norm. $v \in T$: By local class field theory, the index $(K_v^\times : \mathrm{Nm}\, K_v[b^{\frac{1}{n}}]^\times)$ is equal to the degree $[K_v[b^{\frac{1}{n}}] : K_v]$, which divides n. Hence every nth power in K_v is a norm.

$v \notin S \cup T$: Because nb is a unit at v, the field $K_v[b^{\frac{1}{n}}]$ is unramified over K_v, and hence every unit is a norm.

(b) Obviously $\mathbb{I}_S/D = \prod_{v \in T} U_v/U_v^n$, and by hypothesis $U(S) \to \prod_{v \in T} U_v/U_v^n$ is surjective. Hence $\mathbb{I}_S = D \cdot U(S)$, and therefore

$$\mathbb{I}_K = \mathbb{I}_S \cdot K^\times = D \cdot U(S) \cdot K^\times = D \cdot K^\times.$$ □

This completes the proof of Theorem 5.1 (the Second Inequality).

7 Application to the Brauer Group

We let $H^2(L/K) = H^2(\mathrm{Gal}(L/K), L^\times)$ and $H^2(/K) = H^2(\mathrm{Gal}(K^{\mathrm{al}}/K), K^{\mathrm{al}\times})$. Those who have read Chapter IV will recognize that $H^2(L/K) \simeq \mathrm{Br}(L/K)$ and $H^2(/K) = \mathrm{Br}(K)$.

THEOREM 7.1 *For every Galois extension L/K of number fields (possibly infinite), the canonical map*

$$H^2(L/K) \to \bigoplus\nolimits_v H^2(L^v/K_v)$$

is injective.

PROOF. Assume initially that L/K is a finite Galois extension with Galois group G. Because $H^1(G, \boldsymbol{C}_L) = 0$, the cohomology sequence of

$$0 \to L^\times \to \mathbb{I}_L \to \boldsymbol{C}_L \to 0$$

is

$$0 \to H^2(G, L^\times) \to H^2(G, \mathbb{I}_L) \to \cdots.$$

But

$$H^2(G, L^\times) = H^2(L/K)$$

and (see 2.5)

$$H^2(G, \mathbb{I}_L) = \bigoplus H^2(G^v, L^{v\times}) = \bigoplus H^2(L^v/K_v),$$

and so this proves the theorem in this case. To obtain the theorem for an infinite extension, pass to the limit over the finite Galois subextensions. □

An extension L/K of fields is said to be **cyclotomic** if $L \subset K[\zeta]$ for some root ζ of 1. The next proposition will play a role in the proof of the global reciprocity law

PROPOSITION 7.2 *For every $\beta \in H^2(/K)$, there exists a cyclic cyclotomic extension L of K such that β maps to zero in $H^2(/L)$.*

PROOF. The theorem shows that β is determined by its images in $H^2(K_v)$, and hence by the invariants $\text{inv}_v(\beta_v) \in \mathbb{Q}/\mathbb{Z}$ (see Theorem 2.1, Chapter III). For every finite extension L of K and prime $w|v$ of L, $\text{inv}_w(\beta|L) = [L_w : K_v] \cdot \text{inv}_v(\beta)$ (ibid.), and so we have to find a cyclic cyclotomic extension L/K such that

$$[L^v : K_v] \cdot \text{inv}_v(\beta_v) = 0 \bmod \mathbb{Z}$$

for all v. Note that, because $H^2(L/K)!!H^2(/K)$ maps into the direct *sum* of the local groups, $\text{inv}_v(\beta_v) = 0$ for almost all v. Hence there exists an integer $m > 0$ such that $m\,\text{inv}_v(\beta_v) = 0$ for all v. The existence of an L with the correct properties is ensured by the next lemma. □

LEMMA 7.3 *Given a number field K, a finite set S of finite primes of K, and an integer $m > 0$, there exists a totally complex cyclic cyclotomic extension L of K such that $m|[L^v : K_v]$ for all $v \in S$.*

PROOF. It suffices to prove this for $\mathbb{O}$ and $m \cdot [K : \mathbb{Q}]$. Hence we can simply assume $K = \mathbb{Q}$.

Let l be a prime, and let ζ be a primitive l^rth root of 1 with $r > 2$. Then $\text{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}) \simeq (\mathbb{Z}/l^r\mathbb{Z})^\times$, and

$$(\mathbb{Z}/l^r\mathbb{Z})^\times \approx \begin{cases} \Delta \times C(l^{r-1}) & l \text{ odd} \\ \Delta \times C(2^{r-2}) & l = 2 \end{cases}$$

where Δ is of order $l-1$ and 2 in the two cases and $C(t)$ denotes a cyclic group of order t (Serre 1970, II, 3.2). Therefore $L(l^r) \overset{\text{def}}{=} \mathbb{Q}[\zeta]^\Delta$ is a cyclic cyclotomic extension of $\mathbb{O}$ of degree l^{r-2} or l^{r-3}.

Next consider $\mathbb{Q}_p[\zeta]$. If $p = l$, then $\mathbb{Q}[\zeta]$ is totally ramified over p, and so $[\mathbb{Q}_p[\zeta] : \mathbb{Q}_p] = [\mathbb{Q}[\zeta] : \mathbb{Q}] = \varphi(l^r)$. If $p \neq l$, then $\mathbb{Q}[\zeta]$ is totally unramified over p, and $[\mathbb{Q}_p[\zeta] : \mathbb{Q}_p]$ is the smallest integer t such that $l^r | p^t - 1$. In either case, we see that $[\mathbb{Q}_p[\zeta] : \mathbb{Q}_p] \to \infty$ as $r \to \infty$. Thus, for every p, $[L(l^r)^p : \mathbb{Q}_p]$ is a power of l that tends to ∞ as r tends to ∞.

A product of cyclic groups of distinct prime power orders is again cyclic. Therefore, for distinct primes $l_1, \dots, l_s$, $L = L(l_1^{r_1}) \cdots L(l_s^{r_s})$ will be cyclic, and clearly, by choosing $l_1^{r_1} \dots l_s^{r_s}$ to be sufficiently large, we can ensure that the local degrees $m|[L^p : \mathbb{Q}_p]$ are divisible by m for all $p \in S$. □

In more concrete terms, the two results say that: If a central simple algebra over K splits over K_v for all v, then it splits over K.

and

Every central simple algebra over K splits over a cyclic cyclotomic extension of K.

8 Completion of the Proof of the Reciprocity Law

Recall that, for a finite abelian extension L/K of number fields with Galois group G, we have defined a homomorphism $\phi_{L/K} : \mathbb{I}_K \to G$ such that $\phi_{L/K}(\mathbf{a}) = \prod_v \phi_v(a_v)$.

THEOREM 8.1(a) *Let L/K be a finite abelian extension of number fields. Then $\varphi_{L/K}$ takes the value 1 on the principal ideles $K^\times \subset \mathbb{I}_K$.*

(b) *Let L/K be a finite Galois extension of number fields. Then $\sum \mathrm{inv}_v(\alpha) = 0$ for all $\alpha \in H^2(L/K)$.*

Before proving this theorem, we explain why (a) implies the Reciprocity Law for L/K. Statement (a) says that $\phi_{L/K} : \mathbb{I}_K \to \mathrm{Gal}(L/K)$ contains $K^\times$ in its kernel. We know already that it contains $\mathrm{Nm}_{L/K}(\mathbb{I}_L)$ in its kernel[4], and therefore it defines a homomorphism

$$\mathbb{I}_K/K^\times \cdot \mathrm{Nm}_{L/K}\,\mathbb{I}_L \to \mathrm{Gal}(L/K) \qquad (*).$$

For any finite prime v of K unramified in L, $\varphi_{L/K}$ maps the idele with a prime element in v-position to the Frobenius element $(\mathfrak{p}_v, L/K)$, and so (4.7) shows that $\varphi_{L/K}$ is surjective. On the other hand, the Second Inequality (5.1) states that

$$(\mathbb{I}_K : K^\times \cdot \mathrm{Nm}_{L/K}\,\mathbb{I}_L) \le [L : K]$$

and so the homomorphism $(*)$ is an isomorphism.

EXAMPLE 8.2 We verify (8.1a) for the extension $\mathbb{Q}[\zeta_m]/\mathbb{Q}$, where ζ_m a primitive mth root of 1. We identify $\mathrm{Gal}(\mathbb{Q}[\zeta_m]/\mathbb{Q})$ with $(\mathbb{Z}/m\mathbb{Z})^\times$. Thus, for n an integer relatively prime to m, $[n]$ denotes the automorphism of $\mathbb{Q}[\zeta_m]$ sending ζ_m to ζ_m^n. It suffices to show that $\phi(a)|\mathbb{Q}[\zeta_{l^r}] = 1$ for all $l|m$. Thus, we may assume that $m = l^r$, $m \neq 2$.

The homomorphism $\phi_\infty : \mathbb{R}^\times/\mathrm{Nm}(\mathbb{C}^\times) \to \mathrm{Gal}(\mathbb{Q}[\zeta_m]/\mathbb{Q})$ sends any negative real number to complex conjugation. Therefore $\phi_\infty(a) = [\mathrm{sign}(a)]$.

Let $a = up^s \in \mathbb{Q}_p^\times$. If $p \neq l$, then p is unramified in $\mathbb{Q}[\zeta_m]$, and $\phi_p(a)$ acts as the sth power of the Frobenius at p:

$$\phi_p(up^s) = [p^s].$$

The prime l is totally ramified in $\mathbb{Q}[\zeta_m]$ and

$$\phi_l(a) = [u^{-1}]$$

(see I, 3.13).[5]

---

[4] Because this is true locally. [5] As Catherine O'Neil pointed out to me, here I'm making use of a result from I §3, contrary to my promise that §§2–4 of Chapter I can be skipped. However, it is possible to prove (a) of Theorem 8.1 in an elementary fashion for the cyclotomic extensions of $\mathbb{Q}$. For example, use the diagram in V, 5.10, to define $\phi_{\mathbb{Q}}$, and then verify that its local components are correct. This will be clarified in a future version. (See also Remark 8.3.)

It suffices to show that $\phi(a) = 1$ in the three cases: $a = -1$, $a = l$, $a =$ a prime $q \neq l$. We have:

$$\phi_p(-1) = \begin{cases} [-1] & \text{if} \quad p = \infty \\ [-1] & \text{if} \quad p = l \\ [1] & \text{if} \quad p \neq l, \infty. \end{cases}$$

$$\phi_p(l) = \begin{cases} [1] & \text{if} \quad p = l \\ [1] & \text{if} \quad p \neq l \end{cases}$$

$$\phi_p(q) = \begin{cases} [q] & \text{if} \quad p = q \\ [q^{-1}] & \text{if} \quad p = l \\ [1] & \text{if} \quad p \neq l, q. \end{cases}$$

In each case, $\prod \phi_p(a) = 1$.

REMARK 8.3 In Example V 4.10, we showed that the homomorphism $\phi : \mathbb{I}_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}[\zeta_m]/\mathbb{Q})$ attached to the Artin map $\phi : C_{\infty(m)} \to \mathrm{Gal}(\mathbb{Q}[\zeta_m]/\mathbb{Q})$ has local components equal to the local Artin maps. Since, by definition, $\phi(\mathbb{Q}^\times) = 1$, this gives an alternative proof of (8.1a) in the case $\mathbb{Q}[\zeta_m]/\mathbb{Q}$.

LEMMA 8.4(a) *If 8.1(a) holds for L/K, then it holds for every subextension.*

(b) *If 8.1(a) holds for L/K, then it holds for $L \cdot K'/K'$ for every number field $K' \supset K$.*

PROOF. (a) Suppose $L \supset K' \supset K$. Then $\phi_{K'/K}$ is the composite of $\varphi_{L/K}$ and the restriction map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(K'/K)$ (because this is true for the local Artin maps).

(b) Let $L' = L \cdot K'$. For each prime w of K', we have a commutative diagram

$$\begin{array}{ccc} K_w'^\times & \xrightarrow{\phi_w} & \mathrm{Gal}(L'^w/K_w') \\ \downarrow{\scriptstyle \mathrm{Nm}} & & \downarrow \\ K_v^\times & \xrightarrow{\phi_v} & \mathrm{Gal}(L^v/K_v). \end{array}$$

On combining them, we get a commutative diagram:

$$\begin{array}{ccc} \mathbb{I}_{K'} & \xrightarrow{\phi_{L'/K'}} & \mathrm{Gal}(L'/K') \\ \downarrow{\scriptstyle \mathrm{Nm}} & & \downarrow \\ \mathbb{I}_K & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K). \end{array}$$

Because the norm map on ide'les maps $K'^\times$ into $K^\times$, we see that this lemma follows from earlier results. □

From the Example 8.2 and Lemma 8.4, we find that (8.1a) holds for all cyclotomic extensions[6] of a number field K.

We next need to relate the two statements in Theorem 8.1.

LEMMA 8.5 *Let L/K be an abelian extension of number fields. If (8.1b) holds for L/K, then so also does (8.1a). Conversely, if L/K is cyclic and (8.1a) holds for L/K, then so also does (8.1b).*

---

[6] An extension L/K is said to be cyclotomic if $L \subset K[\zeta]$ for some root ζ of 1.

PROOF. Let $\chi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$. We can regard as an element of $H^1(G, \mathbb{Q}/\mathbb{Z})$, and then its image under the boundary map arising from the sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

is an element $\delta\chi \in H^2(G, \mathbb{Z})$. Consider the diagram,

$$\begin{array}{ccccc} K^\times & \longrightarrow & \mathbb{I}_K & \xrightarrow{\phi_{L/K}} & G \\ \downarrow{\scriptstyle \cup\delta\chi} & & \downarrow{\scriptstyle \cup\delta\chi} & & \downarrow{\scriptstyle \chi} \\ H^2(G,L^\times) & \longrightarrow & H^2(G,\mathbb{I}_L) & \longrightarrow & \mathbb{Q}/\mathbb{Z}. \end{array}$$

The first two vertical arrows are cup-product by $\delta\chi$: if $\delta\chi$ is represented by the 2-cocycle $n_{\sigma,\tau}$ then the image of x is represented by the 2-cocycle $\sigma,\tau \mapsto x^{n_{\sigma,\tau}}$. Clearly, the lefthand square commutes. The right-hand vertical map is itself. That the right hand square commutes follows from (III, 3.6). Now assume 8.1b is true for L/K. Then $\chi(\phi_{L/K}(a)) = 0$ for all characters of G, and so $\phi_{L/K}(a)$ itself is zero. Conversely, when G is cyclic, we can choose to be injective, and then 8.1a implies 8.1b since $\cup\delta\chi$ is then an isomorphism (II, 3.5). □

Since we know 8.1a for cyclotomic extensions, it follows that we know 8.1b for cyclic cyclotomic extensions. Moreover, we will have proved the whole theorem once we have proved (b) of the theorem. Thus, the next result completes the proof of the theorem

LEMMA 8.6 *If (8.1b) is true for cyclic cyclotomic extensions, then it is true for all finite Galois extensions.*

PROOF. Let $\beta \in H^2(\ /K)$. W e are given that, if $\beta \in H^2(L/K)$ for some cyclic cyclotomic extension L/K, then $\sum \mathrm{inv}_v(\beta) = 0$, where β_v is the image of β in $H^2(K_v)$, but

Proposition 7.2 says that **every** β in $H^2(K)$ lies in $H^2(L/K)$ for some cyclic cyclotomic extension L/K.

[Mention that we are using the inflation-restriction sequence

$$0 \to H^2(\mathrm{Gal}(L/K), L^\times) \to H^2(G_K, \bar{K}^\times) \to H^2(G_L, \bar{L}^\times),$$

and that β as above is in the middle group and vanishes in the right-hand group.] □

9 The Existence Theorem

In this section we prove the Existence Theorem: every open subgroup of finite index in the ideˊle class group is a norm group. A large part of the proof can be extracted from Section 6. However, at the cost of some repetition, I give a proof independent of Section 6 (except for some elementary statements).

LEMMA 9.1 *If U is a norm group, and $V \supset U$, then V also is a norm group.*

PROOF. Suppose $U = \mathrm{Nm}\, \boldsymbol{C}_L$. According to the Reciprocity Law, the Artin map defines an isomorphism

$$: \boldsymbol{C}_K/U \to \mathrm{Gal}(L/K).$$

If M is the fixed field of $\phi(V)$, then defines an isomorphism

$$\boldsymbol{C}_K/V \to \mathrm{Gal}(M/K),$$

but, according to the Reciprocity Law, the kernel of $\phi : \boldsymbol{C}_K \to \mathrm{Gal}(M/K)$ is $\mathrm{Nm}_{M/K}\, \boldsymbol{C}_M$.□

It is obvious from its factorization into primes, that a rational number a is an nth power if and only if it is an nth power in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all primes $p|a$. The proof of the analogous statement for number fields requires the Reciprocity Law (or complex analysis).

PROPOSITION 9.2 *Let K be a number field containing a primitive nth root of 1, and let $S \supset S_\infty$ be a finite set of primes of K containing all those dividing n and enough primes to generate the class group of K. Any $a \in K^\times$ such that*

◇ *a is an nth power in K_v for all $v \in S$;*

◇ *a is a unit in K_v for all $v \notin S$.*

is an nth power in K.

PROOF. [7] Let $L = K[a^{1/n}]$—because $\zeta_n \in K$, this is an abelian extension of K. For every prime $v \in S$, $X^n - a$ splits completely in $K_v[X]$, and so $L_w = K_v$ for all $w|v$. Hence the norm map $L_w^\times \to K_v^\times$ is onto. On the other hand, L is unramified over K at any prime $v \notin S$, and so the norm map $\mathrm{Nm}_{L/K} : U_w \to U_v$ is onto. Therefore, $\mathrm{Nm}_{L/K}(\mathbb{I}_L) \supset \mathbb{I}_S$, and so

$$K^\times \cdot \mathrm{Nm}_{L/K}(\mathbb{I}_L) \supset K^\times \cdot \mathbb{I}_S = \mathbb{I}_K.$$

The Reciprocity Law now shows that $L = K$, and so a is an nth power in K. □

LEMMA 9.3 (KEY CASE OF THE EXISTENCE THEOREM) *Let K be a number field con- taining a primitive pth root of 1 (p prime). Then every open subgroup V of $\boldsymbol{C}_K$ such that $\boldsymbol{C}_K/V$ is a finite group killed by p is a norm group.*

PROOF. Let $S \supset S_\infty$ be a finite set of primes of K containing the infinite primes, those dividing p, and enough primes so that $\mathbb{I}_K = K^\times \cdot \mathbb{I}_S$. Let L be the extension of K corresponding by Kummer theory to the group $U(S) \cdot K^{\times p}$, i.e., $L = K[U(S)^{\frac{1}{p}}]$, and let

$$E = \prod_{v \in S} K_v^{\times p} \times \prod_{v \notin S} U_v.$$

We shall prove that $K^\times \cdot E = K^\times \cdot \mathrm{Nm}(\mathbb{I}_L)$ by verifying that

(a) $E \subset \mathrm{Nm}(\mathbb{I}_L)$;

(b) $(\mathbb{I}_K : K^\times \cdot E) = p^s = (\mathbb{I}_K : K^\times \cdot \mathrm{Nm}_{L/K}(\mathbb{I}_L))$.

For any prime v of K and prime w of L lying over it, the local Artin map is an isomorphism

$$K_v^\times / \mathrm{Nm}(L_w^\times) \to \mathrm{Gal}(L_w/K_v).$$

Because L/K is has exponent p, $\mathrm{Nm}(L_w^\times) \supset K_v^{\times p}$.

---

[7] From Wojtek Wawro´w: Since $L = K$ in the proof is cyclic, it appears that the proof only uses the First Inequality (specifically Lemma 4.5), not the full Reciprocity Law. Regardless, it appears that this Proposition is not used anywhere.

For any prime $v \notin S$, L is unramified over K and v, and so the norm map $U_w \to U_v$ is onto.

On combining the statements in the last two paragraphs, we obtain (a). From the Reciprocity Law,

$$(\mathbb{I}_K : K^\times \cdot \mathrm{Nm}(\mathbb{I}_L)) = [L : K],$$

and from Kummer theory,

$$[L : K] = (U(S) \cdot K^{\times p} : K^{\times p}).$$

But

$$U(S) \cdot K^{\times p}/K^{\times p} \approx U(S)/U(S) \cap K^{\times p}.$$

If $a^p \in U(S)$, then $a \in U(S)$, and so $U(S) \cap K^{\times p} = U(S)^p$. Now, by the Dirichlet Unit Theorem (ANT, 5.9),

$$U(S) \approx U(S)_{\text{torsion}} \oplus \mathbb{Z}^{s-1},$$

and $U(S)$ is the group of roots of 1 in K, which is a cyclic group whose order is

torsion divisible by p. Hence $(U(S) : U(S)^p) = p^s$.

On the other hand,

$$(\mathbb{I}_K : K^\times \cdot E) = (\mathbb{I}_S \cdot K^\times : E \cdot K^\times),$$

which, by (6.5), equals

$$(\mathbb{I}_S : E)/(\mathbb{I}_S \cap K^\times : E \cap K^\times).$$

Therefore (see 6.8),

$$(\mathbb{I}_S : E) = \prod_{v \in S} (K_v^\times : K_v^{\times p}) = \prod_{v \in S} \frac{p}{|p|_v} p = p^{2s}.$$

Here, we have used that K contains a primitive pth root of 1 and that S contains all v for which $|p|_v \neq 1$, and so $\prod_{v \in S} |p|_v = \prod_{\text{all } v} |p|_v = 1$ by the product formula. It follows that $K^\times \cdot E = K^\times \cdot \operatorname{Nm} \mathbb{I}_L$.

Now let V be an open subgroup of $\boldsymbol{C}_K$ such that $\boldsymbol{C}_K/V$ is killed by p, and let U be the inverse image of V in $\mathbb{I}_K$. Then U is open in $\mathbb{I}_K$ and so there is a finite set of primes S such that $U \supset \prod_{v \in S} 1 \times \prod_{v \notin S} U_v$. Moreover, $\mathbb{I}_K/U$ has exponent p, and so $U \supset \mathbb{I}_K^p$. Hence $U \supset E \cdot K^\times$, and because $E \cdot K^\times/K^\times$ is a norm group, so also must be $U/K^\times = V$. □

For simplicity, in the proof of the next lemma, we assume the Norm Limitation Theorem, which is not proved until the next chapter. For a proof avoiding that theorem, see p. 202 of Tate's article in Cassels and Fro¨hlich 1967, 1967.

LEMMA 9.4 *Let U be an open subgroup of finite index in $\boldsymbol{C}_K$. If there exists a finite extension K'/K such that $\operatorname{Nm}_{K'/K}^{-1}(U)$ is a norm group, then so also is U.*

PROOF. Write U' for $\operatorname{Nm}_{K'/K}^{-1}(U)$, and let L be the abelian extension of K' with $\operatorname{Nm} \boldsymbol{C}_L = U'$. If M is the maximum abelian subextension of L/K, then we have

$$\operatorname{Nm}_{M/K} \boldsymbol{C}_M = \operatorname{Nm}_{L/K} \boldsymbol{C}_L = \operatorname{Nm}_{K'/K} U' \subset U$$

and we can apply Lemma 9.1. □

THEOREM 9.5 *Every subgroup U of finite index in $\boldsymbol{C}_K$ is a norm group.*

PROOF. We prove this by induction on the index of U. If the index is 1, then there is nothing to prove. Otherwise, there exists a prime p dividing $(\boldsymbol{C}_K : U)$. After (9.4) we may assume that K contains a pth root of 1. Choose a subgroup U_1 of $\boldsymbol{C}_K$ containing U and of index p in $\boldsymbol{C}_K$. After (9.3), there exists an abelian extension K' of K such that $\operatorname{Nm}_{K'/K} \boldsymbol{C}_{K'} = U_1$; moreover K' is cyclic of degree p over K. Put $U' = \operatorname{Nm}_{K'/K}^{-1} U$. The map

$$\operatorname{Nm}_{K'/K} : \boldsymbol{C}_{K'} \to \boldsymbol{C}_K/U$$

has image U_1/U and kernel U'. Hence

$$(\boldsymbol{C}_{K'} : U') = (\boldsymbol{C}_K : U)/p$$

and so, by induction, U' is a norm group. Now we can apply (9.4) to deduce that U is a norm group. □

A Appendix: Kummer theory

Throughout this subsection, K is a field containing a primitive nth root of 1, ζ. In particular, K either has characteristic 0 or characteristic p not dividing n. Write μ_n for the group of nth roots of 1 in K. Then μ_n is a cyclic subgroup of $K^\times$ of order n with generator ζ.

PROPOSITION A.1 *Let $L = K[\alpha]$, where $\alpha^n \in K$ and no smaller power of α is in K. Then L is a Galois extension of K with cyclic Galois group of order n. Conversely, if L is cyclic extension of K of degree n, then $L = K[\alpha]$ for some α with $\alpha^n \in K$.*

PROOF. See FT 5.26. □

PROPOSITION A.2 *Two cyclic extensions $K[a^{\frac{1}{n}}]$ and $K[b^{\frac{1}{n}}]$ of K of degree n are equal if and only if $a = b^r c^n$ for some $r \in \mathbb{Z}$ relatively prime to n and some $c \in K^\times$, i.e., if and only if a and b generate the same subgroup of $K^\times/K^{\times n}$.*

PROOF. See FT 5.28. □

The last two results give us a complete classification of the cyclic extensions of K of degree n when K contains a primitive nth root of 1. It is not difficult to extend this to a classification of all abelian extensions of exponent n.

THEOREM A.3 *The map*

$$L \mapsto K^\times \cap L^{\times n}/K^{\times n}$$

defines a one-to-one correspondence between the finite abelian extensions of K of exponent n contained in some fixed algebraic closure Ω of K and the finite subgroups B of $K^\times/K^{\times n}$. The extension corresponding to B is $K[B^{\frac{1}{n}}]$, the smallest subfield of Ω containing K and an nth root of each element of B. If $L \leftrightarrow B$, then $[L : K] = (B : K^{\times n})$.

PROOF. See FT 5.29. □ EXAMPLE A.4 (a) The quadratic extensions of $\mathbb{R}$ are in one-to-one correspondence with the subgroups of $\mathbb{R}^\times/\mathbb{R}^{\times 2} = \{\pm 1\}$.

(b) The finite abelian extensions of $\mathbb{Q}$ of exponent 2 are in one-to-one correspondence with the finite subgroups of

$$\mathbb{Q}^\times/\mathbb{Q}^{\times 2} \approx \{\pm 1\} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \cdots$$

(copies of $\mathbb{Z}/2\mathbb{Z}$ indexed by the prime numbers).

After this review of algebra, we return to some number theory.

PROPOSITION A.5 *Let K be a number field, and let $L = K[a_1^{\frac{1}{n}}, \cdots, a_m^{\frac{1}{n}}]$. Then L is unramified at a finite prime v of K if na_i is a unit in K_v for all i.*

PROOF. We need only consider a cyclic extension $K[a^{\frac{1}{n}}]$, which (see A.1) we can assume to have degree n. Let $\alpha = a^{\frac{1}{n}}$ and $f = X^n - a$. Then

$$\operatorname{disc} f = \pm \operatorname{Nm}_{L/K} f'(\alpha) = \pm \operatorname{Nm}_{L/K} n\alpha^{n-1} = \pm n^n a^{n-1}.$$

Thus if $\mathfrak{p}_v$ does not divide na, it does not divide disc f, and, *a fortiori,* it does not divide $\operatorname{disc}(\mathcal{O}_L/\mathcal{O}_K)$. (See ANT, Chapter 2.) □

REMARK A.6 Determining the ramification in $K[a^{\frac{1}{n}}]/K$ at prime $\mathfrak{p}$ dividing n can be quite complicated. The following summarizes what happens when $n = p$, a prime, and K contains a primitive pth root ζ of 1. Let $\pi = \zeta - 1$, and let $a \in K^\times$ be relatively prime to p and not a pth power in K.

(a)A prime $\mathfrak{p}|p$ splits completely in the extension $K[a^{\frac{1}{p}}]/K$ if and only if $X^p \equiv a \bmod p\pi\mathfrak{p}$ has a nonzero solution in $\mathcal{O}_K$ (a is then said to be **hyperprimary** at $\mathfrak{p}$).

(b)A prime $\mathfrak{p}|p$ is unramified in the extension $K[a^{\frac{1}{p}}]/K$ if and only if $X^p \equiv a \bmod p\pi$ has a nonzero solution in $\mathcal{O}_K$ (a is then said to be **primary** at $\mathfrak{p}$).

(c)The extension $K[a^{\frac{1}{p}}]/K$ is unramified at all finite primes of K if and only if a is primary and $(a) = \mathfrak{a}^p$ for some ideal $\mathfrak{a}$.

For hints of proofs of these statements, see Washington 1997, Exercise 9.3, and Cassels and Fro¨hlich 1967, Exercise 2.12, p. 353. In the case $K = \mathbb{Q}[\zeta]$, see also Cassels 1986, pp 139–140, and Fro¨hlich and Taylor 1991, III, 3.11.

SUPPLEMENT. AN INTRODUCTION TO GALOIS COHOMOLOGY AND ITS APPLICATIONS

Grégory Berhuy

1 Introduction

A recurrent problem arising in mathematics is to decide if two given mathematical structures defined over a field k are isomorphic. Quite often, it is easier to deal with this problem after scalar extension to a bigger field Ωcontaining k, for example an algebraic closure of k, or a finite Galois extension. In the case where the two structures happen to be isomorphic over Ω, this leads to the natural descent problem: if two k-structures are isomorphic over Ω, are they isomorphic over k? Of course, the answer is no in general. For example, consider the following matrices $M, M_0 \in \mathrm{M}_2(\mathbb{R})$:

$$M_0 = \begin{pmatrix} 0 & -2 \\ 1 & 0 \end{pmatrix}, M = \begin{pmatrix} 0 & 2 \\ -1 & 0 \end{pmatrix}.$$

It is easy to see that they are connjjugate by an element of $\mathrm{GL}_2(\mathbb{C})$, since they have same eigenvalues $\pm i\,2$, and therefore are both similar to

Date: March 23, 2018.

$\begin{pmatrix} i\sqrt{2} & 0 \\ 0 & -i\sqrt{2} \end{pmatrix}$. In fact we have

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} M \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}^{-1} = M_0,$$

so M and M_0 are even conjugate by an element of $\mathrm{SL}_2(\mathbb{C})$.

A classical result in linear algebra says that M and M_0 are already conjugate by an element of $\mathrm{GL}_2(\mathbb{R})$, but this is quite obvious here since the equality above rewrites

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} M \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^{-1} = M_0.$$

However, they are not conjugate by an element of $\mathrm{SL}_2(\mathbb{R})$. Indeed, it is easy to check that a matrix $P \in \mathrm{GL}_2(\mathbb{R})$ such that $PM = M_0P$ has the form

$$P = \begin{pmatrix} a & 2c \\ c & -a \end{pmatrix}.$$

Since $\det(P) = -(a^2+2c^2) < 0$, P cannot belong to $\mathrm{SL}_2(\mathbb{R})$. Therefore, M and M_0 are conjugate by an element of $\mathrm{SL}_2(\mathbb{C})$ but not by an element of $\mathrm{SL}_2(\mathbb{R})$.

Hence, the descent problem for conjugacy classes of matrices has a positive answer when we conjugate by elements of the general linear group, but has a negative one when we conjugate by elements of the special linear group. So, how could we explain the difference between these two cases? This is where Galois cohomology comes into play, and we would like now to give an insight of how this could be used to measure the obstruction to descent problems on the previous example. If k is a field, let us denote by $G(k)$ the group $\mathrm{GL}_2(k)$ or $\mathrm{SL}_2(k)$ indifferently.

Assume that $QMQ^{-1} = M_0$ for some $Q \in G(\mathbb{C})$. The idea is to measure how far is Q to have real coefficients, so it is natural to consider the difference $Q\overline{Q}^{-1}$, where Q is the matrix obtained from Q by letting the complex conjugation act coefficientwise. Indeed, we will have $Q \in G(\mathbb{R})$ if and only $Q = Q$, that is if and only if $Q\overline{Q}^{-1} = I_2$. Of course, if $Q\overline{Q}^{-1} = I_2$, then M and M_0 are conjugate by an element of $G(\mathbb{R})$, but this is not the only case when this happens to be true. Indeed, if we assume that $PMP^{-1} = M_0$ for some $P \in G(\mathbb{R})$, then we easily get that $QP^{-1} \in G(\mathbb{C})$ commutes with M_0. Therefore, there exists $C \in Z_G(M_0)(\mathbb{C}) = \{C \in G(\mathbb{C}) \mid CM_0 = M_0C\}$ such that $Q = CP$. We then easily have $Q = \overline{C}\,\overline{P} = \overline{C}P$, and therefore

$$Q\overline{Q}^{-1} = C\overline{C}^{-1} \text{ for some } C \in Z_G(M_0)(\mathbb{C}).$$

Conversely, if the equality above holds then $P = C^{-1}Q$ is an element of $G(\mathbb{R})$ satisfying $PMP^{-1} = M_0$. Indeed, we have

$$\overline{P} = \overline{C}^{-1}\overline{Q} = C^{-1}Q = P,$$

so $P \in G(\mathbb{R})$, and

$$PMP^{-1} = C^{-1}QMQ^{-1}C = C^{-1}M_0C = M_0C^{-1}C = M_0.$$

Thus, M and M_0 will be congugate by an element of $G(\mathbb{R})$ if and only if

$$Q\overline{Q}^{-1} = C\overline{C}^{-1} \text{ for some } C \in Z_G(M_0)(\mathbb{C}).$$

Notice also for later use that $Q\overline{Q}^{-1} \in G(\mathbb{C})$ commutes with M_0, as we may check by applying complex conjugation on both sides of the equality $QMQ^{-1} = M_0$.

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

In our previous example, we have $Q = \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$ and therefore $Q\overline{Q}^{-1} = -I_2$. Direct computation gives

$$Z_G(M_0)(\mathbb{C}) = \left\{ C \in G(\mathbb{C}) \;\middle|\; C = \begin{pmatrix} z & -2z' \\ z' & z \end{pmatrix} \text{ for some } z, z' \in \mathbb{C} \right\}.$$

Thus $C \in Z_G(M_0)(\mathbb{C})$ and $C\overline{C}^{-1} = Q\overline{Q}^{-1} = -I_2$ if and only if

$$C = \begin{pmatrix} iu & -2iv \\ iv & iu \end{pmatrix} \quad \text{for some } u, v \in \mathbb{R},\ (u, v) \neq (0, 0).$$

The determinant of this matrix is $-(u^2 + 2v^2) < 0$. If $G(\mathbb{C}) = \mathrm{GL}_2(\mathbb{C})$, one may take $u = 1$ and $v = 0$. If $G(\mathbb{C}) = \mathrm{SL}_2(\mathbb{C})$, the equation $C\overline{C}^{-1} = -I_2 = Q\overline{Q}^{-1}$ has no solution in $Z_G(M_0)(\mathbb{C})$. This explains the difference between the two descent problems. If $QMQ^{-1} = M_0$ for some $Q \in G(\mathbb{C})$, the matrix $Q\overline{Q}^{-1}$ measures how far M is from being conjugate to M_0 over $\mathbb{R}$.

Of course, all the results above remain valid if M and M_0 are square matrices of size n, and if $G(k) = \mathrm{GL}_n(k)$, $\mathrm{SL}_n(k)$, $\mathrm{O}_n(k)$ or even $\mathrm{Sp}_{2n}(k)$. If we have a closer look to the previous computations, we see that the reason why all this works is that $\mathbb{C}/\mathbb{R}$ is a Galois extension, whose Galois group is generated by complex conjugation.

Let us consider now a more general problem: let Ω/k be a finite Galois extension, and let $M, M_0 \in \mathrm{M}_n(k)$ two matrices such that

$$QMQ^{-1} = M_0 \text{ for some } Q \in G(\Omega).$$

Does there exists $P \in G(k)$ such that $PMP^{-1} = M_0$?

Since Ω/k is a finite Galois extension, then for all $x \in \Omega$, we have $x \in k$ if and only if $\sigma(x) = x$ for all $\sigma \in \mathrm{Gal}(\Omega/k)$. If now $Q \in G(\Omega)$, then let us denote by $\sigma\cdot Q \in G(\Omega)$ the matrix obtained from Q by letting σ act coefficientwise. Then we have

$$\begin{array}{rcl} Q \in G(k) & \iff & \sigma\cdot Q = Q \text{ for all } \sigma \in \mathrm{Gal}(\Omega/k) \\ & \iff & Q(\sigma\cdot Q)^{-1} = I_2 \text{ for all } \sigma \in \mathrm{Gal}(\Omega/k). \end{array}$$

As before, apply $\sigma \in \mathrm{Gal}(\Omega/k)$ to the equality $QMQ^{-1} = M_0$. This shows that $Q(\sigma \cdot Q)^{-1} \in Z_G(M_0)(\Omega)$ and gives the map

$$\alpha^Q : \ \mathrm{Gal}(\Omega/k) \longrightarrow Z_G(M_0)(\Omega), \qquad \sigma \longmapsto \alpha^Q_\sigma = Q(\sigma \cdot Q)^{-1}.$$

Arguing as at the beginning of this introduction, one can show that M and M_0 will be conjugate by an element of $G(k)$ if and only if there exists $C \in Z_G(M_0)(\Omega)$ such that $\alpha^Q = \alpha^C$, that is if and only if there exists $C \in Z_G(M_0)(\Omega)$ such that

$$Q(\sigma\cdot Q)^{-1} = C(\sigma\cdot C)^{-1} \text{ for all } \sigma \in \mathrm{Gal}(\Omega/k).$$

To summarize, to any matrix $M \in \mathrm{M}_n(k)$ which is conjugate to M_0 by an element of $G(\Omega)$, we may associate a map $\alpha^Q : \mathrm{Gal}(\Omega/k) \to Z_G(M_0)(\Omega)$, which measures how far is M to be conjugate to M_0 by an element of $G(k)$.

This has a kind of a converse: for any map

$$\alpha : \mathrm{Gal}(\Omega/k) \to Z_G(M_0)(\Omega), \sigma \mapsto \alpha_\sigma$$

such that $\alpha = \alpha^Q$ for some $Q \in G(\Omega)$, one may associate a matrix of $M_n(k)$ which is conjugate to M_0 by an element of $G(k)$ by setting $M_\alpha = Q^{-1}M_0Q$. To see that M_α is indeed an element of $\mathrm{M}_n(k)$, notice first that we have

$\sigma\cdot(C_1C_2) = (\sigma\cdot C_1)(\sigma\cdot C_2)$ for all $C_1, C_2 \in G(\Omega), \sigma \in \mathrm{Gal}(\Omega/k)$.

Thus, for all $\sigma \in \mathrm{Gal}(\Omega/k)$, we have

$$\begin{array}{rcl} \sigma\cdot M_\alpha & = & (\sigma\cdot Q)^{-1}M_0(\sigma\cdot Q) \\ & = & Q^{-1}Q(\sigma\cdot Q)^{-1}M_0(\sigma\cdot Q) \\ & = & Q^{-1}M_0Q(\sigma\cdot Q)^{-1}(\sigma\cdot Q) \\ & = & Q^{-1}M_0Q \\ & = & M_\alpha, \end{array}$$

the third equality coming from the fact that $\alpha_\sigma = Q(\sigma\cdot Q)^{-1}$ lies in $Z_G(M_0)(\Omega)$.

Not all the maps $\alpha : \mathrm{Gal}(\Omega/k) \to Z_G(M_0)(\Omega), \sigma \mapsto \alpha_\sigma$ may be written α^Q for some $Q \in G(\Omega)$. In fact, easy computations show that a necessary condition for this to hold is that α is a **cocycle**, that is

$$\alpha_{\sigma\tau} = \alpha_\sigma\, \sigma\cdot\alpha_\tau \text{ for all } \sigma, \tau \in \mathrm{Gal}(\Omega/k).$$

This condition is not sufficient in general. However, it happens to be the case if $G(\Omega) = \mathrm{GL}_n(\Omega)$ or $\mathrm{SL}_n(\Omega)$ (this will follow from Hilbert 90). Notice that until now we picked a matrix $Q \in G(\Omega)$ which conjugates M into M_0, but this matrix Q is certainly not unique.We could therefore wonder what happens if we take another matrix $Q' \in G(\Omega)$ which conjugates M into M_0. Computations show that we have $Q'Q^{-1} \in Z_G(M_0)(\Omega)$. Therefore, there exists $C \in Z_G(M_0)(\Omega)$ such that $Q' = CQ$, and we easily get that

$$\alpha^{Q'}_\sigma = C\alpha^Q_\sigma(\sigma\cdot C)^{-1} \text{ for all } \sigma \in \mathrm{Gal}(\Omega/k).$$

Two cocycles $\alpha, \alpha' : \mathrm{Gal}(\Omega/k) \to Z_G(M_0)(\Omega)$ such that

$$\alpha'_\sigma = C\alpha_\sigma(\sigma\cdot C)^{-1} \text{ for all } \sigma \in \mathrm{Gal}(\Omega/k)$$

for some $C \in Z_G(M_0)(\Omega)$ will be called **cohomologous**. Being cohomologous is an equivalence relation on the set of cocycles, and the set of equivalence classes is denoted by $H^1(\mathrm{Gal}(\Omega/k), Z_G(M_0)(\Omega))$. If α is a cocycle, we will denote by $[\alpha]$ the corresponding equivalence class. Therefore, to any matrix $M \in \mathrm{M}_n(k)$ which is conjugate to M_0 by an element of $G(\Omega)$, one may associate a well-defined cohomology class $[\alpha^Q]$, where $Q \in G(\Omega)$ is any matrix satisfying $QMQ^{-1} = M_0$.

It is important to notice that the class $[\alpha^Q]$ does not characterize M completely. Indeed, for every $P \in G(k)$, it is easy to check that $\alpha^{QP^{-1}} = \alpha^Q$. In particular, the cohomology classes associated to the matrices M and PMP^{-1} are equal, for all $P \in G(k)$.

Conversely, if $\alpha = \alpha^Q$ and $\alpha' = \alpha^{Q'}$ are cohomologous, it is not too difficult to see that $P = Q^{-1}C^{-1}Q' \in G(k)$, and that the corresponding matrices M_α and $M_{\alpha'}$ satisfy $PM_{\alpha'}P^{-1} = M_\alpha$.

Thus the previous considerations then show that, in the case where every cocycle $\alpha : \mathrm{Gal}(\Omega/k) \to Z_G(M_0)(\Omega), \sigma \mapsto \alpha_\sigma$ may be written $\alpha = \alpha^Q$ for some $Q \in G(\Omega)$, the set $H^1(\mathrm{Gal}(\Omega/k), Z_G(M_0)(\Omega))$ is in one-to-one correspondence with the set of $G(k)$-conjugacy classes of matrices $M \in \mathrm{M}_n(k)$ which are conjugate to M_0 by an element of $G(\Omega)$.

Many situations can be dealt with in a similar way.For example, reasoning as above and using Hilbert 90, one can show that the set of isomorphism classes of quadratic forms q which are isomorphic to the quadratic form $x_1^2+\cdots+x_n^2$ over $\Omega$is in one-to-one correspondence with $H^1(\mathrm{Gal}(\Omega/k), \mathrm{O}_n(\Omega))$.The case of k-algebras is a little bit more subtle, but one can show that the set of isomorphism classes of k-algebras which are isomorphic to a given k-algebra A over $\Omega$is in one-to-one correspondence with $H^1(\mathrm{Gal}(\Omega/k), \mathrm{Aut}_{\Omega-\mathrm{alg}}(A \otimes_k \Omega))$.

Quite often, algebraic structures can be well understood over a separable closure k_s of k. In the best cases, they even become isomorphic over k_s, and Galois cohomology may be of great interest in this situation. However, to avoid technicalities we will assume that Ω/k is finite, and come back to the infinite case at the very end.

2 Cohomology sets

Definition 2.1. Let G be a finite group. A set A is called a G-**set** if G acts on A on the left. A group A is called a G-**group** if G acts on A by group morphisms, i.e.

$$\sigma\cdot(a_1a_2) = (\sigma\cdot a_1)(\sigma\cdot a_2) \text{ for } \sigma \in G, a_1, a_2 \in A.$$

A G-group which is commutative is called a G-**module**.

A **morphism** of G-sets (resp. G-groups, G-modules) is a map (resp. a group morphism) $f : A \to A'$ satisfying the following property:

$$f(\sigma\cdot a) = \sigma\cdot f(a) \text{ for all } \sigma \in G \text{ and all } a \in A.$$

Examples 2.2.

(1) Let Ω/k be a Galois extension of group $\mathcal{G}_\Omega$. Then the map

$$\mathcal{G}_\Omega \times \Omega \to \Omega, (\sigma, x) \mapsto \sigma\cdot x = \sigma(x)$$

endows $\Omega$with the a structure of a $\mathcal{G}_\Omega$-module. (2) Let Ω/k be a Galois extension of group $\mathcal{G}_\Omega$.Then $\mathcal{G}_\Omega$ acts naturally on $\mathrm{GL}_n(\Omega)$ as follows: for $\sigma \in \mathcal{G}_\Omega$ and $M = (m_{ij}) \in \mathrm{GL}_n(\Omega)$, set

$$\sigma\cdot M = (\sigma(m_{ij})).$$

Clearly, this is an action by group automorphisms. The same is true for other matrix groups such as $\mathrm{SL}_n(\Omega)$ or $\mathrm{O}_n(\Omega)$.

At this point, we may define the 0^{th}-cohomology set $H^0(\mathcal{G}_\Omega, A)$.

Definition 2.3. For any G-set A, we set

$$H^0(G, A) = A^G.$$

If A is a G-group, this is a subgroup of A. The set $H^0(G, A)$ is called the **0^{th} cohomology set of G with coefficients in A.**

We will not really use this notation except once or twice, preferring writing A^G instead of $H^0(G, A)$. We now come to the main object of these lectures:

Definition 2.4. Let A be a G-group. A **1-cocycle** with values in A is a map $\alpha : G \to A, \sigma \mapsto \alpha_\sigma$ such that

$$\alpha_{\sigma\tau} = \alpha_\sigma \, \sigma{\cdot}\alpha_\tau \text{ for } \sigma, \tau \in G.$$

We denote by $Z^1(G, A)$ the set of all 1-cocycles of G with values in A. The constant map $\alpha_\sigma = 1$ is an element of $Z^1(G, A)$, which is called the **trivial** 1-cocycle. Notice also that for any 1-cocycle α, we have $\alpha_1 = 1$.

Remark 2.5. If G acts trivially on A, a 1-cocycle is just a morphism $\alpha : G \to A$. In order to define the cohomology set $H^1(G, A)$, we need now an appropriate notion of cohomologous cocycles, which coincide with the one defined in the introduction in a particular case. This will be provided by the following lemma:

Lemma 2.6. *Let A be a G-group and let $\alpha : G \to A$ be a 1-cocycle. Then for all $a \in A$, the map*

$$\alpha' : G \to A, \sigma \mapsto a\alpha_\sigma \, \sigma{\cdot}a^{-1}$$

is again a 1-cocycle.

This leads to the following definition:

Definition 2.7. Two 1-cocycles α, α' are said to be **cohomologous** if there exists $a \in A$ satisfying

$$\alpha'_\sigma = a\alpha_\sigma \, \sigma{\cdot}a^{-1} \text{ for all } \sigma \in G.$$

It is denoted by $\alpha \sim \alpha'$.

Remark 2.8. The symbol '$\sigma{\cdot}a^{-1}$' may seem ambiguous at first sight, since it could denote $(\sigma{\cdot}a)^{-1}$ as well as $\sigma{\cdot}(a^{-1})$. However, these two elements are equal in our setting, since G acts on A by group automorphisms; we will keep this notation throughout.

Definition 2.9. Let A be a G-group. The relation '$\sim$' is easily checked to be an equivalence relation on $Z^1(G, A)$. We denote by $H^1(G, A)$ the quotient set

$$H^1(G, A) = Z^1(G, A)/\sim .$$

It is called **the first cohomology set of G with coefficients in A.**

The set $H^1(G, A)$ is not a group in general. However, it has a distinguished element, which is the class of the trivial cocycle. Therefore, $H^1(G, A)$ is a pointed set in the following sense:

Definition 2.10. A **pointed set** is a pair (E, x), where E is a nonempty set and $x \in E$. The element x is called the **base point**. A **map of pointed sets** $f : (E, x) \to (F, y)$ is a set-theoretic map such that $f(x) = y$. We will often forget to specify the base point when it is clear from the context. The **kernel** of a map $f : (E, x) \to (F, y)$ of pointed sets is the preimage of y.

Example 2.11. The set $H^1(G, A)$ is a pointed set, and any abstract group G may be considered as a pointed set, whose base point is the neutral element.

Remark 2.12. If A is a G-module, the set $Z^1(G, A)$ is an abelian group for the pointwise multiplication of functions. This operation is compatible with the equivalence relation, hence it induces an abelian group structure on $H^1(G, A)$.

We now look to the behaviour of these sets when G or A vary. **Definition 2.13.** Let G, G' be two finite groups. Let A be a G-group and A' be a G'-group. Moreover, let $\varphi : G' \to G$ and $f : A \to A'$ be two group morphisms.

We say that f and φ are **compatible** if

$$f(\varphi(\sigma') \cdot a) = \sigma' \cdot f(a) \text{ for } \sigma' \in G', a \in A.$$

Notice that it follows from the very definition that if a is fixed by G, then $f(a)$ is fixed by G'.Hence f induces by restriction a map of pointed sets

$$f_* : H^0(G, A) \to H^0(G', A').$$

The following proposition shows that this is also true for H^1.

Proposition 2.14. *Let G, G', A, A' as above, and let $\varphi : G' \to G$ and $f : A \to A'$ be two compatible group morphisms. For any cocycle $\alpha \in Z^1(G, A)$, the map*

$$\beta : G' \to A', \sigma' \mapsto f(\alpha_{\varphi(\sigma')})$$

is a cocycle.

Moreover, the assignment $\alpha \in Z^1(G, A) \mapsto \beta \in Z^1(G', A')$ induces a map of pointed sets (resp. a group morphism if A and A' are abelian)

$$f_* : H^1(G, A) \to H^1(G', A').$$

Proof. By definition, we have $\beta_{\sigma'} = f(\alpha_{\varphi(\sigma')})$. Hence, for all $\sigma', \tau' \in G$, we have $\beta_{\sigma'\tau'} = f(\alpha_{\varphi(\sigma')\varphi(\tau')})$, since φ is a group morphism. Since α is a 1-cocycle, we get

$$\beta_{\sigma'\tau'} = f(\alpha_{\varphi(\sigma')}\, \varphi(\sigma') \cdot \alpha_{\varphi(\tau')}) = f(\alpha_{\varphi(\sigma')}) f(\varphi(\sigma') \cdot \alpha_{\varphi(\tau')}).$$

By compatibility, we get that

$$\beta_{\sigma'\tau'} = f(\alpha_{\varphi(\sigma')})\, \sigma' \cdot f(\alpha_{\varphi(\tau')}) = \beta_{\sigma'} \sigma' \cdot \beta_{\tau'}.$$

Hence β is a 1-cocycle.

Now we have to show that if α and α' are cohomologous, then the corresponding β and β' are also cohomologous, so assume that

$$\alpha'_\sigma = a \alpha_\sigma\, \sigma \cdot a^{-1} \text{ for all } \sigma \in G,$$

for some $a \in A$. Applying this relation to $\sigma = \varphi(\sigma')$ and taking f on both sides gives

$$\beta'_{\sigma'} = f(a \alpha_{\varphi(\sigma')} \varphi(\sigma') \cdot a^{-1}).$$

Since f is a group morphism which is compatible with φ, we get

$$\beta'_{\sigma'} = f(a) f(\alpha_{\varphi(\sigma')})\, \sigma' \cdot f(a)^{-1} = f(a) \beta_{\sigma'}\, \sigma' \cdot f(a)^{-1}.$$

Hence β and β' are cohomologous. Finally, it is clear from the definition that f_* maps the trivial class onto the trivial class. ∎

Example 2.15. Assume that $G = G'$ and $\varphi = \mathrm{Id}_G$. Then a compatible map $f : A \to A'$ is just a morphism of G-groups, and the map f_* just sends the cohomology class of α to the cohomology

class of $f \circ \alpha$. Moreover, if $g : A' \to A''$ is a morphism of G-sets (or G-groups, etc), we have $(g \circ f)_* = g_* \circ f_*$.

In the sequel, f_* will always denote the map induced by Id_G and f. We now provide one example of computation of a Galois cohomology set.

3. Hilbert's 90^{th} theorem

3 Hilbert's 90th theorem

minary results on semi-linear actions.

Definition 3.1. Let Ω/k be a Galois extension of Galois group $\mathcal{G}_\Omega$, and let U be a (right) vector space over $\Omega$with an action $*$ of $\mathcal{G}_\Omega$ on U. We will denote by '$\cdot$' the standard linear action of $\mathcal{G}_\Omega$ on Ω. We say that $\mathcal{G}_\Omega$ acts **by semi-linear automorphisms** on U if we have for all $u, u' \in U, \lambda \in \Omega$

$$\begin{array}{lcl} \sigma * (u + u') & = & \sigma * u + \sigma * u'; \\ \sigma * (u\lambda) & = & (\sigma * u)(\sigma \cdot \lambda). \end{array}$$

Examples 3.2.

(1) Let V be a k-vector space, and let $U = V \otimes_k \Omega$. The action of $\mathcal{G}_\Omega$ on U defined on elementary tensors by

$$\sigma * (v \otimes \lambda) = v \otimes (\sigma \cdot \lambda) \text{ for all } v \in V, \lambda \in \Omega$$

is an action by semi-linear automorphisms. (2) Let $U = \Omega^n$, and let $\mathcal{G}_\Omega$ act in an obvious way on each coordinate. We obtain that way an action by semi-linear automorphisms. Morever, $U^{\mathcal{G}_\Omega} = k^n$, and we have a canonical isomorphism of Ω-vector spaces

$$U^{\mathcal{G}_\Omega} \otimes_k \Omega \to U, u \otimes \lambda \mapsto u\lambda.$$

Notice that this isomorphism is also an isomorphism of $\mathcal{G}_\Omega$modules.

The following lemma generalizes the previous example.

Lemma 3.3. *[Galois descent of vector spaces] Let U be a vector space over Ω. If $\mathcal{G}_\Omega$ acts on U by semi-linear automorphisms, then $U^{\mathcal{G}_\Omega} = \{u \in U \mid \sigma * u = u \text{ for all } \sigma \in \mathcal{G}_\Omega\}$ is a k-vector space and the map*

$$f : U^{\mathcal{G}_\Omega} \otimes_k \Omega \to U, u \otimes \lambda \mapsto u\lambda$$

is an isomorphism of Ω-vector spaces. Proof. It is clear that $U^{\mathcal{G}_\Omega}$ is a k-vector space, and that f is Ω-linear. We first prove the surjectivity of f. Let $u \in U$, let $\lambda_1, \ldots, \lambda_n$ be a k-basis of $\Omega$and let $\sigma_1 = \mathrm{Id}_\Omega, \sigma_2, \ldots, \sigma_n$ be the elements of $\mathcal{G}_\Omega$. Let

$$u_i = \sum_j \sigma_j * (u\lambda_i).$$

For all $k = 1, \ldots, n$, we have

$$\sigma_k * u_i = \sum_j (\sigma_k \sigma_j)(u\lambda_i).$$

The action of σ_k on $\sum_j \sigma_j * (u\lambda_i)$ just permutes the terms of the sum, so $u_i \in U^{G_\Omega}$.

Since $\sigma_1, \ldots, \sigma_n$ are precisely the n k-automorphisms of Ω, they are linearly independent over Ωin $\mathrm{End}_k(\Omega)$ (this is Dedekind's Lemma). Hence the matrix $M = (\sigma_j \cdot \lambda_i)_{i,j}$ lies in $\mathrm{GL}_n(\Omega)$. By definition of u_j, we have $u_j = \sum (\sigma_k * u)(\sigma_k \cdot \lambda_j)$. Now if $M^{-1} = (m'_{ij})$, from the equation

$M^{-1}M = I_n$, we get

$$(\sum_j m'_{1j}(\sigma_k \cdot \lambda_j) = \delta_{1k} \text{ for all } k = 1, \dots n,$$

by comparing first rows. Hence we have

$$\sum_j u_j m'_{1j} = \sum_j \sum_k (\sigma_k * u)(\sigma_k \cdot \lambda_j) m'_{1j} = \sum_k (\sigma_k * u)\delta_{1k} = \sigma_1 * u = u,$$

the last equality coming from the fact that $\sigma_1 = \mathrm{Id}_\Omega$. Therefore, we have

$$u = \sum_j u_j m'_{1j} = f(\sum_j u_j \otimes m'_{1j}),$$

which proves the surjectivity of f. To prove its injectivity, it is enough to prove the following: **Claim:** Any vectors $u_1, \dots, u_r \in U^{\mathcal{G}_\Omega}$ which k-linearly independent remain Ω-linearly independent in U.

Indeed, assume that the claim is proved, and let $x \in \ker(f)$. One may write

$$x = u_1 \otimes \mu_1 + \ldots + u_r \otimes \mu_r,$$

for some $\mu_1, \dots, \mu_r \in \Omega$and some $u_1, \dots, u_r \in U^{\mathcal{G}_\Omega}$ which are linearly independent. By assumption, $f(x) = 0 = u_1\mu_1 + \ldots + u_r\mu_r$. Now the claim implies that $\mu_1 = \ldots = \mu_r = 0$, and thus $x = 0$, proving the injectivity of f.

It remains to prove the claim.We are going to do it by a way of contradiction.Assume that we have k-linearly independent vectors $u_1, \dots, u_r \in U^{\mathcal{G}_\Omega}$ for which there exists $\mu_1, \dots, \mu_r \in \Omega$, not all them being zero, such that

$$u_1\mu_1 + \ldots + u_r\mu_r = 0.$$

We may assume that r is minimal, $r > 1$ and $\mu_1 = 1$. By assumption, the μ_i's are not all in k, so we may also assume that $\mu_2 \notin k$. Choose $\sigma \in \mathcal{G}_\Omega$ such that $\sigma \cdot \mu_2 = \mu_2$. We have

$$\sigma * (\sum_i u_i\mu_i) = \sum_i (\sigma * u_i)(\sigma \cdot \mu_i) = \sum_i u_i(\sigma \cdot \mu_i) = 0$$

Subtracting the original relation gives $\sum_{i \geq 2} u_i(\sigma \cdot \mu_i - \mu_i) = 0$, a nontrivial relation with fewer terms. This contradiction concludes the proof. ∎

Remark 3.4. If we endow $U^{\mathcal{G}_\Omega} \otimes_k \Omega$with the natural semi-linear action as in Example 3.2 (1), we claim that the isomorphism f above is an isomorphism of $\mathcal{G}_\Omega$-modules, that is f is equivariant with respect to the two semi-linear actions.

To check this, it is enough to do it on elementary tensors. Now for all $u \in U^{\mathcal{G}_\Omega}$, $\lambda \in \Omega$and $\sigma \in \mathcal{G}_\Omega$, we have

$$f(\sigma * (u \otimes \lambda)) = u(\sigma \cdot \lambda) = (\sigma * u)(\sigma \cdot \lambda) = \sigma * (u\lambda) = \sigma * f(u \otimes \lambda),$$

hence the claim.

We are now ready for our first example.

Proposition 3.5 (Hilbert 90)**.** *For every Galois extension Ω/k, we have $H^1(\mathcal{G}_\Omega, \mathrm{GL}_n(\Omega)) = 1$.*

Proof. Let $\alpha \in Z^1(\mathcal{G}_\Omega, \mathrm{GL}_n(\Omega))$. We twist the natural action of $\mathcal{G}_\Omega$ on $U = \Omega^n$ in an action by semi-linear automorphisms:

$$\sigma * u = \alpha_\sigma(\sigma \cdot u) \text{ for all } u \in U, \sigma \in \mathcal{G}_\Omega.$$

We then get an isomorphism $f : U^{\mathcal{G}_\Omega} \otimes_k \Omega \xrightarrow{\sim} U$ from the previous lemma. In particular, we have

$\dim_k(U^{\mathcal{G}_\Omega}) = \dim_\Omega(U^{\mathcal{G}_\Omega} \otimes_k \Omega) = \dim_\Omega(U) = n$.

Let $v_1, \dots, v_n$ be a k-basis of $U^{\mathcal{G}_\Omega}$ (which is also an Ω-basis of U), and let $P \in \mathrm{GL}_n(\Omega)$ be the matrix whose columns are $v_1, \dots, v_n$. Then for all $\sigma \in \mathcal{G}_\Omega$, the matrix $\sigma{\cdot}P$ is the matrix whose columns are $\sigma{\cdot}v_1, \dots, \sigma{\cdot}v_n$. Now $v_1, \dots, v_n \in U^{\mathcal{G}_\Omega}$, and therefore we have

$$v_i = \sigma * v_i = \alpha_\sigma(\sigma{\cdot}v_i) \text{ for all } i = 1, \dots, n.$$

Written in terms of matrices, this reads

$$P = \alpha_\sigma(\sigma{\cdot}P) \text{ for all } \sigma \in \mathcal{G}_\Omega.$$

It readily follows that α is cohomologous to the trivial cocycle, and this concludes the proof. ∎

Remark 3.6. Assume that Ω/k is a finite cyclic extension of degree n, and let γ be a generator of $\mathcal{G}_\Omega$. If $\alpha \in Z^1(\mathcal{G}_\Omega, \Omega^\times)$ is a 1-cocycle, we have

$$\alpha_{\gamma^n} = \alpha_{\gamma^{n-1}}\gamma^{n-1}{\cdot}\alpha_\gamma = \dots = N_{\Omega/k}(\alpha_\gamma).$$

Since $\gamma^n = 1$, we get $N_{\Omega/k}(\alpha_\gamma) = 1$. Conversely, any element $x \in \Omega^\times$ of norm 1 determines completely a cocycle with values in $\Omega^\times$ by the formula

$$\alpha_{\gamma^m} = \prod_{0 \le i \le m-1} \gamma^i{\cdot}x \text{ for all } 0 \le m \le n-1.$$

Now let $x \in \Omega^\times$ satisfy $N_{\Omega/k}(x) = 1$, and let α be the corresponding cocycle. By Hilbert 90, it is cohomologous to the trivial cocycle, so there exists $z \in \Omega^\times$ such that $\alpha_\sigma = \sigma(z)/z$ for every $\sigma \in G_\Omega$. Taking $\sigma = \gamma$ gives $x = \gamma(z)/z$, the classical form of Hilbert 90.

4 Exact sequences in cohomology

Definition 4.1. Let $f : A \to B$ be a map of pointed sets. Recall that the kernel of f is the preimage of the base point of B. A sequence of pointed sets

$$A \xrightarrow{f} B \xrightarrow{g} C$$

is called **exact** at B if $\mathrm{im} f = \ker g$.

A sequence of pointed sets

$$A_0 \to A_1 \to \cdots \to A_{i-1} \to A_i \to A_{i+1} \to \cdots$$

is called **exact** if it is exact at A_i for all $i \ge 1$.

An exact sequence of groups (resp. of G-groups, resp. of G-modules) is an exact sequence of pointed sets such that all the maps involved are group morphisms (resp. morphisms of G-groups, resp. of G-modules).

For example, the sequence

$$B \xrightarrow{g} C \longrightarrow 1$$

is exact if and only if g is surjective, and the sequence

$$1 \longrightarrow A \xrightarrow{f} B$$

is exact if and only if f has trivial kernel. This does **not** imply that f is injective, unless A and B are groups and f is a group morphism.

Assume that we have an exact sequence

$$1 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 1$$

of pointed G-sets. The goal of the next paragraphs is to derive some exact sequences in cohomology, under some reasonable conditions on A, B and C. We will keep this notation throughout.

Assume that A and B are G-groups, that f is a group morphism (hence f is injective), and that g induces a bijection of G-sets $B/f(A) \simeq C$, where $B/f(A)$ is the set of right cosets modulo $f(A)$. In other words, g is surjective and for all $b, b' \in B$ we have

$$g(b) = g(b') \iff b' = bf(a) \text{ for some } a \in A.$$

For instance, these conditions are satisfied in the following cases:

(1) A is a G-subgroup of B, $C = B/A$, f is the inclusion and g is the natural projection. (2) C is a G-group and g is a group morphism (this will be the case in the next subsection). As pointed out previously in Example 2.15, f and g induce maps on fixed points by restriction, namely $f_* : A^G \to B^G$ and $g_* : B^G \to C^G$. Our next goal is to define a map of pointed sets

$$\delta^0 : C^G \to H^1(G, A).$$

Let $c \in C^G$, and let $b \in B$ any preimage of c under g, i.e. $g(b) = c$. By assumption, we have $c = \sigma \cdot c$ for all $\sigma \in G$. Therefore, we have

$$g(\sigma \cdot b) = \sigma \cdot g(b) = \sigma \cdot c = c = g(b).$$

By assumption on g, there exists a unique element $\alpha_\sigma \in A$ such that $f(\alpha_\sigma) = b^{-1}\, \sigma \cdot b$.

Lemma 4.2. *The map $\alpha : G \to A, \sigma \mapsto \alpha_\sigma$ is a 1-cocycle, and its class in $H^1(G, A)$ does not depend on the choice of $b \in B$.*

Proof. Let us prove that α is a cocycle.By definition of α, for all $\sigma, \tau \in G$, we have

$$f(\alpha_{\sigma\tau}) = b^{-1}\sigma\tau \cdot b = b^{-1}\, \sigma \cdot (bb^{-1}\tau \cdot b) = (b^{-1}\sigma \cdot b)\, \sigma \cdot (b^{-1}\tau \cdot b).$$

Hence we have

$$f(\alpha_{\sigma\tau}) = f(\alpha_\sigma)\, \sigma \cdot f(\alpha_\tau) = f(\alpha_\sigma) f(\, \sigma \cdot \alpha_\tau) = f(\alpha_\sigma\, \sigma \cdot \alpha_\tau).$$

By injectivity of f, we get $\alpha_{\sigma\tau} = \alpha\, \sigma \cdot \alpha_\tau$.

Let us prove now that the cohomology class of α does not depends on the choice of b. Let $b' \in B$ be another preimage of c under g. We then have $g(b') = c = g(b)$, so $b' = bf(a^{-1}) = bf(a)^{-1}$ for some $a \in A$ by assumption on g, and let α' be the corresponding 1-cocycle. We then have

$$f(\alpha'_\sigma) = f(a)b^{-1}\, \sigma \cdot (bf(a^{-1})) = f(a) f(\alpha_\sigma)\, \sigma \cdot f(a)^{-1} = f(a\alpha_\sigma\, \sigma \cdot a^{-1}),$$

so by injectivity of f, this implies that α and α' are cohomologous. This concludes the proof. ∎

We then have constructed a map of pointed sets

$$\delta^0 : C^G \to H^1(G, A), c \mapsto [\alpha],$$

where the cocycle α is defined by the relations

$$f(\alpha_\sigma) = b^{-1}\, \sigma \cdot b \text{ for all } \sigma \in G,$$

for an arbitrary preimage $b \in B$ of c.

Definition 4.3. The map $\delta^0 : C^G \to H^1(G, A)$ is called the 0^{th} **con- necting map**.

Proposition 4.4. *The sequence of G-sets*

$$1 \longrightarrow A^G \xrightarrow{f_*} B^G \xrightarrow{g_*} C^G \xrightarrow{\delta^0} H^1(G, A) \xrightarrow{f_*} H^1(G, B)$$

is exact.

Proof. The fact that the sequence

$$1 \to A^G \to B^G \to C^G$$

is exact is left to the reader.

Exactness at C^G: clearly if $c = g(b)$ for some $b \in B^G$, then its image under δ^0 is the trivial class. Conversely, assume that $\delta^0(c)$ is trivial, i.e. $\alpha_\sigma = a\,\sigma{\cdot}a^{-1}$ for some $a \in A$. Let $b \in B$ be a preimage of c under g. We then have

$$f(a\,\sigma{\cdot}a^{-1}) = b^{-1}\,\sigma{\cdot}b,$$

so $f(a)\sigma{\cdot}f(a)^{-1} = b^{-1}\sigma{\cdot}b$. Hence $bf(a) \in B^G$, and we have $g(bf(a)) = g(b) = c$ by assumption on g. Hence $\ker(\delta^0) = \mathrm{im}(g_*)$, which is what we wanted to prove.

Exactness at $H^1(G, A)$: Let $c \in C^G$ and let $b \in B$ satisfying $c = g(b)$. Then by definition of f_* and $\delta^0(c)$, $f_*(\delta^0(c))$ is the class of the 1-cocycle $G \to B, \sigma \mapsto b^{-1}\,\sigma{\cdot}b$, which is cohomologous to the trivial cocycle. Now if $[\alpha] \in H^1(G, A)$ satisfies $f_*([\alpha]) = 1$, then $f(\alpha_\sigma) = b^{-1}\,\sigma{\cdot}b$ for some b in B. Therefore, we have

$$\sigma{\cdot}g(b) = g(\,\sigma{\cdot}b) = g(bf(\alpha_\sigma)) = g(b) \text{ for all } \sigma \in G.$$

Hence $c = g(b)$ lies in C^G. Thus $b \in B$ is a preimage of $c \in C^G$ under g and $[\alpha] = \delta^0(c)$ by definition of δ^0. This concludes the proof. ∎

Example 4.5. We have an exact sequence of $\mathcal{G}_\Omega$-groups

$1\ \mathrm{SL}_n(\Omega)\ \mathrm{GL}_n(\Omega)\ \Omega^\times\ 1$,

where the last map is the determinant. Hence we have an exact sequence in cohomology

$\mathrm{GL}_n(k)\cdot k^\times \xrightarrow{\delta^0} H^1(\mathcal{G}_\Omega, \mathrm{SL}_n(\Omega))\cdot H^1(\mathcal{G}_\Omega, \mathrm{GL}_n(\Omega))$ where the first map is the determinant. By Hilbert 90, we get an exact sequence

$\mathrm{GL}_n(k)\cdot k^\times \xrightarrow{\delta^0} H^1(\mathcal{G}_\Omega, \mathrm{SL}_n(\Omega))\ 1$.

Since the determinant map is surjective, and since the sequence above is exact at $k^\times$, it follows that the 0^{th} connecting map is trivial, hence we get $H^1(\mathcal{G}_\Omega, \mathrm{SL}_n(\Omega)) = 1$.

Before continuing, we need to define an action of B^G in C^G. Let $\beta \in B^G$ and $c \in C^G$. Let $b \in B$ be a preimage of c under g, and set

$$\beta \cdot c = g(\beta b) \in C.$$

Let us check that it does not depends on the choice of b. If $b' \in B$ is another preimage of c under g, then $b' = bf(a)$ for some $a \in A$, hence $g(\beta b') = g(\beta b f(a)) = g(\beta b)$ by assumption on g. Hence $\beta \cdot c$ does not depend the choice of b.

We now show that $\beta \cdot c \in C^G$. For $\sigma \in G$, we have

$$\sigma{\cdot}(\beta{\cdot}c) = \sigma{\cdot}g(\beta b) = g(\,\sigma{\cdot}(\beta b)) = g((\,\sigma{\cdot}\beta)(\,\sigma{\cdot}b)).$$

Since $\beta \in B^G$, we get $\sigma{\cdot}(\beta \cdot c) = g(\beta(\,\sigma{\cdot}b))$ for all $\sigma \in G$.Now $g(\,\sigma{\cdot}b) = \sigma{\cdot}g(b) = \sigma{\cdot}c = c$ since $c \in C^G$, so $\sigma{\cdot}b$ is also a preimage of c. Since $\beta \cdot c$ does not depend on the choice of a preimage of c, we conclude that $\sigma{\cdot}(\beta{\cdot}c) = \beta{\cdot}c$ for all $\sigma \in G$, so $\beta{\cdot}c \in C^G$.

It is then clear that the map

$$B^G \times C^G \to C^G, (\beta, c) \mapsto \beta \cdot c$$

gives rise to an action of B^G on C^G. The next result identifies the corresponding orbit set.

Corollary 4.6. *There is a natural bijection between the orbit set of the group B^G in C^G and* $\ker(H^1(G, A) \to H^1(G, B))$.

More precisely, the bijection sends the orbit of $c \in C^G$ onto $\delta^0(c)$.

Proof. Let us denote by C^G/B^G the orbit set of B^G in C^G. By the previous proposition, we have $\ker(H^1(G, A) \to H^1(G, B)) = \mathrm{im}(\delta^0)$. Hence we have to construct a bijection between C^G/B^G and $\mathrm{im}(\delta^0)$.

Let $c, c' \in C^G$ lying in the same orbit, that is $c' = \beta \cdot c$ for some $\beta \in B^G$. Then $c' = g(\beta b)$, for some preimage $b \in B$ of c, and βb is a preimage of c'. Since we have $(\beta b)^{-1}\, \sigma \cdot (\beta b) = b^{-1}\beta^{-1}(\sigma \cdot \beta)(\sigma \cdot b) = b^{-1}\, \sigma \cdot b$, it turns out that $\delta^0(c') = \delta^0(c)$. Therefore, the map

$$\varphi : C^G/B^G \to \mathrm{im}(\delta^0), B^G \cdot c \mapsto \delta^0(c)$$

is a well-defined surjective map. It remains to prove its injectivity. Let $c, c' \in C^G$ such that $\delta^0(c') = \delta^0(c)$, and let α and α' be the cocycles representing $\delta^0(c)$ and $\delta^0(c')$ respectively. By assumption, there exists $a \in A$ such that $\alpha'_\sigma = a\alpha_\sigma\, \sigma \cdot a^{-1}$ for all $\sigma \in G$. If b (resp. b') is a preimage of c (resp. c') in B, applying f to this last equality implies that

$$b'^{-1}\, \sigma \cdot b' = f(a)b^{-1}(\sigma \cdot b)(\sigma \cdot f(a))^{-1}.$$

It easily turns out that $b' f(a) b^{-1} \in B^G$, so $b' f(a) = \beta b$, for some $\beta \in B^G$. Hence $c' = g(b') = g(b' f(a)) = g(\beta b) = \beta \cdot c$. Therefore, c and c' lie in the same orbit, showing that φ is injective. This concludes the proof. ∎

We now assume that we have an exact sequence of G-groups

$$1 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 1$$

so A can be identified with a normal subgroup of B.

Proposition 4.7. *The sequence*

$$1 \to A^G \to B^G \to C^G \to H^1(G, A) \to H^1(G, B) \to H^1(G, C)$$

is exact.

Proof. By Proposition 4.4, only the exactness at $H^1(G, B)$ needs a proof. If $[\beta] = f_*([\alpha])$ for some $[\alpha] \in H^1(G, A)$, the we have

$$g_*([\beta]) = g_*(f_*([\alpha])) = (g \circ f)_*([\alpha]) = 1,$$

since $g \circ f$ is trivial by assumption. Hence $\mathrm{im}(f_*) \subset \ker(g_*)$. Conversely, let $[\beta] \in H^1(G, B)$ such that $g_*([\beta]) = 1$. Then there exists $c \in C$ such that $g(\beta_\sigma) = c^{-1}\, \sigma \cdot c$ for all $\sigma \in G$. Write $c = g(b)$. We then have $g(\beta_\sigma) = g(b^{-1}\, \sigma b)$, so $\beta_\sigma = b^{-1}(\sigma b) f(a_\sigma)$, for some $a_\sigma \in A$. Since $f(A)$ is normal in B, $(\sigma \cdot b) f(a_\sigma)(\sigma \cdot b)^{-1} \in f(A)$, so $\beta_\sigma = b^{-1} f(\alpha_\sigma)\, \sigma \cdot b$ for some $\alpha_\sigma \in A$, and thus

$$b\beta_\sigma\, \sigma \cdot b^{-1} = f(\alpha_\sigma) \text{ for all } \sigma \in G.$$

The fact that the map $G \to B, \sigma \to b\beta_\sigma\, \sigma \cdot b^{-1}$ is a 1-cocycle and the injectivity of f imply easily that α is a cocycle.Moreover, by construction of α, we have $[\beta] = f_*([\alpha]) \in \mathrm{im}(g_*)$. This concludes the proof. ∎

We would like now to go back to the general Galois descent problem: if two k-structures are isomorphic over Ω, are they isomorphic over k? First we need an appropriate setting in order for

all these words to make sense. We therefore starting by examining carefully our solution to the conjugacy problem for matrices.

5 (The) matrix (case) reloaded

In this paragraph, we would like to extract the essential arguments of our solution to the conjugacy problem, and rewrite them in a more concise and formal way, in order to find a general way to attack the general Galois descent problem. Let us first reformulate the result we obtained. In fact, we have proved in the introduction that the set of $G(k)$conjugacy classes of matrices $M \in \mathrm{M}_n(\Omega)$ which are $G(\Omega)$-conjugate to a given matrix $M_0 \in \mathrm{M}_n(k)$ is in one-to-one correspondence with the set of cohomology classes $[\alpha] \in H^1(\mathcal{G}_\Omega, Z_G(M_0)(\Omega))$, which may be written $[\alpha] = [\alpha^C]$ for some $C \in G(\Omega)$, where α^C is the cocycle

$$\alpha^C : \mathcal{G}_\Omega \to Z_G(M_0)(\Omega), \sigma \mapsto C(\sigma \cdot C)^{-1}.$$

This set of cohomology classes is nothing but the kernel of the map

$$H^1(\mathcal{G}_\Omega, Z_G(M_0)(\Omega)) \to H^1(\mathcal{G}_\Omega, G(\Omega))$$

induced by the inclusion $Z_G(M_0)(\Omega) \subset G(\Omega)$.

This observation will allow us to give a more conceptual (and less miraculous) explanation of our result. Notice first that the congugacy class of a matrix may be reinterpreted as an orbit under the action of $G = \mathbf{GL}_n$ of $\mathbf{SL}_n$ by conjugation. This action will be denoted by $*$ in the sequel. The next crucial observation is then the following one: if $M_0 \in \mathrm{M}_n(k)$, we may rewrite $Z_G(M_0)(\Omega)$ as

$$Z_G(M_0)(\Omega) = \{C \in G(\Omega) \mid C * M_0 = M_0\}.$$

In other words, $Z_G(M_0)(\Omega)$ is nothing but the stabilizer of M_0 (viewed as an element of $\mathrm{M}_n(\Omega)$) with respect to the action of $G(\Omega)$ on $\mathrm{M}_n(\Omega)$.

The second important point is that the action of G_Ω on $G(\Omega)$ restricts to an action on $Z_G(M_0)(\Omega)$. To see this, recall that the action of $\mathcal{G}_\Omega$ on a matrix $S = (s_{ij}) \in \mathrm{M}_n(\Omega)$ is given by

$$\sigma \cdot S = (\sigma(s_{ij})).$$

In particular, the following properties hold:

(*i*) $\mathrm{M}_n(\Omega)^{\mathcal{G}_\Omega} = \mathrm{M}_n(k)$ (*ii*) For all $S \in \mathrm{M}_n(\Omega), C \in G(\Omega)$ and $\sigma \in \mathcal{G}_\Omega$, we have

$$\sigma \cdot (C * S) = (\sigma \cdot C) * (\sigma \cdot S).$$

We have in fact an even more general property. If $\iota : K \to L$ is a morphism of field extensions of k and $S \in \mathrm{M}_n(K)$, set

$$\iota \cdot S = (\iota(s_{ij})).$$

We then have

(*ii'*) For all morphism of extensions $\iota : K \to L, S \in \mathrm{M}_n(K)$ and $C \in G(K)$, we have

$$\iota \cdot (C * S) = (\iota \cdot C) * (\iota \cdot S).$$

If now $C \in Z_G(M_0)(\Omega)$ and $\sigma \in G(\Omega)$, we have

$$(\sigma \cdot C) * M_0 = (\sigma \cdot C) * (\sigma \cdot M_0)$$

by (*i*), since $M_0 \in \mathrm{M}_n(k)$. Using (*ii*), we then get

$$(\sigma \cdot C) * M_0 = \sigma \cdot (C * M_0) = \sigma \cdot M_0 = M_0,$$

the second equality coming from the fact that $C \in Z_G(M_0)(\Omega)$. Hence the action of $\mathcal{G}_\Omega$ on $G(\Omega)$ restricts to an action on $Z_G(M_0)(\Omega)$ as claimed.Now it follows from elementary group theory that we have a bijection

$$G(\Omega)/Z_G(M_0)(\Omega) \simeq G(\Omega) * M_0.$$

Equivalently, we have an exact sequence

$1 \to Z_G(M_0)(\Omega) \to G(\Omega) \to G(\Omega) * M_0 \to 1,$

which may be easily seen to be an exact sequence of pointed G_Ω-sets satisfying the conditions explained in § 4, the base point of $G(\Omega) * M_0$ being M_0.

The apparition of $\ker[H^1(\mathcal{G}_\Omega, Z_G(M_0)(\Omega)) \to H^1(\mathcal{G}_\Omega, G(\Omega))]$ is not a real surprise then, in view of Corollary 4.6. The same corollary says that this kernel is in one-to-one correspondence with the orbit set of $G(\Omega)^{\mathcal{G}_\Omega}$ in $(G(\Omega) * M_0)^{\mathcal{G}_\Omega}$.

Let us now check that this orbit set is precisely the set of $G(k)$conjugacy classes of matrices which become $G(\Omega)$-conjugate to M_0. Notice that since G = **GL**$_n$ or **SL**$_n$, we have

(iii) $G(\Omega)^{\mathcal{G}_\Omega} = G(k)$.

Moreover, by definition of the action of $G(\Omega)$ on $\mathrm{M}_n(\Omega)$, $G(\Omega)*M_0$ is the set of matrices of $\mathrm{M}_n(\Omega)$ which are $G(\Omega)$-conjugate to M_0. Therefore by (i), $(G(\Omega) * M_0)^{\mathcal{G}_\Omega}$ is the set of matrices of $\mathrm{M}_n(k)$ which are $G(\Omega)$conjugate to M_0. Notice now that the action $G(\Omega)^{\mathcal{G}_\Omega} = G(k)$ on $(G(\Omega) * M_0)^{\mathcal{G}_\Omega}$ defined before Corollary 4.6 is simply the restriction of the action of $G(k)$ on $\mathrm{M}_n(k)$ by conjugation. Indeed, if $M \in \mathrm{M}_n(k)$ has the form $M = Q*M_0$ for some $Q \in G(\Omega)$, and if $P \in G(k)$, Q is a preimage of M under the map $G(\Omega) \to G(\Omega) * M_0$, and therefore we have

$$P \cdot M = (PQ) * M_0 = P * (Q * M_0) = P * M.$$

Thus the orbit set of $G(\Omega)^{\mathcal{G}_\Omega}$ in $(G(\Omega) * M_0)^{\mathcal{G}_\Omega}$ is nothing but the set of $G(k)$-conjugacy classes of matrices $M \in \mathrm{M}_n(k)$ which become $G(\Omega)$conjugate to M_0.

Therefore, we have proved that our solution the conjugacy problem for matrices was nothing but an application of Corollary 4.6, and we have identified three important properties which make this actually work. Notice that (i) and (iii) may seem redundant a priori, but this is only due to our specific example. In more abstract situations, both conditions may be of different nature. For example, one may replace matrices by quadratic forms of dimension n and study the Galois descent problem for isomorphism classes of quadratic forms. In this case, we see that properties (i) and (iii) do not concern the same objects. Our next goal is now to reformulate this new approach in a more abstract context, and derive a solution for general Galois descent problems. In particular, we will need to find appropriate substitutes for $Z_G(M_0)(\Omega)$ and properties $(i) - (iii)$. Of course, Galois descent problems only makes sense if the algebraic objects may be 'defined over an arbitrary field', and if we have a notion of 'scalar extension' of our objects.For example, to each field extension K/k of a field k, we can consider the set $\mathrm{M}_n(K)$ of matrices with coefficients in K, and if $K \to L$ is a morphism of extensions of k, one can associate a map $\mathrm{M}_n(K) \to \mathrm{M}_n(L)$, $M = (m_{ij}) \mapsto (\iota(m_{ij}))$. which is in fact the canonical inclusion. Another example may be obtained by considering the set **Alg**$_n(K)$ of K-algebras of dimension n over K. In this case, the map **Alg**$_n(K) \to$ **Alg**$_n(L)$ associated to a morphism $K \to L$ is given by the tensor product $\otimes_K L$. In both cases, scalar extension maps satisfy some natural properties: the scalar extension map from K to itself is the identity map, and extending scalars from K to L, then from L to M is the same as extending scalars from K to M.

We now formalize this situation by introducing the concept of a functor.

6 Functors

Definition 6.1. Let k be a field. A **functor** defined over k is a rule $\mathbf{F}$ which associates to every field extension K/k a set (a group, a ring...) $\mathbf{F}(K)$, and to any morphism of field extensions $\varphi : K \to K'$ a map (group morphism, ring morphism) $\mathbf{F}(\varphi) : \mathbf{F}(K) \to \mathbf{F}(K')$ such that the following properties hold: (1) For all K/k, $\mathbf{F}(\mathrm{Id}_K) = \mathrm{Id}_{\mathbf{F}(K)}$ (2) For all $\varphi_1 : K_1 \to K_2$, $\varphi_2 : K_2 \to K_3$, we have

$$\mathbf{F}(\varphi_2 \circ \varphi_1) = \mathbf{F}(\varphi_2) \circ \mathbf{F}(\varphi_1).$$

The maps $\mathbf{F}(\varphi)$ has to be understood as 'scalar extension maps'. If $\varphi : K \to L$ is a morphism of extensions, for all $x \in \mathbf{F}(K)$ we will denote by x_L the element $\mathbf{F}(\varphi)(x)$ if there is no ambiguity in the choice of the map φ.

Examples 6.2. (1) The rules

$$K \to \mathrm{M}_n(K), K \to \mathrm{GL}_n(K), K \to \mathrm{SL}_n(K)$$

are functors. If $\iota : K \to L$ is a morphism of extensions, the induced map is just

$$(m_{ij}) \mapsto (\iota(m_{ij})).$$

(2) If A is a k-algebra, the rule

$$h_A : K \mapsto \mathrm{Hom}_{k-alg}(A, K)$$

is a functor. Therefore, the algebraic objects we are going to work with are points of a functor $\mathbf{F}$. What we need now is an action of $\mathcal{G}_\Omega$ on $\mathbf{F}(\Omega)$ for every Galois extension Ω/k, playing the role of the action of $\mathcal{G}_\Omega$ on matrices.

Notice that if $\mathbf{F}$ is a functor, then for any Galois extension Ω/k and every $\sigma \in \mathcal{G}_\Omega$, we have an induced bijection

$$\mathbf{F}(\sigma) : \mathbf{F}(\Omega) \to \mathbf{F}(\Omega).$$

For $x \in \mathbf{F}(\Omega)$ and $\sigma \in \mathcal{G}_\Omega$, we set

$$\sigma \cdot x = \mathbf{F}(\sigma)(x).$$

Lemma 6.3. *The map*

$$\mathcal{G}_\Omega \times \mathbf{F}(\Omega) \to \mathbf{F}(\Omega), (\sigma, x) \mapsto \sigma \cdot x = \mathbf{F}(\sigma)(x)$$

gives rise to an action of $\mathcal{G}_\Omega$ on $\mathbf{F}(\Omega)$.

If Ω/k and Ω'/k are two Galois extensions such that $\Omega \subset \Omega'$, we have

$$\sigma' \cdot x_{\Omega'} = (\sigma'_{|_\Omega} \cdot x)_{\Omega'} \text{ for all } x \in \mathbf{F}(\Omega), \sigma' \in \mathcal{G}_{\Omega'}.$$

Moreover, if $\mathbf{F}$ is a group-valued functor, the action above is an action by group automorphisms, that is

$$\sigma \cdot (xy) = (\sigma \cdot x)(\sigma \cdot y) \text{ for all } \sigma \in \mathcal{G}_\Omega, x, y \in \mathbf{F}(\Omega).$$

Proof. Since $\mathbf{F}$ is a functor, we have $\mathbf{F}(\mathrm{Id}_\Omega) = \mathrm{Id}_{\mathbf{F}(\Omega)}$. Therefore,

$$\mathrm{Id}_\Omega \cdot x = x \text{ for all } x \in \mathbf{F}(\Omega).$$

Now let $\sigma, \tau \in \mathcal{G}_\Omega$. Since $\mathbf{F}$ is a functor, we have

$$\mathbf{F}(\sigma \circ \tau) = \mathbf{F}(\sigma) \circ \mathbf{F}(\tau),$$

and thus $(\sigma \circ \tau) \cdot x = \sigma \cdot (\tau \cdot x)$ for all $x \in \mathbf{F}(\Omega)$. This proves the first part of the lemma.

Let Ω/k and Ω'/k be two Galois extensions such that $\Omega \subset \Omega'$, and let $\mathbf{F}(\iota) : \mathbf{F}(\Omega) \to \mathbf{F}(\Omega')$ be the map induced by the inclusion $\iota : \Omega \subset \Omega'$. For all $\sigma' \in \mathcal{G}_{\Omega'}$, the diagram

$$\begin{array}{ccc} \Omega & \xrightarrow{\sigma'_{|\Omega}} & \Omega \\ \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle \iota} \\ \Omega' & \xrightarrow{\sigma'} & \Omega' \end{array}$$

is commutative. Therefore, it induces a commutative diagram

$$\begin{array}{ccc} \mathbf{F}(\Omega) & \xrightarrow{\mathbf{F}(\sigma'_{|\Omega})} & \mathbf{F}(\Omega') \\ \downarrow{\scriptstyle \mathbf{F}(\iota)} & & \downarrow{\scriptstyle \mathbf{F}(\iota)} \\ \mathbf{F}(\Omega') & \xrightarrow{\mathbf{F}(\sigma')} & \mathbf{F}(\Omega) \end{array}$$

In other words, for all $x \in \mathbf{F}(\Omega)$, we have

$$\mathbf{F}(\iota) \circ \mathbf{F}(\sigma'_{|\Omega})(x) = \mathbf{F}(\sigma') \circ \mathbf{F}(\iota)(x),$$

that is

$$(\sigma'_{|\Omega} \cdot x)_{\Omega'} = \sigma' \cdot x_{\Omega'}.$$

Finally, if $\mathbf{F}$ is a group-valued functor, $\mathbf{F}(\sigma)$ is a group morphism and the last part follows. This concludes the proof. ∎

Example 6.4. If $\mathbf{F} = \mathbf{M}_n$, $\mathbf{GL}_n$ or $\mathbf{SL}_n$, this action of σ is nothing but

$$\sigma \cdot (m_{ij}) = (\sigma(m_{ij})).$$

In particular, functors give a cheap way to produce $\mathcal{G}_\Omega$-sets and $\mathcal{G}_\Omega$groups. Now that the decor is set and the actors are in place, we are ready look at general Galois descent problems.

7 Functorial group actions

To setup the Galois descent problem for conjugacy classes of matrices, we needed an action of some subfunctor of $\mathbf{GL}_n$ on matrices. As we have seen in a previous paragraph, this action has some nice functorial properties. This leads to the following definition:

Definition 7.1. Let G be a group-valued functor, and let $\mathbf{F}$ any functor. We say that G **acts on** $\mathbf{F}$ if the following conditions hold:

(1) For every field extension K/k, the group $G(K)$ acts on the set $\mathbf{F}(K)$. This action will be denoted by $*$. (2) For every morphism $\iota : K \to L$ of field extensions, the following diagram is commutative:

$$\begin{array}{ccc} G(K) \times \mathbf{F}(K) & \longrightarrow & \mathbf{F}(K) \\ \downarrow{\scriptstyle (G(\iota),\mathbf{F}(\iota))} & & \downarrow{\scriptstyle \mathbf{F}(\iota)} \\ G(L) \times \mathbf{F}(L) & \longrightarrow & \mathbf{F}(L) \end{array}$$

That is, $\mathbf{F}(\iota)(g * a) = \mathbf{G}(\iota)(g) * \mathbf{F}(\iota)(a)$ for all $a \in \mathbf{F}(K)$ and $g \in \mathbf{G}(K)$.

In other words, for every field extension K/k, we have a group action of $G(K)$ on $\mathbf{F}(K)$ which is functorial in K.

Notice that the last condition rewrites

$(g * a)_L = g_L * a_L$ for all $a \in \mathbf{F}(K), g \in G(K)$

for a given field extension L/K if we use the short notation introduced at the beginning of the previous paragraph.

Examples 7.2.

(1) Let $G = \mathbf{GL}_n, \mathbf{SL}_n, \mathbf{O}_n, \mathbf{Sp}_{2n}, \ldots$ and let $\mathbf{F}$ be the functor defined by $\mathbf{F}(K) = K^n$ for every field extension K/k. Then G acts by left multiplication on $\mathbf{F}$. (2) If $G = \mathbf{GL}_n, \mathbf{SL}_n, \mathbf{O}_n, \mathbf{Sp}_{2n}, \ldots$ and $\mathbf{F} = \mathbf{M}_n$, then G acts on $\mathbf{F}$ by conjugation.

Remark 7.3. Let Ω/k be Galois extension. Recall from Lemma 6.3 that, given a functor $\mathbf{F}$, we have a natural action of $\mathcal{G}_\Omega$ on $\mathbf{F}(\Omega)$ defined by

$$\mathcal{G}_\Omega \times \mathbf{F}(\Omega) \to \mathbf{F}(\Omega), (\sigma, a) \mapsto \sigma \cdot a = \mathbf{F}(\sigma)(a).$$

If G is a group-scheme acting on $\mathbf{F}$, we have by definition

$\mathbf{F}(\sigma)(g * a) = G(\sigma)(g) * \mathbf{F}(\sigma)(a)$ for all $a \in \mathbf{F}(\Omega), \sigma \in \mathcal{G}_\Omega$,

which rewrites as

$\sigma \cdot (g * a) = (\sigma \cdot g) * (\sigma \cdot a)$ for all $a \in \mathbf{F}(\Omega), \sigma \in \mathcal{G}_\Omega$.

We would like to continue by giving a reformulation of the general Galois descent problem. For, we need to introduce the concept of a twisted form.

8 Twisted forms

Let G be a group-valued functor acting on a functor $\mathbf{F}$. This action of G allows us to define an equivalence relation on the set $\mathbf{F}(K)$ for every field extension K/k by identifying two elements which are in the same $G(K)$-orbit. For example, in the case of matrices, two matrices of $\mathrm{M}_n(K)$ will be equivalent if and only if they are $G(K)$-conjugate. More precisely, we have the following definition:

Definition 8.1. Let G be a group-scheme defined over k acting on $\mathbf{F}$. For every field extension K/k we define an equivalence relation $\sim_K$ on $\mathbf{F}(K)$ as follows: two elements $b, b' \in \mathbf{F}(K)$ are **equivalent over** K if there exists $g \in G(K)$ such that $b = g * b'$. We will denote by $[b]$ the corresponding equivalence class.

We may now formulate a general descent problem.

Galois descent problem: let $\mathbf{F}$ be a functor, and let G be a groupvalued functor acting on $\mathbf{F}$. Finally, let Ω/k be a Galois extension and let $a, a' \in \mathbf{F}(k)$. Assume that $a_\Omega \sim_\Omega a'_\Omega$. Do we have $a \sim_k a'$?

Notice that the answer to this question only depends on the $G(k)$equivalence class of a and a'. We now give a special name to elements of $\mathbf{F}$ which become equivalent to a fixed element $a \in \mathbf{F}(k)$.

Definition 8.2. Let $a \in \mathbf{F}(k)$, and let Ω/k be a Galois extension. An element $a' \in \mathbf{F}(k)$ is called **a twisted form of** a if $a'_\Omega \sim_\Omega a_\Omega$.

Clearly, if $a' \in \mathbf{F}(k)$ is a twisted form of a and $a' \sim_k a''$, then a'' is also a twisted form of a, so the equivalence relation $\sim_k$ restricts to the set of twisted forms of a. We denote by $\mathbf{F}_a(\Omega/k)$ the set of k-equivalence classes of twisted forms of a, that is

$$\mathbf{F}_a(\Omega/k) = \{[a'] \mid a' \in \mathbf{F}(k), a'_\Omega \sim_\Omega a_\Omega\}.$$

Notice that $\mathbf{F}_a(\Omega/k)$ always contains the class of a, so it is natural to consider $\mathbf{F}_a(\Omega/k)$ as a pointed set, where the base point is $[a]$.

Example 8.3. As pointed out before, if $\mathbf{F} = \mathbf{M}_n$, then $G \subset \mathbf{GL}_n$ acts on $\mathbf{F}$ by conjugation, and two matrices $M, M' \in \mathrm{M}_n(k)$ are then equivalent if and only if they are conjugate by an element

of $G(k)$. Moreover, if $M_0 \in \mathrm{M}_n(k)$, then $\mathbf{F}_{M_0}(\Omega/k)$ is the set of $G(k)$-conjugacy classes of matrices $M \in \mathrm{M}_n(k)$ which are $G(\Omega)$-conjugate to M_0.

Using the notation introduced previously, the Galois descent problem may be reinterpreted in terms of twisted forms. Given $a \in \mathbf{F}(k)$ and a Galois extension Ω/k, do we have $\mathbf{F}_a(\Omega/k) = \{[a]\}$?

We would like to describe $\mathbf{F}_a(\Omega/k)$ in terms of Galois cohomology of a suitable group-valued functor associated to a, under some reasonable conditions on $\mathbf{F}$ and G. To do this, we will continue to try to generalize the approach described in § 5.

9 The Galois descent condition

One of the crucial property we used to solve the conjugacy problem is the equality

$$\mathrm{M}_n(\Omega)^{\mathcal{G}_\Omega} = \mathrm{M}_n(k),$$

where we let $\mathcal{G}_\Omega$ act on $S \in \mathrm{M}_n(\Omega)$ coefficientwise.This action is nothing but the action of $\mathcal{G}_\Omega$ induced by the functorial properties of M_n, as described in Lemma 6.3. Now let us go back to our more general setting. For every Galois extension Ω/k, we have an action of $\mathcal{G}_\Omega$ on the set $\mathbf{F}(\Omega)$ given by

$$\sigma \cdot a = \mathbf{F}(\sigma)(a) \text{ for } \sigma \in \mathcal{G}_\Omega \text{ and } a \in \mathbf{F}(\Omega).$$

The second part of Lemma 6.3, applied to the Galois extensions k/k and Ω/k, then yields

$$\sigma \cdot a_\Omega = a_\Omega \text{ for all } \sigma \in \mathcal{G}_\Omega, a \in \mathbf{F}(k).$$

However, contrary to the case of matrices, an element of $\mathbf{F}(\Omega)$ on which $\mathcal{G}_\Omega$ acts trivially does not necessarily comes from an element of $\mathbf{F}(k)$.

Example 9.1. Let us consider the functor $\mathbf{F}$ defined as follows: for a field extension K/k, set

$$\mathbf{F}(K) = \begin{cases} \{0\} & \text{if } [K:k] \leq 1 \\ \{0,1\} & \text{if } [K:k] \geq 2 \end{cases}$$

the map induced by a morphism $K \to K'$ being the inclusion of sets. In particular, for every Galois extension Ω/k, the Galois group $\mathcal{G}_\Omega$ acts trivially on $\mathbf{F}(\Omega)$. However, if $[\Omega\colon k] > 1$, the element $1 \in \mathbf{F}(\Omega)$ does not come from an element of $\mathbf{F}(k)$.

These considerations lead to the following definition:

Definition 9.2. We say that a functor $\mathbf{F}$ satisfies the **Galois descent condition** if for every Galois extension Ω/k the map $\mathbf{F}(k) \to \mathbf{F}(\Omega)$ is injective and induces a bijection

$$\mathbf{F}(k) \simeq \mathbf{F}(\Omega)^{\mathcal{G}_\Omega}.$$

Example 9.3. The functor $\mathbf{M}_n$ satisfies the Galois descent condition.

Notice that this condition was also needed on the group-scheme G in the final argument.

10 Stabilizers

It follows from the considerations of the previous paragraph that it is reasonable to consider Galois descent problems for elements of a functor satisfying the Galois descent condition. Now that we have set a suitable framework for the general Galois descent problem, we need an appropriate substitute for the set $Z_G(M_0)(\Omega)$. As noticed before, denoting by $*$ the action of $G \subset \mathbf{GL}_n$ on matrices by conjugation, the subgroup $Z_G(M_0)(\Omega)$ may be reinterpreted as the stabilizer of M_0 with respect to the action of $G(\Omega)$ on $\mathrm{M}_n(\Omega)$, that is

$Z_G(M_0)(\Omega) = \mathbf{Stab}_G(M_0)(\Omega) = \{C \in G(\Omega) \mid C * M_0 = M_0\}$.

Since in our general setting we have a group-scheme acting on $\mathbf{F}$, it seems sensible to introduce the following definition:

Definition 10.1. Let G be a group-valued functor acting on $\mathbf{F}$. For $a \in \mathbf{F}(k)$, and every field extension K/k, we set

$\mathbf{Stab}_G(a)(K) = \{g \in G(K) \mid \ g * a_K = a_K\}$ for all K/k.

If $K \to K'$ is a morphism of field extensions, the map $G(K) \to G(K')$ restricts to a map $\mathbf{Stab}_G(a)(K) \to \mathbf{Stab}_G(a)(K')$. Indeed, for every $g \in \mathbf{Stab}_G(a)(K)$, we have

$$g_{K'} * a_{K'} = (g * a_K)_{K'} = (a_K)_{K'} = a_{K'}.$$

We then get a functor $\mathbf{Stab}_G(a)$, called the **stabilizer** of a.

Example 10.2. If $\mathbf{F} = \mathbf{M}_n$ and $M_0 \in \mathrm{M}_n(k)$, then

$$\mathbf{Stab}_G(M_0)(K) = Z_G(M_0)(K) \text{ for all } K/k.$$

Remark 10.3. Let Ω/k be a Galois extension. By definition, the map $\mathbf{Stab}_G(a)(\sigma) : \mathbf{Stab}_G(a)(\Omega) \to \mathbf{Stab}_G(a)(\Omega)$ is obtained by restriction of the map $G(\Omega) \to G(\Omega)$. Hence, the natural action of $\mathcal{G}_\Omega$ on $G(\Omega)$ restricts to an action on $\mathbf{Stab}_G(a)(\Omega)$.

We then obtain a Galois cohomology set $H^1(\mathcal{G}_\Omega, \mathbf{Stab}_G(a)(\Omega))$ for any Galois extension Ω/k.

11 Galois descent lemma

We are now ready to state and prove the Galois descent lemma:

Theorem 11.1 (Galois Descent Lemma)**.** *Let $\mathbf{F}$ be a functor, let G be a group-valued functor acting on $\mathbf{F}$, and let $a \in \mathbf{F}(k)$. Assume that $\mathbf{F}$ and G satisfy the Galois descent condition. Then for every Galois extension Ω/k, we have a bijection of pointed sets*

$\mathbf{F}_a(\Omega/k) \xrightarrow{\sim} \ker[H^1(\mathcal{G}_\Omega, \mathbf{Stab}_G(a)(\Omega)) \to H^1(\mathcal{G}_\Omega, G(\Omega))]$. *In particular, if $H^1(\mathcal{G}_\Omega, G(\Omega)) = 1$, we have a bijection*

$$\mathbf{F}_a(\Omega/k) \xrightarrow{\sim} H^1(\mathcal{G}_\Omega, \mathbf{Stab}_G(a)(\Omega)).$$

The bijection works as follows:

(1) *If $[a'] \in \mathbf{F}_a(\Omega/k)$ is the equivalence class of a twisted form $a' \in \mathbf{F}(k)$ of a, pick $g \in G(\Omega)$ such that $g * a'_\Omega = a_\Omega$. The corresponding cohomology class in the kernel of the map*

$$H^1(\mathcal{G}_\Omega, \mathbf{Stab}_G(a)(\Omega)) \to H^1(\mathcal{G}_\Omega, G(\Omega))$$

is the class of the cocycle

$$\alpha : \mathcal{G}_\Omega \to \mathbf{Stab}_G(a)(\Omega), \alpha_\sigma \mapsto \alpha_\sigma = g\,\sigma\cdot g^{-1}.$$

(2) *If $[\alpha] \in \ker[H^1(\mathcal{G}_\Omega, \mathbf{Stab}_G(a)(\Omega))) \to H^1(\mathcal{G}_\Omega, G(\Omega))]$, pick $g \in G(\Omega)$ such that $\alpha_\sigma = g\,\sigma\cdot g^{-1}$ for all $\sigma \in \mathcal{G}_\Omega$; the corresponding class in $\mathbf{F}_a(\Omega/k)$ is the equivalence class of the unique element $a' \in \mathbf{F}(k)$ satisfying $a'_\Omega = g^{-1} * a_\Omega$.*

Remark 11.2. Saying that we have a bijection of pointed sets means that it preserves the base points. Hence the class of $[a]$ corresponds to the class of the trivial cocycle.

Proof. The key ingredient of the proof is Corollary 4.6. By Remark 10.3, the action of $\mathcal{G}_\Omega$ on $G(\Omega)$ restricts to an action on $\mathbf{Stab}_G(a)(\Omega)$. Moreover, we have an exact sequence

$1 \to \mathbf{Stab}_G(a)(\Omega) \to G(\Omega) \to G(\Omega) * a_\Omega \to 1$

which satisfies the conditions of § 4. By Corollary 4.6, the kernel of $H^1(\mathcal{G}_\Omega, \mathbf{Stab}_G(a)(\Omega)) \to H^1(\mathcal{G}_\Omega, G(\Omega))$ is in one-to-one correspondence with the orbit set of $G(\Omega)^{\mathcal{G}_\Omega}$ in $(G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}$. Notice that $G(\Omega) * a_\Omega$ is simply the set of elements of $\mathbf{F}(\Omega)$ which are equivalent to a_Ω. Since $\mathbf{F}$ satisfies the Galois descent condition, it implies that $(G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}$ is equal to the set

$$\{a'_\Omega \mid a' \in \mathbf{F}(k), a'_\Omega \sim_\Omega a_\Omega\}.$$

In other words, $(G(\Omega) * a)^{\mathcal{G}_\Omega}$ is the image of the set of twisted forms of a under the map $\mathbf{F}(k) \to \mathbf{F}(\Omega)$. Now since G is Galois functor, $G(\Omega)^{\mathcal{G}_\Omega}$ is the image of $G(k)$ under the map $G(k) \to G(\Omega)$. Now we claim that if $g_\Omega \in G(\Omega)^{\mathcal{G}_\Omega}$ and $a'_\Omega \in (G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}$, then we have $g_\Omega \cdot a'_\Omega = (g * a')_\Omega$, where '$\cdot$' denotes here the action defined before

Corollary 4.6. Indeed, since a' is a twisted form of a, we may write $a'_\Omega = g' * a_\Omega$ for some $g' \in G(\Omega)$.Then g' is a preimage of a'_Ω under the map $G(\Omega) \to G(\Omega) * a_\Omega$ and thus

$$\begin{aligned} g_\Omega \cdot a'_\Omega &= (g_\Omega g') * a_\Omega \\ &= g_\Omega * (g' * a_\Omega) \\ &= g_\Omega * a'_\Omega \\ &= (g * a')_\Omega. \end{aligned}$$

We then get the $G(\Omega)^{\mathcal{G}_\Omega}$ orbit of a'_Ω in $(G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}$ is the image of $G(k) * a'$ under the map $\mathbf{F}(k) \to \mathbf{F}(\Omega)$. Hence the map $\mathbf{F}(k) \to \mathbf{F}(\Omega)$ induces a bijection between $\mathbf{F}_a(\Omega/k)$ and the orbit set of $G(\Omega)^{\mathcal{G}_\Omega}$ in $(G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}$. This proves the first part.

Let us now make the bijection a bit more explicit. If $[a'] \in \mathbf{F}_a(\Omega/k)$, the corresponding orbit of $G(\Omega)^{\mathcal{G}_\Omega}$ in $(G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}$ is the orbit of a'_Ω.By a definition of a twisted form, we may write $g * a'_\Omega = a_\Omega$ for some $g \in G(\Omega)$.Thus g^{-1} is a preimage of a'_Ω under the map $G(\Omega) \to G(\Omega) * a_\Omega$. By Corollary 4.6, the corresponding cohomology class is $\delta^0(g^{-1})$, that is the cohomology class represented by the cocycle

$$\alpha : \mathcal{G}_\Omega \to \mathbf{Stab}_G(a)(\Omega), \sigma \mapsto g\,\sigma\cdot g^{-1}.$$

Conversely, if $[\alpha] \in \ker[H^1(\mathcal{G}_\Omega, \mathbf{Stab}_G(a)(\Omega)) \to H^1(\mathcal{G}_\Omega, G(\Omega))]$, then there exists $g \in G(\Omega)$ such that

$$\alpha_\sigma = g\,\sigma\cdot g^{-1} \text{ for all } \sigma \in \mathcal{G}_\Omega.$$

In other words, we have $[\alpha] = \delta^0(g^{-1})$, and the corresponding element in $\mathbf{F}_a(\Omega/k)$ is represented by the unique element $a' \in \mathbf{F}(\Omega)$ satisfying $a'_\Omega = g^{-1} * a_\Omega$. ∎

We now give several examples of use of Galois descent.

Example 11.3. Let $\mathbf{F}$ be the functor defined by

$\mathbf{F}(K) = \{$ regular quadratic forms of dimension n over $K\}$,

the induced map being

$$\mathbf{F}(K) \to \mathbf{F}(L), q \mapsto q_L.$$

Then $\mathrm{GL}_n(K)$ acts on $\mathbf{F}(K)$ by $(f, q) \mapsto q \circ f^{-1}$, and this action is functorial. The corresponding equivalence relation is the usual 'isometry relation'. Moreover, the stabilizer of the unit form

$$k^n \to k, (x_1, \ldots, x_n) \mapsto x_1^2 + \ldots + x_n^2$$

is $\mathbf{O}_n$.

It is not difficult to see that all the conditions of the Galois descent lemma are satisfied. Hence, we have a bijection between the set of isometry classes of quadratic forms of dimension n which becomes isometric to the unit form over Ωand $H^1(\mathcal{G}_\Omega, \mathrm{O}_n(\Omega))$.

Example 11.4. Let A be a finite dimensional k-vector space. For any field extension K/k, let $\mathbf{F}(K)$ be the set of K-algebras with underlying K-vector space $\underline{A}_K = \underline{A} \otimes_k K$. If $\iota : K \to L$ is a morphism of field extensions of k, we define the induced map by

$$\mathbf{F}(\iota) : \mathbf{F}(K) \to \mathbf{F}(L), A \mapsto A_L = A \otimes_k L.$$

We then obtain a functor $\mathbf{F}$. Now let $f \in \mathrm{GL}(\underline{A}_K)$, and let A be a Kalgebra. We will write $x \cdot_A y$ for the product of two elements $x, y \in A$. The map

$$\underline{A}_K \times \underline{A}_K \to \underline{A}_K, (x, y) \mapsto f(f^{-1}(x) \cdot_A f^{-1}(y))$$

endows $\underline{A}_K$ with a structure of a K-algebra, that we will denote by $f \cdot A$. Straightforward computations show that this induces an action of $\mathbf{GL}(A)$ on $\mathbf{F}$. Notice that by definition, we have

$$f(x) \cdot_{f \cdot A} f(y) = f(x \cdot_A y) \text{ for all } x, y \in A,$$

so that f is an isomorphism of K-algebras from A onto $f \cdot A$. It easily follows that two K-algebras A and B are equivalent if and only if there are isomorphic as K-algebras.

Now fix a K-algebra $A \in \mathbf{F}(k)$. Then $\mathbf{Stab}_{\mathbf{GL}(\underline{A})}(A)$ is nothing but the functor $\mathbf{Aut}_{alg}(A)$ defined by

$$\mathbf{Aut}_{alg}(A)(K) = \mathrm{Aut}_{K-alg}(A \otimes_k K).$$

It is easy to check that $\mathbf{F}$ and $\mathbf{GL}(A)$ satisfy the conditions of the Galois descent lemma.Hence for any k-algebra A, the pointed set $H^1(\mathcal{G}_\Omega, \mathbf{Aut}_{alg}(A)(\Omega))$ classifies the isomorphism classes of k-algebras which become isomorphic to A over Ω. Moreover, the class of the trivial cocycle corresponds to the isomorphism class of A.

Remark 11.5. Let A be a k-algebra and let Ω/k be a Galois extension. If B is a k-algebra such that there exists an isomorphism $f : B_\Omega \xrightarrow{\sim} A_\Omega$ of Ω-algebras, the corresponding cohomology class is represented by the cocycle

$$\alpha : \mathcal{G}_\Omega \to \mathrm{Aut}_\Omega(A_\Omega), \sigma \mapsto f \circ \sigma \cdot f^{-1}.$$

Indeed, since f is a Ω-algebra isomorphism, we have

$$x \cdot_{f \cdot B_\Omega} y = f(f^{-1}(x) \cdot_{A_\Omega} f^{-1}(y)) = x \cdot_{A_\Omega} y \text{ for all } x, y \in A_\Omega,$$

and therefore $f \cdot B_\Omega = A_\Omega$. The description of the bijection in the Galois descent lemma then yields the result.

Conversely, the k-algebra corresponding to a cohomology class $[\alpha] \in H^1(\mathcal{G}_\Omega, \mathbf{Aut}_{\Omega-alg}(A_\Omega))$ is the isomorphism class of

$$B = \{a \in A_\Omega \mid \alpha_\sigma(\sigma \cdot a) = a \text{ for all } \sigma \in \mathcal{G}_\Omega\},$$

where the k-algebra structure is given by restriction of the algebra structure on A_Ω.

To see this, notice first that the isomorphism of Ω-vectors spaces

$$f : B_\Omega \xrightarrow{\sim} A_\Omega$$

given by Lemma 3.3 is in fact an isomorphism of Ω-algebras, so that $f \cdot B_\Omega = A_\Omega$.In view of the Galois descent lemma, it is therefore enough to show that we have

$$\alpha_\sigma = f \circ \sigma \cdot f^{-1} \text{ for all } \sigma \in \mathcal{G}_\Omega.$$

Since the elements of $B \otimes_k 1$ span A_Ω as an Ω-vector space (this simply comes from the fact that f is an isomorphism), it is enough to check this equality on the elements of the form $x \otimes 1, x \in B$. Now for all $x \in B$ and $\sigma \in \mathcal{G}_\Omega$, we have

$$\begin{aligned} \alpha_\sigma((\,\sigma\cdot f)(x \otimes 1)) &= \alpha_\sigma(\,\sigma\cdot(f(\sigma^{-1} \cdot (x \otimes 1)))) \\ &= \alpha_\sigma(\,\sigma\cdot(f(x \otimes 1))) \\ &= \alpha_\sigma(\,\sigma\cdot x) \\ &= x \\ &= f(x \otimes 1), \end{aligned}$$

which is the result we were looking for.

Let us now consider the case of G-algebras.

Definition 11.6. Let k be a field and let G be an abstract group. A G-**algebra** over k is a k-algebra on which G acts faithfully by k-algebra automorphisms. Two G-algebras over k are **isomorphic** if there exists an isomorphism of k-algebras which commutes with the actions of G. It will be denoted by $\simeq_G$.

Example 11.7. Let A be a finite dimensional k-vector space and let G be an abstract finite group. For any field extension K/k, let $\mathbf{F}(K)$ be the set of G-algebras over K with underlying vector space A. If $\iota : K \to L$ is a morphism of field extensions of k, we define the induced map by

$$\mathbf{F}(\iota) : \mathbf{F}(K) \to \mathbf{F}(L), A \mapsto A_L,$$

where the structure of G-algebra on A_L is given on elementary tensors by

$g \cdot (a \otimes \lambda) = (g \cdot a) \otimes \lambda$ for all $g \in G, a \in A, \lambda \in L$. Now let $f \in \mathrm{GL}(\underline{A} \otimes_k K)$, and let A be a G-algebra over K. Consider the K-algebra $f \cdot A$ as defined above. The map

$$G \times f \cdot A \to f \cdot A, (g, x) \mapsto f(g \cdot f^{-1}(x))$$

endows $f \cdot A$ with a structure of a G-algebra over K.

We then get an action of $\mathbf{GL}(A)$ on $\mathbf{F}$. Moreover, two G-algebras over K are equivalent if and only if they are isomorphic as G-algebras. Once again, all the conditions of the Galois descent lemma are fulfilled, and we get that for any G-algebra A and every Galois extension Ω/k, the pointed set

$$H^1(\mathcal{G}_\Omega, \mathbf{Aut}_{G-alg}(A)(\Omega))$$

classifies the G-isomorphism classes of G-algebras over k which become G-isomorphic to A over Ω. Moreover, the class of the trivial cocycle corresponds to the G-isomorphism class of A.

12 The conjugacy problem again

Let $G \subset \mathbf{GL}_n$ be a group-valued functor defined by polynomial equations. By Galois descent, the $G(k)$-conjugacy classes over k of matrices M which are $G(\Omega)$-conjugate to M_0 are in one-to-one correspondence with $\ker[H^1(\mathcal{G}_\Omega, Z_G(M_0)(\Omega)) \to H^1(\mathcal{G}_\Omega, G(\Omega))]$. Moreover, the $G(k)$conjugacy class of M_0 corresponds to the trivial cocycle.

Therefore, the conjugacy problem has a positive answer for all matrices M if and only if the map $H^1(\mathcal{G}_\Omega, Z_G(M_0)(\Omega)) \to H^1(\mathcal{G}_\Omega, G(\Omega))$ has trivial kernel. In particular, if $H^1(\mathcal{G}_\Omega, G(\Omega)) = 1$, the total obstruction to this problem is measured by $H^1(\mathcal{G}_\Omega, Z_G(M_0)(\Omega))$. Before examining the case of $G = \mathbf{SL}_n$, we need to generalize a bit Hilbert 90:

Proposition 12.1. *Let $L = L_1 \times \cdots \times L_r$, where $L_1, \ldots, L_r$ are finite field extensions of k. Then for every Galois extension Ω/k, we have*

$$H^1(\mathcal{G}_\Omega, (L \otimes_k \Omega)^\times) = 1.$$

Proof. Assume first that $r = 1$, that is L is a field. Set $A = L \otimes_k \Omega$. We will use Galois descent for vector spaces, as for the proof of Hilbert 90. Let $\alpha : \mathcal{G}_\Omega \to A^\times$ be a cocycle. We twist the action of $\mathcal{G}_\Omega$ on A by setting

$$\sigma * x = \alpha_\sigma \, \sigma \cdot x \text{ for all } \sigma \in \mathcal{G}_\Omega, x \in A.$$

The action above is semi-linear and then we have an isomorphism of Ω-vector spaces

$$f : V \otimes_k \Omega \xrightarrow{\sim} A, v \otimes \lambda \mapsto v \cdot \lambda = v(1 \otimes \lambda),$$

where $V = \{x \in A \mid \sigma * x = x \text{ for all } x \in \mathcal{G}_\Omega\}$. It is easy to check that V is an L-vector space and that f is an isomorphism of A-modules (left as an exercice for the reader).Since $V \otimes_k \Omega \simeq A = L \otimes_k \Omega$, we have

$\dim_k(V) = \dim_\Omega(V \otimes_k \Omega) = \dim_\Omega(L \otimes_k \Omega) = \dim_k(L)$,

and thus

$$\dim_L(V) = \frac{\dim_k(V)}{\dim_k(L)} = 1.$$

Hence $V = e \cdot L$, for some $e \in V$. Now $e \otimes 1$ is an A-basis of $V \otimes_k \Omega$, so f is just multiplication by $f(e \otimes 1) \in A$. Since f is bijective, $f(e \otimes 1) \in A^\times$. Now $f(e \otimes 1) = e \in V$, and therefore

$$e = \sigma * e = \alpha_\sigma \, \sigma \cdot e \text{ for all } \sigma \in \mathcal{G}_\Omega.$$

This implies that $\alpha = e \, \sigma \cdot e^{-1}$ for all $\sigma \in \mathcal{G}_\Omega$, meaning that α is trivial.

Let us go back to the general case. If $L = L_1 \times \cdots \times L_r$, then we have an isomorphism of $\mathcal{G}_\Omega$-modules,

$(L \otimes_k \Omega)^\times \simeq (L_1 \otimes_k \Omega)^\times \times \cdots \times (L_r \otimes_k \Omega)^\times$.

We then have

$H^1(\mathcal{G}_\Omega, L \otimes_k \Omega) \simeq H^1(\mathcal{G}_\Omega, (L_1 \otimes_k \Omega)^\times) \times \cdots \times H^1(\mathcal{G}_\Omega, (L_r \otimes_k \Omega)^\times)$,

and we use the previous case. ∎

If E is a finite dimensional algebra over a field F, we denote by $N_{E/F}(x)$ the determinant of left multiplication by x (considered as an endomorphism of the F-vector space E).

Example 12.2. Let $E = k^n, n \geq 1$. If $x = (x_1, \ldots, x_n)$, then we have

$$N_{E/k}(x) = x_1 \cdots x_n,$$

since the representative matrix of ℓ_x in the canonical basis of E is simply the diagonal matrix whose diagonal entries are $x_1, \ldots, x_n$.

Definition 12.3. If L/k is a finite dimensional commutative k-algebra, we denote by $\mathbb{G}^{(1)}_{m,L}$ the functor defined by

$$\mathbb{G}^{(1)}_{m,L}(K) = \{x \in (L \otimes_k K)^\times \mid N_{L \otimes_k K/K}(x) = 1\},$$

for every field extension K/k.

We now compute $H^1(\mathcal{G}_\Omega, \mathbb{G}^{(1)}_{m,L}(\Omega))$ in a special case.

Lemma 12.4. *Let L be a finite dimensional commutative k-algebra, and let Ω/k be a finite Galois extension. Assume that $L \otimes_k \Omega \simeq \Omega^n$ for some $n \geq 1$. Then we have*

$$H^1(\mathcal{G}_\Omega, \mathbb{G}^{(1)}_{m,L}(\Omega)) \simeq k^\times / N_{L/k}(L^\times).$$

Proof. The idea of course is to fit $\mathbb{G}^{(1)}_{m,L}(\Omega)$ into an exact sequence of $\mathcal{G}_\Omega$-modules. We first prove that the norm map

$$N_{L\otimes_k\Omega/\Omega} : (L\otimes_k\Omega)^\times \to \Omega^\times$$

is surjective.For, let $\varphi : L\otimes_k\Omega \xrightarrow{\sim} \Omega^n$ be an isomorphism of Ωalgebras. We claim that we have $N_{L\otimes_k\Omega}(x) = N_{\Omega^n/k}(\varphi(x))$ for all $x \in L\otimes_k\Omega$. Indeed, if $\mathbf{e} = (e_1,\dots,e_n)$ is a Ω-basis of $L\otimes_k\Omega$, then $\varphi(\mathbf{e}) = (\varphi(e_1),\dots,\varphi(e_n))$ is a Ω-basis of Ω^n, and we have easily

$$\mathrm{Mat}(\ell_{\varphi(x)},\varphi(\mathbf{e})) = \mathrm{Mat}(\ell_x,\mathbf{e}).$$

The desired equality then follows immediately. Now for $\lambda\in\Omega^\times$, set $x_\lambda = \varphi^{-1}((\lambda,1,\dots,1))$. The equality above and Example 12.2 then yield

$$N_{L\otimes_k\Omega/\Omega}(x_\lambda) = N_{\Omega^n/\Omega}((\lambda,1,\dots,1)) = \lambda.$$

Therefore $N_{L\otimes_k\Omega/\Omega}$ is surjective and we have an exact sequence of $\mathcal{G}_\Omega$modules

$1\cdot\mathbb{G}^{(1)}_{m,L}(\Omega)\ (L\otimes_k\Omega)^\times\ \Omega^\times\ 1$,

where the last map is given by the norm $N_{L\otimes\Omega/\Omega}$. It is known that the condition on L implies in particuliar that L is the direct product of finitely many finite field extensions of k. Applying Galois cohomology and using Proposition 12.1 yield the exact sequence

$$(L\otimes_k 1)^\times \to k^\times \to H^1(\mathcal{G}_\Omega,\mathbb{G}^{(1)}_{m,L}(\Omega)) \to 1,$$

the first map being $N_{L\otimes_k\Omega/\Omega}$. Now it is obvious from the properties of the determinant that we have

$$N_{L\otimes_k\Omega/\Omega}(x\otimes 1) = N_{L/k}(x) \text{ for all } x\in L.$$

The exactness of the sequence above then gives the desired result. ∎

Remark 12.5. The isomorphim above works as follows: If $\overline{a}\in k^\times/N_{L/k}(L^\times)$, pick $z\in L\otimes_k\Omega$such that $a = N_{L\otimes_k\Omega/\Omega}(z)$ (this is possible since $N_{L\otimes_k\Omega/\Omega}$ is surjective). Then the corresponding cohomology class is represented by the cocycle

$$\alpha : \mathcal{G}_\Omega \to \mathbb{G}^{(1)}_{m,L}(\Omega), \sigma\mapsto z^{-1}\sigma\cdot z.$$

Conversely, if $[\alpha]\in H^1(\mathcal{G}_\Omega,\mathbb{G}^{(1)}_{m,L}(\Omega))$, pick $z\in(L\otimes_k\Omega)^\times$ such that

$$\alpha_\sigma = z^{-1}\sigma\cdot z \text{ for all } \sigma\in\mathcal{G}_\Omega.$$

Then $a = N_{L\otimes_k\Omega/}(z)$ lies in fact in $k^\times$, and $\overline{a}\in k^\times/N_{L/k}(L^\times)$ is the class corresponding to $[\alpha]$.

Now let us go back to the conjugacy problem of matrices.

Assume that $M_0 = C_\chi\in \mathrm{M}_n(k)$ is a companion matrix of some monic polynomial $\chi\in k[X]$ of degree $n\geq 1$. In this case, it is known that every matrix commuting with M_0 is a polynomial in M_0, so $Z_G(M_0)(\Omega) = \Omega[M_0]\cap G(\Omega)$. Moreover, the minimal polynomial and the characteristic polynomial are both equal to χ. Set $L = k[X]/(\chi)$, so that we have an isomorphism of k-algebras

$$L\to k[M_0], \overline{P}\to P(M_0),$$

which induces in turn a Galois equivariant isomorphism of Ω-algebras

$$f : L\otimes_k\Omega\xrightarrow{\sim}\Omega[M_0], \overline{X}\otimes\lambda\mapsto\lambda M_0.$$

In particular, f induces an isomorphism of $\mathcal{G}_\Omega$-modules

$$(L\otimes_k\Omega)^\times\simeq\Omega[M_0]^\times.$$

Notice now that if $C \in \mathrm{GL}_n(\Omega)$ commutes with M_0, then C^{-1} also commutes with M_0. Therefore, we have the equalities

$$Z_{\mathbf{GL}_n}(M_0)(\Omega) = \Omega[M_0] \cap \mathrm{GL}_n(\Omega) = \Omega[M_0]^\times,$$

so f induces an isomorphism of $\mathcal{G}_\Omega$-modules

$$(L \otimes_k \Omega)^\times \simeq Z_{\mathbf{GL}_n}(M_0)(\Omega).$$

By Proposition 12.1, we then get $H^1(\mathcal{G}_\Omega, Z_{\mathbf{GL}_n}(M_0)(\Omega)) = 1$, as expected. Now let us identify $Z_{\mathbf{SL}_n}(M_0)(\Omega)$. **Claim:** We have $\det(f(x)) = N_{L\otimes_k\Omega/\Omega}(x)$ for all $x \in L \otimes_k \Omega$.

To see this, set $\alpha = \overline{X} \in L$. The tuple $\mathbf{e} = (1 \otimes 1, \alpha \otimes 1, \dots, \alpha^{n-1} \otimes 1)$ is an Ω-basis of $L \otimes_k \Omega$. Let

$$x = \sum_{i=0}^{n-1} \alpha^i \otimes \lambda_i \in L \otimes_k \Omega \quad \text{and} \quad P = \sum_{i=0}^{n-1} \lambda_i X^i.$$

We have $\ell_x = P(\ell_{\alpha\otimes 1})$. The matrix of $\ell_{\alpha\otimes 1}$ in the basis $\mathbf{e}$ is $C_\chi = M_0$, so the matrix of ℓ_x is $P(M_0) = f(x)$. Therefore $\det(\ell_x) = \det(f(x))$, as claimed.

We then get $Z_{\mathbf{SL}_n}(M_0)(\Omega) \simeq \mathbb{G}^{(1)}_{m,L}(\Omega)$ as a Galois module.

Assume now that χ is separable (i.e. χ has only simple roots in an algebraic closure of k) and that Ω/k is a Galois extension containing all the roots of χ. In this case, we have $L \otimes_k \Omega \simeq \Omega^n$, and by the previous lemma, we have

$$H^1(\mathcal{G}_\Omega, Z_{\mathbf{SL}_n}(M_0)(\Omega)) \simeq k^\times / N_{L/k}(L^\times),$$

which is not trivial in general.

For example, assume that $\mathrm{char}(k) \neq 2$ and take $d \in k^\times$ with $d \notin k^{\times 2}$. Set

$$M_0 = \begin{pmatrix} 0 & 1 \\ d & 0 \end{pmatrix} \qquad \text{and} \qquad M = \begin{pmatrix} 0 & -1 \\ -d & 0 \end{pmatrix}.$$

Then M_0 is the companion matrix of $\chi = X^2 - d$, and $L = k(\sqrt{d})$. The field $\Omega = k(i, \sqrt{d})$, where $i^2 = -1$, contains all the roots of χ. The extension Ω/k is Galois with Galois group isomorphic to $\mathbb{Z}/2\mathbb{Z}$ or $(\mathbb{Z}/2\mathbb{Z})^2$, depending on whether $-d$ is a square in $k^\times$.

With $Q = \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$ we have $QMQ^{-1} = M_0 \in M_2(\Omega)$. Thus M and M_0 are conjugate by an element of $\mathrm{SL}_2(\Omega)$.

However, they are not conjugate by an element of $\mathrm{SL}_2(k)$ in general. To see this, let us compute the class in $k^\times/N_{L/k}(L^\times)$ corresponding to the conjugacy class of M. Notice first that $Q\dot{\sigma}\cdot Q^{-1}$ is the identity matrix I_2 if $\sigma(i) = i$ and is -I_2 otherwise. In other words, we have

$$\alpha^Q_\sigma = (iI_2)^{-1}\sigma\cdot(iI_2) \text{ for all } \sigma \in \mathcal{G}_\Omega.$$

Via the isomorphism $H^1(\mathcal{G}_\Omega, \mathbb{G}^{(1)}_{m,L}(\Omega)) \simeq H^1(\mathcal{G}_\Omega, Z_{\mathbf{SL}_n}(M_0)(\Omega))$ induced by f_*, the cohomology class $[\alpha^{(Q)}]$ correspond to the cohomology class of the cocycle

$$\beta^{(Q)} : \mathcal{G}_\Omega \to \mathbb{G}^{(1)}_{m,L}(\Omega), \sigma \mapsto (1 \otimes i)^{-1}\sigma\cdot 1 \otimes i.$$

Now $N_{L\otimes\Omega/\Omega}(1 \otimes i) = (1 \otimes i)^2 = -1$, and thus the conjugacy class of M corresponds to the class of -1 in $k^\times/N_{L/k}(L^\times)$. In particular, M and M_0 are conjugate over k if and only if $-1 \in N_{L/k}(L^\times)$. Therefore, to produce counterexamples, one may take for k any subfield of $\mathbb{R}$ and $d < 0$, as we did in the introduction.

13 The case of infinite Galois extensions

In this ultimate paragraph, we would like to indicate quickly how to generalize all this machinery to arbitrary Galois extensions, even infinite ones. I will be extremely vague here, since it can become very quickly quite technical.

Let us come back to the conjugacy problem of matrices one last time, but assuming that Ω/k is completely arbitrary, possibly of infinite degree.The main idea is that the problem locally boils down to the previous case. Let us fix $M_0 \in \mathrm{M}_n(k)$ and let us consider a specific matrix $M \in \mathrm{M}_n(k)$ such that

$$QMQ^{-1} = M_0 \text{ for some } Q \in \mathrm{SL}_n(\Omega).$$

If L/k is any finite Galois subextension of Ω/k with Galois group $\mathcal{G}_L$ containing all the entries of Q, then $Q \in \mathrm{SL}_n(L)$ and the equality above may be read in $\mathrm{M}_n(L)$. Therefore, for this particular matrix M, the descent problem may be solved by examining the corresponding element $[\alpha^{(L)}] \in H^1(\mathcal{G}_L, Z_{\mathrm{SL}_n}(M_0)(L))$. Now if we take another finite Galois subextension L'/k such that $M \in \mathrm{M}_n(L')$ and $Q \in \mathrm{SL}(L')$, we obtain an obstruction $[\alpha^{(L')}] \in H^1(\mathcal{G}_{L'}, Z_{\mathrm{SL}_n}(M_0)(L'))$. But the fact that M is conjugate or not to M_0 by an element of $\mathrm{SL}_n(k)$ is an intrisic property of M and of the field k, and should certainly not depend on the chosen Galois extension L/k. Therefore, we need to find a way to patch these local obstructions together.

There are two ways to proceed. First of all, notice that if L_1/k and L_2/k are two finite Galois extensions such that $L_1 \subset L_2$, then the maps

$$\mathcal{G}_{L_2} \to \mathcal{G}_{L_1}, \sigma_2 \mapsto (\sigma_2)_{|_{L_1}} \text{ and } Z_{\mathrm{SL}_n}(M_0)(L_1) \hookrightarrow Z_{\mathrm{SL}_n}(M_0)(L_2)$$

are compatible, so we have a well-defined map

$$\inf_{L_1,L_2} : H^1(\mathcal{G}_{L_1}, Z_{\mathrm{SL}_n}(M_0)(L_1)) \to H^1(\mathcal{G}_{L_2}, Z_{\mathrm{SL}_n}(M_0)(L_2)),$$

which sends $[\alpha]$ to the class of the cocycle

$$\mathcal{G}_{L_2} \to Z_{\mathrm{SL}_n}(M_0)(L_2), \sigma_2 \mapsto \alpha_{(\sigma_2)_{|_{L_1}}}.$$

If we examine the classes $[\alpha^{(L)}]$ and $[\alpha^{(L')}]$ above, one can check that they are both equal to $[\alpha^{(LL')}]$ when we "push them to LL'". More precisely, we have

$\inf_{L,LL'}([\alpha^{(L)}]) = [\alpha^{(LL')}] = \inf_{L',LL'}([\alpha^{(L')}])$,

so we have a whole collection of cohomology classes which coincide when seen "high enough". The idea is then to force all of these classes to be equal by factoring by an appropriate equivalence relation. Of course, there is no particular reason to limit ourselves to $Z_G(M_0)$. If G is a group-valued functor, we may consider the disjoint union

$$\coprod_L H^1(\mathcal{G}_L, G(L)),$$

where L/k runs over all finite Galois subextensions of Ω.We now put the following equivalence relation on this set: we say that $[\alpha] \in H^1(\mathcal{G}_L, G(L))$ and $[\alpha'] \in H^1(\mathcal{G}_{L'}, G(L'))$ are equivalent if there exists a finite Galois extension $L'', L'' \supset L, L'' \supset L'$ such that

$$\inf_{L,L''}([\alpha]) = \inf_{L',L''}([\alpha']).$$

We denote the quotient set by

$$H^1_{ind}(\mathcal{G}_\Omega, G(\Omega)).$$

We then see that our collection of classes $[\alpha^{(L)}]$ define the same element in this set.However, this might be a bit difficult to handle in the applications, so we propose now an alternative.

First of all, we introduce a topology on $\mathcal{G}_\Omega$. The Krull topology is the topology generated by the subsets

$$\sigma \mathrm{Gal}(\Omega/K), \sigma \in \mathcal{G}_\Omega, K \subset \Omega, [K : k] < +\infty.$$

We now consider a group-valued functor G such that:

(1) For all finite Galois subextension L/k, the map $G(L) \to G(\Omega)$ is injective and induces a group isomorphism

$$G(L) \simeq G(\Omega)^{\mathrm{Gal}(\Omega/L)}$$

(2) For all $g \in G(\Omega)$, the subgroup $\{\sigma \in \mathcal{G}_\Omega \mid \sigma \cdot g = g\}$ is open.

These two conditions say that an element $g \in G(\Omega)$ 'comes from' an element of $G(L)$ for some finite Galois subextension L/k of Ω/k, and that the action of $\mathcal{G}_\Omega$ is in fact the same as the action of $\mathcal{G}_L$ on g when viewed as an element of $G(L)$. One can show that any functor G defined by a finite set of polynomial equations with coefficients in k satisfy these assumptions. For example, this is exactly what happens in the case of matrices.

We may then define a cohomology set $H^1_{cont}(\mathcal{G}_\Omega, G(\Omega))$ as in the finite case, but we ask for **continuous** cocycles, where $\mathcal{G}_\Omega$ is endowed with the Krull topology and $G(\Omega)$ is endowed with the discrete topology. The nice thing is that we have

$$H^1_{cont}(\mathcal{G}_\Omega, G(\Omega)) \simeq H^1_{ind}(\mathcal{G}_\Omega, G(\Omega)).$$

Therefore, we have achieved what we wanted, that is finding a way to patch a family of cohomology classes together. Moreover, as long as (1) and (2) are satisfied, all the previous results generalize to arbitrary Galois extensions.

As a final remark, we should point out that we could define the pointed set $H^1(\mathcal{G}_\Omega, G(\Omega))$ dropping the continuity condition, but the equality above does not hold anymore, and therefore one cannot always do patching, so this definition is not really suitable.