树仁書院
SHUREN COLLEGE

数学 讲...班 ...

12012612 董...

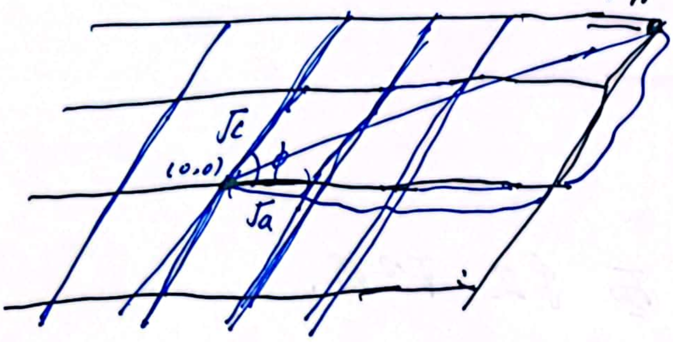
主要参考 ① 克莱因，数学在19世纪的发展
（中，英皆有，于图书馆藏）
② 冯克勤，代数数论简史

## 二、模形式的导入

A、正定二次型的格网表示

$am_1^2+2bm_1m_2+cm_2^2$，正定。

$\therefore \begin{cases} a>0 \\ b^2-ac=-D<0 \\ c>0 \end{cases}$ 现考虑 $m_1, m_2$ 为整数时的情况




一边长为 $\sqrt{a}$
一边长为 $\sqrt{c}$
夹角为 $\phi$

$\therefore$ 格点 $(m_1,m_2)$ 到原点距离为

$$c^2 = m_1^2 a + m_2^2 c + 2\cos\phi\sqrt{ac}$$

$$= m_1^2 a + 2bm_1m_2 + m_2^2 c$$

所以，在几何上表现了当 $m_1, m_2 \in \mathbb{Z}$ 时
二次型 $am_1^2+2bm_1m_2+cm_2^2$ 的取值情况

二次型格网的表示.

记 denote $D = ac - b^2$

~~$\sqrt{D} = \sqrt{a}\sqrt{c}\sin\phi =$~~

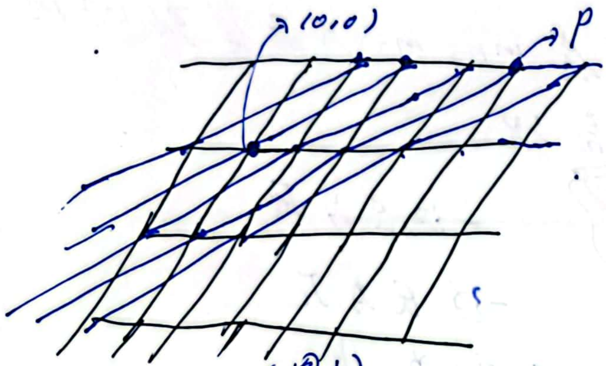
∴ ~~$\sqrt{D} = \sqrt{a}\sqrt{c}\sin\phi$~~ ∴ $\sqrt{D} = \sqrt{ac-b^2} = \sqrt{a}\sqrt{c}\sin\phi$

表示平行四边形之面积

~~格网的等价~~

Defition:

两个格网等价, if 它们包含相同的格点.




就是二相似格网.

(图1)

Prop. ① 相似格网面积相同.

② 设 ~~存格网上~~ 对同一格点,

有格网间的变换

$m_1' = \alpha m_1 + \beta m_2$ 则对于相似的格网,

$m_2' = \gamma m_1 + \delta m_2$ 有 $\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = \alpha\delta - \beta\gamma = 1$

例: ~~对P, 在存格网中坐标为(4, 1)~~

~~现格网中坐标为~~

图1中, $\begin{cases} m_1' = m_1 \\ m_2' = 2m_1 + m_2 \end{cases}$ $\begin{vmatrix} 1 & 0 \\ 2 & 1 \end{vmatrix} = 1$

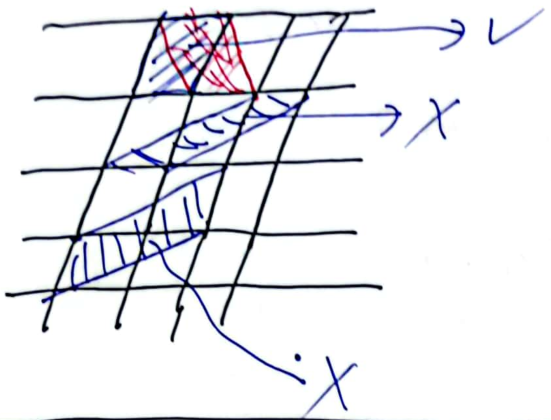
树仁書院 SHUREN COLLEGE

讨论班 

等价类中的格相注元.

易知，每类格网中恰有两 infinite 的格网.

格注元选为基本平行四边形最接近正方形的矩形的




初等计算后，
在不计旋转下，
等价类中仅此格网唯1.

整格网

当我 now, consider $a, b, c \in \mathbb{Z}$

问题：对给定 $D$，在 $a, b, c \in \mathbb{Z}$ 时，有多少二次型的等价类？

下面建立函数论点之间的联系（模形式）

核心：考虑3变量函数 $f(u, w_1, w_2)$.

~~由群变换~~ 对 $u, w_1, w_2$，有变换

$u' = u + m_1 w_1 + m_2 w_2$ （平移，对 $u$ 平面）
（几何意义为在格网中解释）

$w_1' = \alpha w_1 + \beta w_2$ $\quad(\alpha\delta - \beta\gamma = 1)$

$w_2' = \gamma w_1 + \delta w_2$

（模变换）

南方科技大学

研究在这些变换构成的变换群下的不变式 $f$

~~至于解析椭圆函数的~~
本自成一般的椭圆函数理论.

---

具体的例子.

魏尔氏函数

$$\begin{cases} \wp(u|w_1,w_2), & g_2(w_1,w_2) \\ \wp'(u|w_1,w_2)=\frac{\partial \wp}{\partial u}, & g_3(w_1,w_2) \end{cases}$$

→ 不变量

其中,

$$\wp(u|w_1,w_2)=u^{-2}+\sum{}'\left\{(u+m_1w_1+m_2w_2)^{-2}-(m_1w_1+m_2w_2)^{-2}\right\}$$

$$\wp'(u|w_1,w_2)=-2\sum(u+m_1w_1+m_2w_2)^{-3}$$

$$g_2(w_1,w_2)=60\sum{}'(m_1w_1+m_2w_2)^{-4}$$

$$g_3(w_1,w_2)=140\sum{}'(m_1w_1+m_2w_2)^{-6}$$

( $\sum'$表示求和中去掉 $m_1=m_2=0$ 这项 )

$\wp,\wp'$ 为 $u'=u+m_1w_1+m_2w_2$ 变换下不变的函数 (双周期意义)

- 变数转为椭圆函数
- 变数转为自守函数

Theorem: 任意三变量自守函数, 皆为 $\wp,\wp',g_2,g_3$ 的有理函数.

已阅

在 $\begin{cases}\bar{w}_1 = \alpha w_1 + \beta w_2 \\ \bar{w}_2 = \gamma w_1 + \delta w_2\end{cases}$ $\det\begin{pmatrix}\alpha & \beta \\ \gamma & \delta\end{pmatrix} = 1$ 下不变的函数.

魏尔斯特拉斯 σ-函数：

$$\sigma(u) = u \cdot \prod{}'\left(1 - \frac{u}{m_1w_1 + m_2w_2}\right) \cdot \exp\left[\frac{u}{m_1w_1+m_2w_2} + \frac{1}{2}\left(\frac{u}{m_1w_1+m_2w_2}\right)^2\right]$$

当研究上述换 $w_1, w_2$ 的函数时,

~~此 $w_1, w_2$~~ 权k 模形式中的一个条件是

$\cancel{f(z) = f(\alpha z), \ \alpha \in SL_2(\mathbb{Z})}$

$\cancel{\alpha z = \frac{az+b}{cz+d}}$ $\cancel{f(z) = (cz+d)^k f(\ldots)}$

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z), \quad z \in H$$

$\begin{pmatrix}a & b \\ c & d\end{pmatrix} \in SL_2(\mathbb{Z})$ $f$ 是 $H$ 上全纯函数.

当 $k=0$ 时, 有

$$f(w) = f\left(\frac{\alpha w + \beta}{\gamma w + \delta}\right)$$

从而类似对 $u$ 平面的格子分割

与对 $u$ 平面的格子分割.

克氏说的是 关于 $m_1w_1 + m_2w_2$ 的二次型 $am_1^2 + 2bm_1m_2 + cm_2^2$ 的理论有关.

但是我看不懂！
(王兄上场讨论)

## 应用 | 大纲.

### 二次型的整数解.

设有理数域Q上

$$f(x_1,\dots,x_k)=\sum_{i,j=1}^{k} a_{ij}x_ix_j \quad (a_{ij}\in Q)$$

为有理系数正定二次型.

对于 $n\in N^*$ ， $f(x_1,\dots,x_k)=n$

的整数解个数为 $N_f(n)$

Def: $\theta_f(\tau)=\sum_{n=0}^{\infty} N_f(n)e^{2\pi i n\tau}$ $(\tau\in H)$

对于任意 $f$， $\theta_f(\tau)$ 为某个子群的

权 $\frac{k}{2}$ 的模形式 (P1)

之后经过我看不懂的操作，得.

在有些时候，就可得到 $N_f(n)$ 的表达式.

例：当 $f(x_1,\dots,x_8)=\sum_{i,j=1}^{8} a_{ij}x_ix_j$

则 $N_f(n)=240\sum_{d|n} d^3$

(学了上面以后希望可以会.)

最后的我也看不懂了，希望一起学会.

P6

第一次讨论班 王开元

树仁書院 SHUREN COLLEGE

① $\boxed{\text{Finite field}}$

12012612 . 王开元

I. Characteristic of finite field

$char(F)=p$ , if $\underbrace{1+1+\cdots+1}_{p}=0$

Prop 1. $\begin{cases} F \text{ is finite, then } char(F)=p \text{, prime} \\ \text{if } char(F)=0 \text{, then } \mathbb{Q} \text{ 为 } F \text{ 之 sub field,} \\ \text{从而 } F \text{ is infinite} \end{cases}$

问题：试找出 $char(F)\neq 0$ 的 infinite field 的例子，如果存在的话。

Prop 2. 对 $char(F)=p$，设 $\Omega$ 为 $F$ 的 algebraically closed field，则在 $\Omega$ 上

注：设 $K$ 为 field，$K$ 上任意高于0次的多项式均于 $K$ 上有零点，也就是任意高于0次多项式可分解为一次多项式之积，则称 $K$ 为代数闭域。

任意域 $F$ 皆存在代数闭域 $K$ 为扩域。

存在唯一域 $F_q$，$q=p^f$，$f\in N^*$。

pf: consider $x^{p^f}-x=0$ $\therefore p^f x^{p^f-1}-1=-1$

又 $(x^{p^f}-x, -1)=1$ $\therefore$ 无重根，故有 $p^f$ 个解。记解集为 $F_q$

$(\alpha+\beta)^{p^f}=\alpha^{p^f}+\beta^{p^f}$,

$\therefore \begin{cases} 1,0\in F_q \\ F_q \text{ 关于 “+”、“×” 封闭} \\ p=2\text{时}, 1=-1 \quad p\neq 2\text{时}, (-\alpha)^{p^f}+\alpha=(-1)^{p^f}\alpha^{p^f}+\alpha \\ \qquad\qquad =-\alpha^{p^f}+\alpha=0 \\ \therefore -\alpha\in F_q, \text{ if } \alpha\in F_q \\ ((\alpha^{-1})^{p^f}-(\alpha^{-1}))(\alpha^{p^f+1})=\alpha-\alpha^{p^f}=0 \\ \therefore \alpha^{-1}\in F_q, \text{ if } \alpha\in F_q \end{cases}$

注: in fact

而 $\Omega \longmapsto \Omega$, $x \longmapsto x^q$ 为 - automorphism

$F_q$ 为其 invariant point set.

故为 field.

唯一性: 由 ∵ $q$ 阶群 $G$, $G^*$ 有 $q-1$ 个元素

$\therefore \forall \theta \in G^*$, $\theta^{q-1}=1$ $\therefore \theta^q=\theta$

而 $x^q=x$ 在 $\Omega$ 中仅有 $q$ 个根

II、the multiplicative group of a finite field.

Theorem: any finite ~~group~~ field, $F_q^*$ is a ~~circle~~ cyclic group.

proof ① (serre)

lemma 1. $n \in N^*$, then $n=\sum_{d|n}\phi(d)$

pf ① (serre)

$\mathbb{Z}/n\mathbb{Z}$ 关于"+"为 cyclic group of order $n$.

对于 $\forall d$, $d|n$, 易知 $\mathbb{Z}/n\mathbb{Z}$ 有唯一 $d$ 阶子群

($\because s \in G_d$, 则 $sd=kn$ $\therefore s=\frac{k}{d}n$)

而 $d$ 阶子群中 generators 个数为 $\phi(d)$

$(\frac{n}{d}, 2\frac{n}{d}, \dots, (d-1)\frac{n}{d}, 0)$

显然, 若 $\alpha$ 为 $d$ 阶子群的 generator,

则 $\alpha$ 在 $\mathbb{Z}/n\mathbb{Z}$ 中阶为 $d$. 反之亦然。

$\because \forall \alpha \in \mathbb{Z}/n\mathbb{Z}$, 皆有唯一阶对应, 故:

$$\sum_{d|n}\phi(d)=\#(\mathbb{Z}/n\mathbb{Z})=n$$

Pf ② (Gauss)

(§40) 设 $a, a', a''$ 为 $A$ 之 divisors

由 将与 $a$ 互素且小于 $a$ 之数乘以 $\frac{A}{a}$

$a'$ $\qquad\qquad \frac{A}{a'}$

...

故 共有 $\phi(a)+\cdots+\phi(a'')$ 个数，皆不大于 $A$

① 其中数两两不同

if $u\frac{A}{a'} = v\frac{A}{a^2}$, $(u, a')=1$, $(v, a^2)=1$

则 $ua^2 = va'$ $\therefore u \mid v,\ v \mid u \Rightarrow u=v$

$\therefore a' = a^2$

② $1, \ldots, A$ 中数皆在其中

$\forall t$, 设 $(t, A)=\delta$, $\frac{A}{\delta} \mid A$.

$\frac{t}{\delta} \le \frac{A}{\delta}$, 且 $(\frac{t}{\delta}, \frac{A}{\delta})=1$ $\therefore \frac{t}{\delta}\times\delta = t$ 在其中

综上, $\sum_{d\mid n}\phi(d) = n$

注: Serre 之证法实际是高斯应用此结论证明 $\mathbb{Z}/p\mathbb{Z}^*$ 中原根存在性的方法.

~~以此证~~

既: 设 $d \mid n$, 则 $d$ 阶原根~~若存在~~要有, 则有 $\phi(d)$ 个. 要么没有 ($x^d \equiv 1\ (p)$)

又 $\because \sum_{d\mid p-1}\phi(d) = p-1$, 且 $\forall$ $p-1$ 中元素, 都是某个 $d$ 阶元之原根 (§55)

故 都存在, 且为 $\phi(d)$ 个.

Lemma 2.

H is a finite group of order n.

if $x^d = 1$ has at most d solutions in H for all $d \mid n$, then H is a cyclic.

Pf. (与 Gauss 证 p-1 存在原根的证明相同)

设 $d \mid n$，若 H 中 d 阶元素存在，那么有 $\phi(d)$ 个。

又 ∀ H 中元素，一定是某个阶元。

又 $n = |H| = \sum_{d \mid n} \phi(d)$ ∴ ∀ $d \mid n$，d 阶元皆有 $\phi(d)$ 个。

∴ 有 n 阶元有 $\phi(n)$ 个；故 $F^*$ is a cyclic.

theorem: $F_q^*$ is a cyclic

∵ $F_q$ 上，∀ 方程 $x^\theta = 1$，∀ $\theta \in N^*$，皆至多只有 θ 个解。于 $F_q^*$ 上亦然 #

---

志村的证明

~~Theorem: Every finitely genear generated abelian group~~ ~~设 F~~

Theorem: G is a ~~finitly~~ finite abelian group.

Then $G \cong \sum_{m \in M} \mathbb{Z}/m\mathbb{Z}$ M 为由正整数组成的有限集 (证明略)

Theorem: F is a finite field, then $F^*$ is cyclic.

pf. 由前，$F^* \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_2\mathbb{Z} \oplus \cdots \mathbb{Z}/m_k\mathbb{Z}$

若仅有 $\mathbb{Z}/m_1\mathbb{Z}$，得证。不然，下证 $(m_i, m_j) = 1$，$i \neq j$.

∵ 若 $(m_i, m_j) \neq 1$，则有 prime $p > 1$，$p \mid (m_i, m_j)$

∴ $\mathbb{Z}/m_i\mathbb{Z}$ 中 $0, \frac{m_i}{p}, \ldots, \frac{m_i}{p}(p-1)$

树仁書院 SHUREN COLLEGE

第一次讨论班
组号 12012612 [illegible]

$\mathbb{Z}/m_j\mathbb{Z}$ 中 $0, \frac{m_j}{p}, \dots, \frac{m_j}{p}(p-1)$ 皆满足 $x^p=0$

∴ 对 $(\frac{m_i}{p}\alpha, \frac{m_j}{p}\beta, 0, \dots, 0)$ 共有 $p^2$ 个组，满足 $x^p=0$. 对应到 $F^*$ 中，则 $x^p=1$ 有 $p^2$ 个解

而 $x^p=1$ 于 $F^*$ 中解等价于在 $F$ 中的解. 但在 $F$ 上其中最多只有 $p$ 个解. 矛盾.

插入一个引理.

对~~环~~ $R$，设 $I_1, I_2, \dots, I_n$ 为其理想，且

交换幺环 $I_i + I_j = R$, $i \neq j$.

则 $R/I_1I_2\cdots I_n \cong R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_n$

Pf.(不证)(归纳法) (chinese rimder theorem)

而对于互素的 $m_1, \dots, m_k$，显然

$m_i\mathbb{Z} + m_j\mathbb{Z} = \mathbb{Z}$, $i \neq j$

∴ $R/m_1\mathbb{Z} \oplus \cdots \oplus R/m_k\mathbb{Z} \cong R/(m_1\mathbb{Z})(m_2\mathbb{Z})\cdots(m_k\mathbb{Z})$

$= R/(m_1 \times \cdots \times m_k)\mathbb{Z}$

∴ $F^* \cong R/(m_1 \times \cdots \times m_k)\mathbb{Z}$ 故为 cyclic. #

~~Quard~~ Quadratic reciprocity low

① 介绍高斯的原始想法 (IV)

~~Serry~~ Serre 的证明.

① legendre symbol, other symbol

$p$, a prime, $p \neq 2$. $x \in F_p^*$.

then $\left(\frac{x}{p}\right) := x^{\frac{p-1}{2}}$

$$\varepsilon(n) \equiv \frac{n-1}{2} \ (2) \ \Rightarrow \begin{cases} 0 & n = 4k+1 \\ 1 & n = 4k+3 \end{cases}$$

$$w(n) = \frac{n^2-1}{8} \ (2) = \begin{cases} 0 & n = 8k \pm 1 \\ 1 & n = 8k \pm 5 \end{cases}$$

② some example

$\left(\frac{1}{p}\right) = 1$ $\quad \left(\frac{-1}{p}\right) = (-1)^{\varepsilon(p)}$ $\quad \left(\frac{2}{p}\right) = (-1)^{w(p)}$

pf: 只需证 $\left(\frac{2}{p}\right) = (-1)^{w(p)}$

一个事实: ~~对~~在 $F_p$ 的代数闭包 $\Omega$ 上, 对 $(l,p)=1$ 之 $l$, 总有 $\Omega$ 上元素 $x$, s.t. $x^l = 1$,

且 $x, \dots, x^l$ 两两不等.

pf: $\because (x^l - 1)' = l x^{l-1}$, 而显然 $(l x^{l-1}, x^l - 1) =$

$(\because (l,p)=1)$ 故 $x^l$ 有 $l$ 个解. (于 $\Omega$ 上)

易知其解关于"$\times$"构成群.

由之前的 lemma, 其为 cyclic 的 # 级 ~~数~~

---

~~设~~

现设 $\alpha$ 为 $F_p$ 的 $\Omega$ 上的 ~~8th root of~~ 8th primitive root of unity. denote $y = \alpha + \alpha^{-1}$

notice that $\alpha^4 = -1$, $\therefore (\alpha^2 + \alpha^{-2})^2 = 2\alpha^4 + 2 = 0$

$\therefore \alpha^2 + \alpha^{-2} = 0$ $\quad \therefore y^2 = \alpha^2 + \alpha^{-2} + 2 = 2$

& $y^p = \alpha^p + \alpha^{-p}$

$\therefore \left(\frac{2}{p}\right) = \left(\frac{y^2}{p}\right) = y^{p-1}$

当 $p \equiv \pm 1\ (8)$ 时, $y^p = \alpha + \alpha^{-1} = y$

$\therefore y(y^{p-1}-1)=0 \quad \therefore y^{p-1}=1 \quad \therefore \left(\frac{2}{p}\right)=1$

当 $p \equiv \pm 5\ (8)$ 时

$y^p = \alpha^5 + \alpha^{-5} \quad \because \alpha^4 = -1 \quad \therefore y^p = -\alpha - \alpha^{-1} = -y$

$\therefore y(y^{p-1}+1)=0 \quad \therefore y^{p-1} = -1 \quad \therefore \left(\frac{2}{p}\right) = -1$

---

Main theorem for this section.

if $l, p$ are two distinct prime numbers differen from 2, we ~~have~~ will have

$$\left(\frac{l}{p}\right) = \left(\frac{p}{l}\right)(-1)^{\varepsilon(l)\varepsilon(p)}$$

(当然, $l$ 为 prime)

② Gauss sum.

设 $\Omega$ 为 $F_p$ 的代数闭包, $w$ 为其上 $l$ 次元根 (存在性之后已证). $F_l = \mathbb{Z}/l\mathbb{Z}$.

则称 $\sum_{x \in l} \left(\frac{x}{l}\right) w^x$ 为 Gauss sum.

~~注: $x$ 对应在 $F_p$ 中的 $\underbrace{1+\cdots+1}_{x\text{个}}$ 当 $x=0$ 时 $\left(\frac{0}{p}\right)=0$~~

Lemma 1.

if $y = \sum_{x\in F_l^*} \left(\frac{x}{l}\right) w^x$

则 $y^2 = (-1)^{\varepsilon(l)} l$

Pf $y^2 = \left(\sum_{x_i\in F_l}\left(\frac{x_i}{l}\right)w^{x_i}\right)\left(\sum_{x_j\in F_l}\left(\frac{x_j}{l}\right)w^{x_j}\right)$

$= \sum_{x_i,x_j\in F_l}\left(\frac{x_i x_j}{l}\right)w^{x_i+x_j}$

$= \sum_{u\in F_l}\left(\underbrace{\sum_{t\in F_l}\left(\frac{t(u-t)}{l}\right)w^u}_{※}\right)$

※ ∵ $t=0$ 时, $\left(\frac{t(u-t)}{l}\right) = \left(\frac{0}{l}\right) = 0$

∴ ※ $= \sum_{t\in F_l^*}\left(\frac{t(u-t)}{l}\right)w^u = \sum_{t\in F_l^*}\left(\frac{-t^2}{l}\right)\left(\frac{1-ut^{-1}}{l}\right)w^u$

$= \sum_{t\in F_l^*}(-1)^{\varepsilon(l)}\left(\frac{1-ut^{-1}}{l}\right)w^u$

~~对~~ ~~对当~~ 当 $u=0$ 时, $(-1)^{\varepsilon(l)}\left(\frac{1}{l}\right)w^0 = (-1)^{\varepsilon(l)}$

∴ 此时 ※ $=(l-1)(-1)^{\varepsilon(l)}$

当 $u\neq 0$ 时, 当 $t$ 取遍 $F_l^*$ 时, $1-ut^{-1}$ 取遍 $F_l\setminus\{1\}$

∵ 对 $F_l^*$, $\sum_{\alpha\in F_l^*}\alpha = 0$

注: 设 $\beta$, 对 $\forall \beta\in F_l^*$, $\beta\neq 1$.

则 $\sum_{\alpha\in F_l^*}\alpha = \sum_{\alpha\in F_l^*}\beta\alpha$ ∴ $(\beta-1)\left(\sum_{\alpha\in F_l^*}\alpha\right)=0$

∴ $\sum_{\alpha\in F_l^*}(\alpha)=0$

∴ $\sum_{t\in F_l^*}\left(\frac{1-ut^{-1}}{l}\right) = 0-\left(\frac{1}{l}\right) = -1$

∴ ※ $= (-1)^{\varepsilon(l)+1}w^u$

树仁书院
SHUREN COLLEGE

第一次 讨论班
山阳男.

~~$\therefore y^2 = \sum_{u\in F_l} (-1)^{\varepsilon(l)+1} w^u = (-1)^{\varepsilon(l)+1} \sum_{u\in F_l^*} w^u + \sum_{t\in F_l} \left(\frac{-t^2}{l}\right)$~~

~~易知, $\sum_{t\in F_l} \left(\frac{-t^2}{l}\right) = 0$~~

~~$\therefore y^2 = (-1)^{\varepsilon(l)+1} \sum_{u\in F_l^*} w^u$~~

$\therefore y^2 = \sum_{u\in F_l^*} (-1)^{\varepsilon(l)+1} w^u + (l-1)(-1)^{\varepsilon(l)}$

而 $\sum_{u\in F_l^*} (-1)^{\varepsilon(l)+1} w^u = (-1)^{\varepsilon(l)}$

$\therefore y^2 = (-1)^{\varepsilon(l)} l$ #

---

Lemma 2. $y^{p-1} = \left(\frac{p}{l}\right)$

pf: $y^p = \left(\sum_{x\in F_l} \left(\frac{x}{l}\right) u^x\right)^p = \sum_{x\in F_l} \left(\frac{x}{l}\right) u^{xp}$ ($\because p$ is odd)

$= \sum_{z\in F_l} \left(\frac{zp^{-1}}{l}\right) u^z = \left(\frac{p^{-1}}{l}\right) \sum_{z\in F_l} \left(\frac{z}{l}\right) u^z = y\left(\frac{p^{-1}}{l}\right)$

$\therefore y^{p-1} = \left(\frac{p^{-1}}{l}\right) = \left(\frac{p}{l}\right)$

注: ① $y = \sum_{x\in F_l} \left(\frac{x}{l}\right) u^x$ 是 $F_p$ 的闭包 $\Omega$ 中之元素.

$\therefore$ 有 $(\alpha+\beta)^p = \alpha^p + \beta^p$.

② $\because 1 = \left(\frac{1}{l}\right) = \left(\frac{pp^{-1}}{l}\right) = \left(\frac{p}{l}\right)\left(\frac{p^{-1}}{l}\right)$

$\therefore \left(\frac{p}{l}\right) = \left(\frac{p^{-1}}{l}\right)$.

南方科技大学 P9

~~main th~~

Main theorem

$$\left(\frac{l}{p}\right) = (-1)^{\varepsilon(l)\varepsilon(p)}\left(\frac{p}{l}\right)$$

$\because \left(\frac{p}{l}\right)$ pf: $\left(\frac{y^2}{p}\right) = y^{p-1} = \left(\frac{p}{l}\right)$

而 $y^2 = (-1)^{\varepsilon(l)} l$

$\therefore \left(\frac{y^2}{p}\right) = \left(\frac{(-1)^{\varepsilon(l)}}{p}\right)\left(\frac{l}{p}\right) = \left(\frac{p}{l}\right)$

$\therefore \left(\frac{l}{p}\right) = \left(\frac{p}{l}\right)(-1)^{\varepsilon(l)\varepsilon(p)}$ #

---

志村与之相似的证明 $\boxed{(P_2)}$

① 一般形式的 Gauss sum

a. Dirichlet character

Def. $2 < r \in \mathbb{Z}$.

$$\chi : (\mathbb{Z}/r\mathbb{Z})^* \longmapsto T$$

is a Dirichlet character modulo $r$

if $\chi$ is a homorphism.

其中, $T = \{\alpha \in \mathbb{C} \mid |\alpha| = 1\}$

进一步的,为何要如此定义,有何背景? 可进一步探究

$\chi$ is primitive, if
① $\chi$ is nontrivial
② 对任意 $s$, $s \mid r$,
不存在 Dirichlet character
$\varphi$, s.t $\varphi(c) = \chi(c)$
for every $c$ prime to $r$

问题: 对任意 $r$, 是否皆存在 primitive Dirichlet character? 唯一性?

6. Gauss Sum

first, we denote $\exp(2\pi i z)$ by $e(z)$, $z\in\mathbb{C}$

$\therefore$ $e(\frac{1}{m})$ is m-th primitive root of unit

~~Define~~ let primitive Dirichlet character modulo r. $\chi$,

称 $\tau(\chi)=\sum_{a=1}^{r}\chi(a)e(\frac{a}{r})$

为 $\chi$ 的 Gauss Sum.

注: 此时将 $\chi$ 看为 $\mathbb{Z}\longmapsto T$ 的函数!

$$\chi=\begin{cases}\chi\ (c\ (\mathrm{mod}\ r)) & c \text{ is prime to } r\\ 0 & c \text{ is not prime to } r\end{cases}$$

Propoties.

① $\sum_{a=1}^{r}\chi(a)e(\frac{ab}{r})=\bar{\chi}(b)\tau(\chi)$, $\forall b\in\mathbb{Z}$.

pf: if $(b,c)=1$, then $\sum_{a=1}^{r}\chi(a)e(\frac{ab}{r})$

$=\sum_{c=1}^{r}\chi(cb^{-1})e(\frac{c}{r})$.

又 $\chi(1)=1=\chi(b)\chi(b^{-1})$ $\therefore \chi(b^{-1})=\bar{\chi}(b)$

$\therefore \sum_{a=1}^{r}\chi(a)e(\frac{ab}{r})=\bar{\chi}(b)\tau(\chi)$

(此时,与之前 $y^p=(\frac{p}{q})y$ 情况相同).

[illegible] 若 $(b,r)\neq 1$

设 $(b,r)=\delta$

记 $H=\{x\in \mathbb{Z}/r\mathbb{Z}^* \mid x\equiv 1\ (\frac{r}{\delta})\}$

则 $H$ 是 $\mathbb{Z}/r\mathbb{Z}^*$ 之子群

$\therefore$ 存 $Y$, s.t. $\mathbb{Z}/r\mathbb{Z}^* = \bigsqcup_{y\in Y} yH$

$$\therefore \sum_{a=1}^{r}\chi(a)e\left(\frac{ba}{r}\right)=\sum_{y\in Y}\sum_{h\in H}\chi(yh)e\left(\frac{yhb}{r}\right)$$

$\because h\equiv 1\ (\frac{r}{\delta})\quad \therefore bh\equiv b\ (r)$

$$\therefore \sum_{a=1}^{r}\chi(a)e\left(\frac{ba}{r}\right)=\sum_{y\in Y}\sum_{h\in H}\chi(yh)e\left(\frac{yb}{r}\right)$$

$$=\left(\sum_{y\in Y}\chi(y)e\left(\frac{yb}{r}\right)\right)\left(\sum_{h\in H}\chi(h)\right)$$

I claim: $\sum_{h\in H}\chi(h)=0$

lemma: $f: G\longmapsto \mathbb{C}^*$, $G$ is a finite group.

Then if $f$ is a nontrivial homorphism,

$$\sum_{g\in G} f(g)=0.$$

pf: $\because$ nontrival, suppose $g_0\in G$, s.t. $f(g_0)\neq 1$

$$\therefore \sum_{g\in G}f(g)=\sum_{g\in G}f(yg)=f(y)\left(\sum_{g\in G}f(g)\right)$$

$$\therefore (f(y)-1)\left(\sum_{g\in G}f(g)\right)=0 \quad \therefore \sum_{g\in G}f(g)=0$$

$$\therefore \sum_{a=1}^{r}\chi(a)e\left(\frac{ab}{r}\right)=0=\chi(b)\tau(\chi)$$

(mi#1)

P12

第一次作业 [illegible]

12012612 [illegible]

② $\tau(\chi)\tau(\overline{\chi}) = \chi(-1)r$

pf: $\tau(\chi)\tau(\overline{\chi}) = \tau(\chi)\left(\sum_{b=1}^{r}\overline{\chi}(b)e\left(\frac{b}{r}\right)\right)$

$= \sum_{b=1}^{r}\overline{\chi}(b)\tau(\chi)e\left(\frac{b}{r}\right)$

$= \sum_{b=1}^{r}\sum_{a=1}^{r}\chi(a)e\left(\frac{ab}{r}\right)e\left(\frac{b}{r}\right)$

$\cancel{= \left(\sum_{a=1}^{r}\chi(a)\right)} = \sum_{a=1}^{r}\chi(a)\sum_{b=1}^{r}e\left(\frac{ab}{r}\right)e\left(\frac{b}{r}\right)$

而后者 $\sum_{b=1}^{r}e\left(\frac{(a+1)b}{r}\right)$ 当 $a+1\neq 0$ 时，其值为0。

(∵ 为为循环群之和) 当 $a=-1$ 时，$\sum_{b=1}^{r}e\left(\frac{0}{r}\right)=r$

$\therefore \tau(\chi)\tau(\overline{\chi}) = \chi(-1)r$

③ $|\tau(\chi)|^2 = r$ ④ $\overline{\tau(\chi)} = \chi(-1)\tau(\overline{\chi})$

pf: 对于④

$\overline{\tau(\chi)} = \sum_{a=1}^{r}\overline{\chi(a)}e\left(-\frac{a}{r}\right) = \overline{\chi}(-1)\tau(\overline{\chi})$

$= \chi(-1)\tau(\overline{\chi})$

对于③ $|\tau(\chi)|^2 = \tau(\chi)\overline{\tau(\chi)} = \tau(\chi)\tau(\overline{\chi})\chi(-1)$

$= \chi(-1)r\chi(-1) = r$

( ∵ ~~$\chi(-1)=\pm 1$~~ ∵ $\chi(-1)\chi(-1) = \chi(1) = 1$ )

~~这 这是因为 $\chi(1)$~~ $=1$

P13

# quadratic reciplocity law

定义：$\left(\frac{q}{p}\right) := \begin{cases} 1 & q\,R\,p \\ -1 & q\,N\,R\,p \end{cases}$

为 $\mathbb{Z}/p\mathbb{Z} \longmapsto \{1,-1\}$ 的 homomorphism.

且 primitive. 记作 $\chi$.

---

~~Theorem: $\chi(p) = \chi(-1)^{\frac{p-1}{2}} \left(\frac{r}{p}\right)$~~

a ~~more~~ stronger theorem

then quadratic redprocity law.

Theorem: $\chi$ is a primitive character modulor $r$ s.t $\bar{\chi} = \chi$.

Then $\chi(p) = \chi(-1)^{\frac{p-1}{2}} \left(\frac{r}{p}\right)$, for odd ~~pf~~ Prime $p$ prime to $r$.

pf: $(\tau(\chi))^p = (\tau^2(\chi))^{\frac{p-1}{2}} \tau(\chi)$

$= (\chi(-1)\, r)^{\frac{p-1}{2}} \tau(\chi)$

$= (\chi(-1))^{\frac{p-1}{2}} r^{\frac{p-1}{2}} \tau(\chi)$

又 $(\tau(\chi))^p = \left(\sum_{a=1}^{r} \chi(a) e\left(\frac{a}{r}\right)\right)^p \equiv \sum_{a=1}^{r} \left(\chi(a) e\left(\frac{a}{r}\right)\right)^p \ (pR)$

$= \sum_{a=1}^{r} \chi(a) e\left(\frac{ap}{r}\right)$

$= \chi(p)\, \tau(\chi)$

where $R = \mathbb{Z}[\zeta]$

$\therefore \chi(p)\tau(\chi) \equiv (\chi(-1))^{\frac{p-1}{2}} r^{\frac{p-1}{2}} \tau(\chi) \quad (pR)$

$\therefore \tau(\chi)\left(\chi(p) - \chi(-1)^{\frac{p-1}{2}} r^{\frac{p-1}{2}}\right) \equiv 0 \quad (pR)$

又 $\because |\tau(\chi)| = r$ $\therefore$ ~~$\tau(\chi) \not\equiv 0 \ (pR)$~~

$\therefore$ 又 $(r,p)=1$

$\therefore \chi(p) \equiv \chi(-1)^{\frac{p-1}{2}} r^{\frac{p-1}{2}} \quad (pR)$

$\therefore \underbrace{\chi(p)}_{\alpha} \equiv \underbrace{\chi(-1)^{\frac{p-1}{2}} r^{\frac{p-1}{2}}}_{\beta} \quad (pZ)$

又 ~~$\alpha - \beta$~~ $\therefore \left(\frac{r}{p}\right) = \chi(p)\,\chi(-1)^{\frac{1-p}{2}}$

$\therefore \chi(p) = \chi(-1)^{\frac{p-1}{2}} \left(\frac{r}{p}\right)$ #

对 $q$ 为 prime 时, 令 $\chi : a \in \mathbb{Z}/q\mathbb{Z} \longmapsto \left(\frac{a}{q}\right)$

$\therefore$ 有 $\left(\frac{p}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \left(\frac{q}{p}\right)$

$= (-1)^{\frac{q-1}{2}\frac{p-1}{2}} \left(\frac{q}{p}\right)$ #

$=$

Serre 之证明

与志村证明的比较.

① $y=\sum_{x\in G_l}\left(\frac{x}{l}\right)w^{x} \iff \tau(\chi)=\sum_{a=1}^{l}\chi(a)e\left(\frac{a}{l}\right)$

② $y^{2}=(-1)^{\varepsilon(l)}l \iff \tau(\chi)\tau(\bar{\chi})=\chi(-1)r$

③ $y^{p-1}=\left(\frac{p}{l}\right) \iff (\tau(\chi))^{p}\equiv\chi(p)\tau(\chi)\ (pR)$

志村给出的 τ 的 4 个性质

$\sum_{a=1}^{r}\chi(a)e\left(\frac{ab}{r}\right)=\bar{\chi}(b)\tau(\chi)$ ①

$\tau(\chi)\tau(\bar{\chi})=\chi(-1)r$ ②

$|\tau(\chi)|^{2}=r$ ③

$\overline{\tau(\chi)}=\chi(-1)\tau(\bar{\chi})$ ④

③，④ 实际上在证明 Strong theorem 时没用到（可以不证）

而①在 r 为素数时很平凡，从而②亦容易得到，~~互相~~, in fact，在此时两者基本相同.

志村证明是抽象，推广了的 Serre 的证明.

树仁書院 SHUREN COLLEGE

附录

Appendix.（∵已忘掉）

§2. equation over a finite field

（设 $q=p^f$，$p$为 odd prime）

2.1 lemma

$u\in N$, $\sum_{x\in k} x^u = \begin{cases} -1 & \text{if } q-1 \mid u,\ u\neq 0 \\ 0 & \text{otherwise} \end{cases}$

（$k$为 $q=p^f$ 的域）

pf: 当 $q-1\mid u$，$u\neq 0$时

$\sum_{x\in k} x^u = \sum_{x\in k} 1 = p^f = 0$

当 $q-1\nmid u$ 时，$u\neq 0$时

$\sum_{x\in k} x^u = 0^u + \sum_{\alpha=1}^{q-1} \theta^{\alpha u}$，$\theta$为 $F_q^*$ 的元根.

$= \sum_{\alpha=1}^{q-1} \theta^{\alpha u}$

设 $\theta^u$ 为 $s$ 阶元，$s\mid q-1$

$\therefore \theta^1+\dots+\theta^s=0 \quad \therefore \sum_{\alpha=1}^{q-1}\theta^{\alpha u}=0$

$\therefore \sum_{x\in k} x^u = 0$

当 $u=0$时，$\sum_{x\in k} x^u = p^f = 0$

$\therefore 0$

南方科技大学

Theorem

Chevaley − Warning

$f_\alpha \in k[x_1 \cdots x_n]$

为 n 元多项式.　(k 为 $q=p^f$ 个元素域)

当 $\sum_\alpha \deg f_\alpha < n$ 时

Denote the common zeros of them by $V$.

Then, $\#(V) \equiv 0 \ (p)$

Pf: Consider the function

$G = \prod_\alpha (1 - f_\alpha^{q-1})$

Then $\forall x \in V$, $G(x) = 1$　$x \notin V$,

则 some $f_\alpha(x) \neq 0$　$\therefore (f_\alpha(x))^{q-1} = 1$

$\therefore G(x) = 1$

$\therefore \#(V) \equiv \sum_{x \in K^n} G(x) \ (p)$

($\because G(x) \in K$, 故只能模 p 后相等)

I 的 ~~caim~~ claim: $\sum_{x \in K^n} G(x) = 0$

$\because G(x)$ ~~开方~~ 的非常数项为 $x_1^{y_1} x_2^{y_2} \cdots x_n^{y_n}$ 的

初始. 又 $\because \sum_\alpha \deg f_\alpha < n$　$\therefore 0 < y_1 + \cdots + y_n < n(q-1)$

$\therefore \exists\, y_i$, s.t. $0 < y_i < q-1$

$\therefore \sum_{x \in K^n} (x_1^{y_1} \cdots x_n^{y_n})(x_i^{y_i}) = \left(\sum_{x \in K^{n-1}} (x_1^{y_1} \cdots x_n^{y_n})\right)\left(\sum_{x \in K} x_i^{y_i}\right)$

由前, $\sum_{x \in K} x_i^{y_i} = 0$ 且常数项总和为 $K^n = 0$

$\therefore \sum_{x \in K^n} G(x) = 0$

忠宏尾

~~Corollary~~

Example: ~~$x_1 - 1$ $x_2 - 2$~~ $f_1 = x_1 - 1$ $f_2 = x_2 - 2$

对 $k[x_1, x_2, x_3]$,

~~则~~ $V(f_1, f_2) = P \equiv 0 \cdot (P)$

Corollary:

If $\sum_\alpha \deg f_\alpha < n$, $f_\alpha$ 常数项 皆为0

则 $f_\alpha$ have nontirvaial comme zero.

pf: 显然。

Corollary:

All quadratic from in at least 3 variables over $k$

have a non trival zero.

$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \begin{pmatrix} a & b & c \\ b & e & d \\ c & d & f \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ 在 $k$ 上 有非平凡解.

(every conic over a finite field has a rational point)

总结，演讲计划

与问题.

① 模形式介绍.

问题：双曲平面的划分.

Cauchy conformal map 而是. $H \longmapsto H$ 的变换类群

为 $\frac{az+b}{cz+d}$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$

② 二次互反律

上节的部分讲结束!

主讲两个不同的证明

③ Chevalley — Warning theorem.