LECTURE NOTES ON NUMBER THEORY

RUNLIN ZHANG

Abstract. This is a course note wrote for a course taught in 2025SP, 2025AU. It mainly follows Cox's book, Primes of the form $x^2 + ny^2$, chapter 1 to 6 and Ireland–Rosen's GTM 84 book.

Contents

1. Congruence relation

1.1. Divisors.

- Let a, b be two integers. We say that a **divides** b iff $b = a \cdot q$ for some integer q, written as $a \mid b$. Integers that divide a given integer b are called **divisors** of b. Whether a divides b or not, if a is nonzero, one can always find $q, r \in \mathbb{Z}$, $0 \leq r \leq |a| - 1$ such that $b = aq + r$. This is called division with remainders.
- Certain unusual cases:

$$\begin{aligned} a = 1: &\quad 1 \text{ divides every integer} \\ a = 0: &\quad 0 \text{ only divides } 0 \\ b = 0: &\quad \text{every integer divides } 0 \end{aligned}$$

- A positive integer p is called a **prime number** iff $p > 1$ and the only divisors of p are $\{1, p\}$.
- An induction argument shows that every positive integer (other than 1) can be written as a product of prime numbers (possibly with multiplicities), e.g.

$$60 = 2^2 \cdot 3 \cdot 5.$$

Exercise 1.1. *Prove the uniqueness of prime decomposition of a positive integer. Precisely, let $N > 1$ be a positive integer and assume*

- *$(p_1, ..., p_l)$, $(q_1, ..., q_m)$ are two sets of pairwise different prime numbers (that is, $p_i \neq p_i$ and $q_i \neq q_j$ if $i \neq j$);*
- *$(r_1, ..., r_l)$, $(s_1, ..., s_m)$ are two sets of positive integers;*
- $$N = \prod_{i=1}^{l} p_i^{r_i} = \prod_{j=1}^{m} q_j^{s_j}.$$

Show that there is a bijection $\sigma : \{1, ..., l\} \to \{1, ..., m\}$ such that $q_{\sigma(i)} = p_i$, $s_{\sigma(i)} = s_i$ for all $i = 1, ..., l$.

- Given two positive integers a, b, the **greatest common divisor** of a, b, denoted as $\gcd(a, b)$, is

$$\gcd(a, b) = \max \left\{ d \in \mathbb{Z}^+ \;\middle|\; d \mid a,\ d \mid a \right\}.$$

  a, b are said to be **coprime** iff $\gcd(a, b) = 1$.
- There is an **algorithm** that finds this g.c.d. It is simply by applying division with remainders repeatedly until there is no remainder. We assume $a > b > 0$. The claim is that there is some $k \in \mathbb{Z}_{\geq 0}$ and integers $q_1, ..., q_{k+1}$, $r_1, ..., r_k$ satisfying

$0 < r_k < r_{k-1} < ... < r_1 < r_0 := a < r_{-1} := b$ and

$$\begin{aligned} b &= a \cdot q_1 + r_1 \\ a &= r_1 \cdot q_2 + r_2 \\ r_1 &= r_2 \cdot q_3 + r_3 \\ &... \\ r_{k-3} &= r_{k-2} \cdot q_{k-1} + r_{k-1} \\ r_{k-2} &= r_{k-1} \cdot q_k + r_k \\ r_{k-1} &= r_k \cdot q_{k+1} \end{aligned} \tag{1}$$

Clearly, $k < a$.

- By Eq.(1), we find that
$$\gcd(a, b) = \gcd(r_1, b) = \gcd(r_1, r_2) = ... = \gcd(r_{k-1}, r_k) = r_k.$$
- By Eq.(1) again, we have
$$\begin{aligned} r_k &= r_{k-2} - q_k \cdot r_{k-1} \\ &= r_{k-2} - q_k(r_{k-3} - r_{k-2}q_{k-1}) \\ &= -q_k \cdot r_{k-3} + (1 + q_k q_{k-1}) \cdot r_{k-2} \\ &... \end{aligned}$$
The conclusion is that
$$\gcd(a, b) = r_k = \alpha \cdot a + \beta \cdot b$$
for some integers α, β, which can be explicitly found by the above process.

Exercise 1.2. *Show that*

$$\frac{b}{a} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + ... + \cfrac{1}{q_{k+1}}}}.$$

There is a unsolved conjecture related to this, which asserts that there exists $M > 0$ such that for all positive integer a, one can find $b \in \mathbb{Z}^+$ coprime to a such that $k+1 \leq M$.

Lemma 1.1. *Let a, b be two positive integers, then*

$$\gcd(a, b) = \inf \{d > 0 \mid d \in \mathbb{Z}.a + \mathbb{Z}.b\}.$$

In particular

$$\gcd(a, b) = 1 \iff \lambda a + \mu b = 1,\ \exists\, \lambda, \mu \in \mathbb{Z}.$$

Exercise 1.3. *Let (m, n) be a pair of coprime positive integers. Show that there exists $N_0 > 0$ such that for every integer $N \geq N_0$, there exist two **positive** integers α, β such that $N = \alpha m + \beta n$. Can you find the smallest such N_0?*

1.2. **Congruence.** Let us fix some nonzero integer N.

- Two integers a, b are said to be **congruent modulo N** iff $N \mid a - b$, denoted as $a \equiv b \pmod N$ or $a \equiv b\ (N)$.
- Being congruent modulo N defines an **equivalence relation**, namely,
  (1) $a \equiv b \pmod N \iff b \equiv a \pmod N$;
  (2) $a \equiv b \pmod N$, $b \equiv c \pmod N$ imply $a \equiv c \pmod N$;
  (3) $a \equiv a \pmod N$.
- The set of modulo N equivalence classes $\{a + N\mathbb{Z}\}$ is denoted as $\mathbb{Z}/N\mathbb{Z}$. The equivalence class containing a given integer a is denoted as $[a]_N$ or $[a]$ if it clear from the context what N is. Explicitly,
$$\mathbb{Z}/N\mathbb{Z} = \{[0]_N, [1]_N, [2]_N, ..., [N-1]_N\}.$$
- $\mathbb{Z}/N\mathbb{Z}$ has a (unital, commutative) **ring** structure such that the natural map $\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ is a ring homomorphism:
  (1) $[a] + [b] := [a + b]$, $[a] \cdot [b] := [a \cdot b]$;
  (2) $[0]$ is the zero element, $[1]$ is the multiplicative identity.
  (3) Associativity can be verified.

- If $M \mid N$, then there is a natural map $\mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/M\mathbb{Z}$ such that

$$\begin{array}{ccc} \mathbb{Z} & & \\ \downarrow & \searrow & \\ \mathbb{Z}/N\mathbb{Z} & \longrightarrow & \mathbb{Z}/M\mathbb{Z} \end{array}$$

  is a commutative diagram of ring homomorphisms.

1.3. **Chinese remainder theorem.**

Lemma 1.2. *For a pair of coprime integers $M, N \in \mathbb{Z}$, the natural map $\mathbb{Z}/MN\mathbb{Z} \to \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ is an isomorphism.*

- Let us prove this. Since this is a ring homomorphism, it suffices to show 1. injectivity; 2. the domain and target have the same cardinality.
- 2. is rather direct. To prove 1., let us take $a \in \mathbb{Z}$ such that $a \equiv 0\ (M)$ and $a \equiv 0\ (N)$. We need to show $a \equiv 0\ (MN)$, which is true since $\gcd(M, N) = 1$.
- Of course, we can prove surjectivity directly. That is to say, given $[a]_M$ and $[b]_N$, we will construct some $c \in \mathbb{Z}$ such that

$$c \equiv a \pmod{M}, \quad c \equiv b \pmod{N}.$$

  Since $[a]_M = [a + xM]_M$ for any integer x, we hope to find $x \in \mathbb{Z}$ such that $[a + xM]_N = [b]_N$ or equivalently,

$$xM \equiv b - a \pmod{N}.$$

  By previous lemma, $\gcd(M, N) = 1$ implies that $\alpha M + \beta N = 1$ for some integers α, β. By modulo N, we have

$$\alpha M \equiv 1 \pmod{N}$$

  That is α is the inverse of M modulo N. So x is uniquely solved as $[(b-a)\alpha]_N$. That is, $c := a + (b-a)\alpha M$ satisfies the requirement.

Applying the above lemma several times we obtain

Theorem 1.3. *Let $N_1, ..., N_l$ be finitely many pairwise coprime nonzero integers. Then the natural map $\mathbb{Z}/N_1 \cdot ... \cdot N_l\mathbb{Z} \to \mathbb{Z}/N_1\mathbb{Z} \times ... \times \mathbb{Z}/N_l\mathbb{Z}$ is an isomorphism.*

Note that pairwise coprime implies $\gcd(N_i, \prod_{j \neq i} N_j) = 1$ for every i.

Corollary 1.4. *Assume $N = p_1^{r_1} \cdot p_2^{r_2} \cdot ... \cdot p_l^{r_l}$ for some distinct prime numbers $p_1, ..., p_l$ and positive integers $r_1, ..., r_l$. Then*

$$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times ... \times \mathbb{Z}/p_l^{r_l}\mathbb{Z}.$$

1.4. **Units, its cardinality.** Let N be some fixed nonzero integer.

- $[u] \in \mathbb{Z}/N\mathbb{Z}$ is called a **unit** iff there exists some other $[u^*] \in \mathbb{Z}/N\mathbb{Z}$ such that $[u][u^*] = [1]$. The subset of units is denoted by $(\mathbb{Z}/N\mathbb{Z})^\times$ or $\mathrm{U}(\mathbb{Z}/N\mathbb{Z})$.
- By unwrapping the definition, for an integer u, $[u] \in \mathbb{Z}/N\mathbb{Z}$ is a unit iff there are integers u^* and λ such that

$$u^*u + \lambda N = 1$$

  or in other words, $\gcd(u, N) = 1$.
- By Chinese remainder theorem, if $N = p_1^{r_1}p_2^{r_2}...p_l^{r_l}$,

$$\mathrm{U}(\mathbb{Z}/N\mathbb{Z}) \cong \mathrm{U}(\mathbb{Z}/p_1^{r_1}\mathbb{Z}) \times ... \times \mathrm{U}(\mathbb{Z}/p_l^{r_l}\mathbb{Z}).$$

- We let $\phi(N) := |\mathrm{U}(\mathbb{Z}/N\mathbb{Z})|$, called the **Euler's totient function**. So $\phi(N) = \prod_{i=1}^{l} \phi(p_i^{r_i})$. Then

$$\begin{aligned} \phi(p^r) &= \#\{a = 0, ..., p^r - 1 \mid a \text{ is coprime to } p\} \\ &= \#\left(\mathbb{Z}/p^r\mathbb{Z} \setminus \{0, p, 2p, ..., (p^{r-1} - 1)p\}\right) \\ &= p^r - p^{r-1} = p^r(1 - \frac{1}{p}) \end{aligned}$$

$$\implies \frac{\phi(N)}{N} = \prod_{i=1}^{l}(1 - \frac{1}{p_i}).$$

Now we turn to the group structure of $\mathrm{U}(\mathbb{Z}/N\mathbb{Z})$. By definition,

$$a^{\phi(N)} \equiv 1 \pmod{N} \quad \forall\, a \in \mathbb{Z},\ \gcd(a, N) = 1.$$

But is $\phi(N)$ the smallest number with this property? By CRT, it suffices to understand that of $\mathrm{U}(\mathbb{Z}/p^r\mathbb{Z})$, which we explain in the next two sections. Roughly speaking when $p \neq 2$, it is cyclic and when $p = 2$, it is the product of $\{\pm 1\}$ and a cyclic group. In particular, if $N = p$ is prime, then $\phi(p)$ is indeed the smallest number with the above property.

1.5. **Unit group of $\mathbb{Z}/p\mathbb{Z}$.** We start by showing that $\mathrm{U}(\mathbb{Z}/p\mathbb{Z})$ is cyclic for a prime number p. Indeed, noting that $\mathbb{Z}/p\mathbb{Z}$ is a **field**, we can do it in a slightly more general manner.

Lemma 1.5. *Let $\mathbb{F}_q$ be a finite field consisting of q elements. Then $\mathbb{F}_q^\times$ is a cyclic group of order $q-1$.*

Lemma 1.6. *Let A be a finite abelian group. If A is **not** cyclic, then there exists a positive integer $n \mid |A|$ but $n \neq |A|$ such that $a^n = 1$ for all $a \in A$.*

Proof of Lemma 1.5 assuming Lemma 1.6. If $\mathbb{F}_q^\times$ were not cyclic, we would find $m \mid q-1$, $m \neq q-1$ such that

$$x^m = 1 \quad \forall\, x \in \mathbb{F}_q^\times.$$

On the other hand, a polynomial of degree m can have at most m distinct roots in any field. So

$$\left|\{x \in \mathbb{F}_q^\times : x^m = 1\}\right| \leq m < q-1.$$

This contradicts against the fact that $\mathbb{F}_q^\times$ has exactly $q-1$ elements. Therefore, $\mathbb{F}_q^\times$ must be cyclic. □

Exercise 1.4. *Prove the assertion that a polynomial of degree m can have at most m distinct roots in any field.*

We have used the fundamental theorem of finite abelian group through Lemma 1.6.

Theorem 1.7. *Every finite abelian group A is isomorphic to a direct product of cyclic groups $A \cong C_1 \times ... \times C_k$.*

Here is a proof bypassing the above theorem (from Serre's book: a course in arithmetic):

Proof of Lemma 1.6. It suffices to show that if an abelian group A has the property that

- $\#\{a \in A \mid a^n = 1\} \leq n$ for all $n \mid |A|$

then A is cyclic. For a divisor d of N, let $A[d] := \{x \in A,\ x^d = 1\}$ and $A[d]^{\mathrm{prim}}$ be the smaller subset collect all elements with order d. Then

$$|A| = \sum_{d \mid |A|} \left|A[d]^{\mathrm{prim}}\right|. \tag{2}$$

We view $\left(\left|A[d]^{\mathrm{prim}}\right|\right)$ as an important invariant of finite groups. Letting $N := |A|$, we will compare the invariant of A and $\mathbb{Z}/N\mathbb{Z}$.

Let $q := N/d$. Then

$$(\mathbb{Z}/N\mathbb{Z})[d] = \{[0], [q], [2q], ..., [(d-1)q]\} = q\mathbb{Z}/|A|\mathbb{Z} \cong \mathbb{Z}/d\mathbb{Z}$$

and

$$(\mathbb{Z}/N\mathbb{Z})[d]^{\mathrm{prim}} = \{[aq],\ \gcd(a, d) = 1\} \cong \mathrm{U}(\mathbb{Z}/d\mathbb{Z}).$$

In particular,

$$\left|(\mathbb{Z}/N\mathbb{Z})[d]^{\mathrm{prim}}\right| = \phi(d).$$

Now we turn to A. Suppose that $A[d]^{\mathrm{prim}}$ is non-empty and we pick some $a \in A[d]^{\mathrm{prim}}$. Then the subgroup generated by a

$$C_a := \langle a \rangle = \{1, a, a^2, ..., a^{d-1}\},$$

is a cyclic subgroup of order d. Note that every element x in C_a satisfies $x^d = 1$. Since there can be at most d-many such x's, this shows that

$$x \in A,\ x^d = 1 \implies x \in C_a$$

Thus

$$A[d]^{\mathrm{prim}} = C_a[d]^{\mathrm{prim}} \implies \left|A[d]^{\mathrm{prim}}\right| = \phi(d).$$

In conclusion $\left|A[d]^{\mathrm{prim}}\right| \leq \phi(d) = \left|(\mathbb{Z}/N\mathbb{Z})[d]^{\mathrm{prim}}\right|$ for each divisor d of N. But

$$\sum_{d|N} \left|A[d]^{\mathrm{prim}}\right| = N = \sum_{d|N} \phi(d),$$

so we must have $A[d]^{\mathrm{prim}} = \phi(d)$ for all divisors d. In particular, $A[N]^{\mathrm{prim}} \neq \emptyset$, showing that A is cyclic.

□

1.6. **Fundamental theorem of finite abelian groups.** Though it is not necessary, we sketch a proof of Theorem 1.7 for the reader's convenience.

Definition 1.8. *If G is a group and $g \in G$, we let the* ***order of*** *g be* $\mathrm{ord}(g) := \min\{n \in \mathbb{Z}^+ \mid g^n = 1\}$ *if such an n exists, otherwise let* $\mathrm{ord}(g) := +\infty$. *We let $\langle g \rangle$ be the subgroup generated by g. Thus,* $\mathrm{ord}(g)$ *is the size of $\langle g \rangle$.*

Lemma 1.9. *Let G be a finite group and $g \in G$. Let n be a positive integer. Then*

(1) $\mathrm{ord}(g) \,\big|\, \#G$;

(2) $\mathrm{ord}(g^n) = \dfrac{\mathrm{ord}(g)}{\gcd(n, \mathrm{ord}(g))}$.

Proof. The first follows from the fact that if $H \leq G$ is a subgroup, then $\#H \,\big|\, \#G$.

For (2) there are two special cases. One is when n is coprime to $\mathrm{ord}(g)$ and another is when n divides $\mathrm{ord}(g)$. The general case is a combination of these two.

Let $m := \mathrm{ord}(g)$ and $m' := m/\gcd(m,n)$, $n' := n/\gcd(m,n)$. So $\gcd(n', m) = 1$. We claim that $\mathrm{ord}(g^{n'}) = \mathrm{ord}(g)$, that is, $g^{n'}$ also generates $\langle g \rangle$. Indeed, by Euclidean algorithm, we find $\alpha, \beta \in \mathbb{Z}$ such that $\alpha n' + \beta m = 1$. Then

$$g = g^{\alpha n' + \beta m} = (g^{n'})^{\alpha}$$

showing that $\langle g \rangle = \langle g^{n'} \rangle$ and also $\mathrm{ord}(g^{n'}) = \mathrm{ord}(g) = n$. Let $g_1 := g^{n'}$.

$$(g^n)^{n'} = (g_1^{\gcd(m,n)})^{n'} = g^n = 1, \text{ which implies } \mathrm{ord}(g^n) \mid n'.$$

On the other hand take a positive integer $l \mid m'$ such that $\left(g_1^{\gcd(m,n)}\right)^l = 1$. Then $n \mid l \cdot \gcd(m,n)$ showing that $l \geq n'$. In sum, we have $\mathrm{ord}(g) = n'$. □

It suffices to show that A is isomorphic to a product of cyclic groups. Using CRT, one can then arrange that $\#C_{i+1} \mid \#C_i$.

Step 1, A is a product of cyclic groups if $|A| = p^r$.

We prove this by induction. So assume that if $|A'| = p^{r'}$ with $r' < r$ and A' an abelian group, then A' is a product of cyclic groups.

Take an $a_0 \in A_p$ such that $\mathrm{ord}(a_0)$ attains $p^{r_0} := \max\{\mathrm{ord}(a),\ a \in A_p\}$. Let $\pi : A \to A/\langle a_0 \rangle =: B$ be the quotient homomorphism. By assumption B is a product of cyclic groups $C_1 \times C_2 \times ... \times C_k$. Let x_i be a generator of C_i.

We **claim** that any element $x \in A_p/\langle a_0 \rangle$, say of order p^s, can be lifted to $a_x \in A$ (that is, $a_x \in \pi^{-1}(x)$) of the same order.

Proof of claim. We choose some arbitrary $a_1 \in \pi^{-1}(x)$ first. In general we only know that $p^s \mid \mathrm{ord}(a_1)$. We hope to find n such that p^s is equal to $\mathrm{ord}(a_1 a_0^n)$. Or equivalently

$$a_1^{p^s} a_0^{p^s n} = 1. \tag{3}$$

Setting $a_x := a_1 a_0^n$ would then complete the claim.

Since $\pi(a_1^{p^s}) = x^{p^s} = 1$, we can find $t \in \mathbb{Z}_{\geq 0}$ and $l \in \mathbb{Z}^+$ coprime to p such that $p^t \cdot l \in \{0, ..., p^{r_0} - 1\}$ and

$$a_1^{p^s} = a_0^{p^t \cdot l}$$

We will search n of the form $n' \cdot l$. So we want

$$a_0^{p^t \cdot l} a_0^{p^s l n'} = a_0^{l(p^t + p^s n')} = 1. \tag{4}$$

A natural choice of n' would be $n' := \dfrac{p^{r_0} - p^t}{p^s} = p^{r_0 - s} - p^{t-s}$. But to ensure n' is an integer, we need to show $s \leq r_0$ and $s \leq t$ (since $t \leq r_0$, suffices to prove the latter).

Indeed, by the maximality of $\mathrm{ord}(a_0)$,

$$p^{r_0} \geq \mathrm{ord}(a_1) = \mathrm{ord}(a_1^{p^s}) \cdot p^s = \mathrm{ord}(a_0^{p^t l}) \cdot p^s = p^{r_0 - t + s} \implies t \geq s.$$

This proves the lemma. □

Going back to step one, let $a_1, ..., a_k$ be the lifts of $x_1, ..., x_k$ provided by this lemma. Then, sending x_i to a_i gives a well-defined injective homomorphism from C_i to A. Let $\varphi : C_1 \times ... \times C_l \times \langle a_0 \rangle \to A$ be the product of these homomorphisms. We show φ is an isomorphism.

Stare at the following commutative diagram

$$\begin{array}{ccc} C_1 \times ... \times C_l \times \langle a_0 \rangle & \xrightarrow{\varphi} & A \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi} \\ C_1 \times ... \times C_l & \xrightarrow{\cong} & A/\langle a_0 \rangle \end{array}$$

where the bottom arrow is an isomorphism and π_1 is the natural surjective projection. It is direct for one to check that φ is indeed surjective and injective.

Step 2, the general case.

Let $\#A = N = p_1^{d_1} \cdot p_2^{d_2} \cdot ... \cdot p_k^{d_k}$ be the prime decomposition of $\#A$. Let $A_{p_i} := \{a \in A \mid a^{p_i^{d_i}} = 1\}$. We claim that $A \cong A_{p_1} \times ... \times A_{p_k}$. T

There is a natural homomorphism $\varphi : \prod A_{p_i} \to A$ sending (a_i) to $a_1 \cdot a_2 \cdot ... \cdot a_k$.

(1) φ is injective: If $\prod a_i = 1$ with $a_i \in A_{p_i}$ and $c_j := \frac{N}{p_j^{d_j}}$, then c_j is divisible by the order of a_i for all $i \neq j$ but is coprime to the order of a_j. So

$$1 = (\prod a_i)^{c_j} = \prod a_i^{c_j} = a_j^{c_j} \implies a_j = 1.$$

(2) φ is surjective: Take $a \in A$ and assume $\mathrm{ord}(a) = \prod_{i=1}^k p_i^{e_i}$. Define $c_j := \prod_{i \neq j} p_i^{e_i}$. Then $a_j := a^{c_j} \in A_{p_j}$ by definition. Since $\gcd(c_1, \ldots, c_k) = 1$, we can find $(\alpha_i)_{i=1}^k$ integers such that $\sum c_i \alpha_i = 1$. Hence $a = \varphi\left(\oplus a_j^{\alpha_j}\right)$, so we have shown surjectivity.

It remains to observe that $\#A_{p_i} = p_i^d$ for some d (then it will be forced that $d = d_i$). Indeed, if not, we can find a chain of (normal) cyclic subgroups (C_j)

$$C_1 \leq A_1 := A_{p_i},\ C_2 \leq A_2 := A/C_1,\ C_3 \leq A_3 := A_2/C_2, ..., C_{l+1} = A_l/C_l.$$

Then $\#A_{p_i} = \prod \#C_k$. If $\#A_{p_i}$ has some prime factor $q \neq p_i$ then at least one of $\#C_j$ has a prime factor q. By lifting the generator of C_j to A_{p_i}, one get an element whose order has a factor q, which is a contradiction.

Now the general case has been reduced to the situation in step one and we are done.

1.7. **Unit group of $\mathbb{Z}/p^r\mathbb{Z}$.**

Lemma 1.10. *Let p be an odd prime and $r \in \mathbb{Z}^+$. Then as a group $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is isomorphic to $\mathbb{Z}/p^{r-1}\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^\times$.*

Proof. Note that the set $1 + p\mathbb{Z}$ is (saturated) a union of modulo-p^r equivalence classes. And we let $1 + p\mathbb{Z}/p^r\mathbb{Z}$ denote these equivalence classes, a subset of $\mathbb{Z}/p^r\mathbb{Z}$. Concretely, each element in $1 + p\mathbb{Z}/p^r\mathbb{Z}$ takes the form $1 + p\lambda + p^r\mathbb{Z}$ for some integer λ and two such sets $1 + p\lambda_i + p^r\mathbb{Z}$ $(i = 1, 2)$ are the same iff $\lambda_1 \equiv \lambda_2 \pmod{p^{r-1}}$. Then one finds that this subset is multiplicatively closed and every element admits an inverse, which is still in this subset. In sum, $1 + p\mathbb{Z}/p^r\mathbb{Z} \subset (\mathbb{Z}/p^r\mathbb{Z})^\times$ is a subgroup.

There is a natural exact sequence

$$1 \longrightarrow 1 + p\mathbb{Z}/p^r\mathbb{Z} \longrightarrow (\mathbb{Z}/p^r\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow 1.$$

Since $|(1 + p\mathbb{Z}/p^r\mathbb{Z})| = p^{r-1}$, which is coprime to $p - 1$, we know by structure theorem of abelian group (or see the lemma below) that

$$(\mathbb{Z}/p^r\mathbb{Z})^\times \approx (1 + p\mathbb{Z}/p^r\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})^\times.$$

Next we show that $[1 + p]_{p^r}$ is an element of order p^{r-1} and hence a generator, making $1+p\mathbb{Z}/p^r\mathbb{Z}$ a cyclic group of order p^{r-1}. This follows from the elementary fact that raising to p-th power maps (for each $k \in \mathbb{Z}^+$) induces a map

$$\begin{aligned} 1 + p^k\mathbb{Z} \setminus 1 + p^{k+1}\mathbb{Z} &\to 1 + p^{k+1}\mathbb{Z} \setminus 1 + p^{k+2}\mathbb{Z} \\ x &\mapsto x^p. \end{aligned} \tag{5}$$

Indeed, for λ coprime to p,

$$(1 + \lambda p^k)^p \in 1 + \lambda p^{k+1} + p^{k+2}\mathbb{Z}.$$

From Eq.(5), we conclude that $(1 + p)^{p^\star} \notin p^r\mathbb{Z}$ if $\star < r - 1$ and $(1 + p)^{p^{r-1}} \in p^r\mathbb{Z}$. This shows that $\mathrm{ord}([1 + p]_{p^r}) = p^{r-1}$ and hence $[1 + p]$ generates $1 + p\mathbb{Z}/p^r\mathbb{Z}$. □

Lemma 1.11. *Assume that m, n is a pair of coprime positive integers and A is a finite abelian group with cardinality mn. Write $A[d] := \{a \in A,\ a^d = 1\}$, which is a subgroup, for an integer d. Then the natural map $A[m] \times A[n] \to A$ is an isomorphism. Moreover, $|A[m]| = m$ and $|A[n]| = n$.*

Proof. By assumption find $\alpha, \beta \in \mathbb{Z}$ with $\alpha m + \beta n = 1$.

Injectivity.

It suffices to show that $A[m] \cap A[n] = \{1\}$. Take $b \in A[m] \cap A[n]$, then $b^m = b^n = 1$. Then $b^{\alpha m} = b^{\beta n} = 1$ so $b^{\alpha m + \beta n} = b = 1$.

Surjectivity.

Take $a \in A$ and let $m_a := \gcd(\mathrm{ord}(a), m)$, $n_a := \gcd(\mathrm{ord}(a), n)$. Then $\mathrm{ord}(a) = m_a n_a$. (Indeed, if not true, then $m_a n_a l = \mathrm{ord}(a)$ for some positive integer $l \neq 1$. $l \mid mn$ implies $\gcd(l, m)$ or $\gcd(l, n)$ is not 1. Say $\gcd(l, m) =: m_l \neq 1$. Then $m_a m_l \mid \gcd(m_a m_l, mn) \mid \gcd(\mathrm{ord}(a), mn) = m_a$. This is a contradiction.) Let $b := a^{m_a}$ and $c := a^{n_a}$. Find $\alpha_a, \beta_a \in \mathbb{Z}$ with $\alpha_a m_a + \beta_a n_a = 1$. Then $a = b^{\alpha_a} \cdot c^{\beta_a}$. But $b \in A[n_a] \subset A[n]$ and $c \in A[m_a] \subset A[m]$. So we are done.

□

Remark 1.12. *Geometrically, one should think of the map $x \mapsto x^p$ in $\mathrm{U}(\mathbb{Z}/p^r\mathbb{Z})$ as $x \mapsto x/p$ on the disk of radius 1: $\|x\| \leq p^{r-1}$, raising to p^{r-1}-th power sending everything into the unit disk of radius p^{r-1}, the analogue of identity modulo p^r.*

Lemma 1.13. *Let $r \geq 3$ be an integer. There is a canonical isomorphism $\{\pm 1\} \times \mathbb{Z}/2^{r-2}\mathbb{Z} \cong (\mathbb{Z}/2^r\mathbb{Z})^\times$ where ± 1 goes to $[\pm 1]_{2^r}$ and the $[1] \in \mathbb{Z}/2^{r-2}\mathbb{Z}$ is sent to $[5]_{2^r}$.*

Proof. The map defined in the statement is a group homomorphism from $\{\pm 1\} \times \mathbb{Z}/2^{r-2}\mathbb{Z}$ to $(\mathbb{Z}/2^r\mathbb{Z})^\times$. Indeed, since $5 \equiv 1 \pmod 4$, the order of $[5]_{2^r}$ is at most $\frac{1}{2} \cdot |(\mathbb{Z}/2^r\mathbb{Z})^\times|$. But $|(\mathbb{Z}/2^r\mathbb{Z})^\times| = 2^{r-1}$ (the number of odd numbers in $0, 1, 2, ..., 2^r - 1$), so $\mathrm{ord}([5]_{2^r}) \mid 2^{r-2}$, showing that the homomorphism is well-defined.

Next we check that $\mathrm{ord}([5]_{2^r}) = 2^{r-2}$ and so this homomorphism is really an isomorphism. Similar to the odd prime case, we have that for $k \in \mathbb{Z}_{\geq 2}$ (not true if $k = 1$!), taking square induces a map

$$\begin{aligned} 1 + 2^k\mathbb{Z} \setminus 1 + 2^{k+1}\mathbb{Z} &\to 1 + 2^{k+1}\mathbb{Z} \setminus 1 + 2^{k+2}\mathbb{Z} \\ x &\mapsto x^2. \end{aligned} \tag{6}$$

Hence $(1+4)^{2^\star} \notin 1 + 2^r\mathbb{Z}$ for all $\star \leq r-3$, showing that $\mathrm{ord}([5]_{2^r}) = 2^{r-2}$. This completes the proof. □

1.8. **Multiplicative structure of $\mathbb{Z}/N\mathbb{Z}$.** Let N be a nonzero integer.

- When $N = p$ is a prime number $\mathbb{Z}/p\mathbb{Z} = \mathrm{U}(\mathbb{Z}/p\mathbb{Z}) \sqcup \{[0]\}$, which is a finite field.
- For general N, one can write

$$\mathbb{Z}/N\mathbb{Z} = \bigsqcup_{d \mid N} \{[a] \in \mathbb{Z}/N\mathbb{Z} \mid \gcd(a, N) = d\}.$$

Proposition 1.14. *Given a nonzero integer N and a divisor d of N. Let $X_d := \{[a] \in \mathbb{Z}/N\mathbb{Z} \mid \gcd(a, N) = d\}$. Then*

$$X_d = \{[u][d] \mid [u] \in \mathrm{U}(\mathbb{Z}/N\mathbb{Z})\}.$$

In words, $\bullet \mapsto \gcd(\bullet, N)$ classifies the orbits of $\mathrm{U}(\mathbb{Z}/N\mathbb{Z}) \curvearrowright \mathbb{Z}/N\mathbb{Z}$.

That X_d contains the latter set is direct. Indeed $\gcd(ac, b) = \gcd(a, b)$ if $\gcd(c, b) = 1$.

Lemma 1.15. *Let (x, y) be a pair of coprime integers. Then for every $N \in \mathbb{Z}$, there exists an integer λ_N such that $\gcd(x + \lambda_N y, N) = 1$.*

Proof. First we find λ_p such that $\gcd(x + \lambda_p y, p) = 1$ for each prime factor p of N. This is quite easy: if $\gcd(x, p)$, $\gcd(x + y, p)$ are not 1, then p is a common factor of x and y, a contradiction. To find λ, apply Chinese remainder theorem. □

Proof of Proposition 1.14. So given an integer a with $\gcd(a, N) = d$ we need to find some u coprime to N such that $a \equiv ud \pmod N$.

By consequence of Euclidean algorithm Lemma 1.1, we find $\alpha, \beta \in \mathbb{Z}$ such that $\alpha a + \beta N = d$. If α is coprime to N, then we are done by taking u to be the mod-N inverse of α.

If not, note that

$$\alpha \cdot \frac{a}{d} + \beta \cdot \frac{N}{d} = 1 \implies (\alpha + \lambda \frac{N}{d})a + (\beta - \lambda \frac{a}{d})N = d, \ \forall \lambda \in \mathbb{Z}$$

Since α is coprime to $\frac{N}{d}$, we can find λ by previous lemma such that $\alpha' := \alpha + \lambda \frac{N}{d}$ is coprime to N. Therefore we may take u to be the mod-N inverse of α'. □

1.9. **Proof of Proposition 1.14 avoiding the lemma.** Now we present a different proof from the point view of group action.

Consider the action $(\mathbb{Z}/N\mathbb{Z})^\times \curvearrowright \mathbb{Z}/N\mathbb{Z}$. Then

$$\left\{ [d]_N \;\middle|\; d \mid N,\ d \in \mathbb{Z}^+ \right\}$$

lies in different orbits. If $\mathrm{Stab}_{[d]}$ denotes the stabilizer of $[d]_N$, then

$$|\mathbb{Z}/N\mathbb{Z}| \geq \sum_{d|N,\, d\in\mathbb{Z}^+} \left|\mathrm{U}(\mathbb{Z}/N\mathbb{Z})/\mathrm{Stab}_{[d]}\right| = \sum_{d|N,\, d\in\mathbb{Z}^+} \frac{|\mathrm{U}(\mathbb{Z}/N\mathbb{Z})|}{\left|\mathrm{Stab}_{[d]}\right|} \tag{7}$$

with equality holds iff $\{[d]_N \mid d \mid N,\ d \in \mathbb{Z}^+\}$ is a full set of representative of orbits.

The left hand side of Eq.(7) is just N. We will complete the proof by showing the RHS is also N.

Let us calculate the cardinality of (for each $d \mid N$, $d \in \mathbb{Z}^+$)

$$\mathrm{Stab}_{[d]} = \{[u] \in \mathrm{U}(\mathbb{Z}/N\mathbb{Z}) \mid ud \equiv d \pmod N\} = \{[u] \in \mathrm{U}(\mathbb{Z}/N\mathbb{Z}) \mid (u-1)d \equiv 0 \pmod N\}.$$

Write $N = dq$ for some other $q \in \mathbb{Z}^+$, then

$$N \mid (u-1)d \iff q \mid u-1 \iff u \equiv 1 \pmod q \iff [u]_q = [1]_q \in \mathrm{U}(\mathbb{Z}/q\mathbb{Z}).$$

This shows that

$$\begin{aligned} & \mathrm{Stab}_{[d]} = \ker\left(\mathrm{U}(\mathbb{Z}/N\mathbb{Z}) \to \mathrm{U}(\mathbb{Z}/q\mathbb{Z})\right) \\ \implies & \left|\mathrm{Stab}_{[d]}\right| = \frac{|\mathrm{U}(\mathbb{Z}/N\mathbb{Z})|}{|\mathrm{U}(\mathbb{Z}/q\mathbb{Z})|} = \frac{\phi(N)}{\phi(q)} \\ \implies & \sum_{d|N,\, d\in\mathbb{Z}^+} \frac{|\mathrm{U}(\mathbb{Z}/N\mathbb{Z})|}{\left|\mathrm{Stab}_{[d]}\right|} = \sum_{d|N,\, d\in\mathbb{Z}^+} |\phi(q)| = \sum_{d|N,\, d\in\mathbb{Z}^+} |\phi(d)| = N. \end{aligned} \tag{8}$$

This is exactly what we want.

1.10. **Linear congruence equation.** Given N, a, b, we are interested in the equation

$$ax \equiv b \pmod N. \tag{9}$$

- if $\gcd(a, N) = 1$, then it admits a unique solution modulo N.
- A necessary condition for the existence of solutions :

$$\gcd(a, N) \mid \gcd(b, N).$$

We will prove this is also sufficient.

Proposition 1.16. *Fix a nonzero integer N and two integers a, b. Then*

$$\textit{Eq.(9) has one solution} \iff \gcd(a, N) \mid \gcd(b, N).$$

If this holds, there are $\gcd(a, N)$-many solutions (in $\mathbb{Z}/N\mathbb{Z}$).

Proof. Let us assume that $d_a := \gcd(a, N)$ divides $d_b := \gcd(b, N)$. Since d_a divides d_b, we can find $q \in \mathbb{Z}$ such that $d_a q = d_b$.

By Proposition 1.14, we find u_a, u_b coprime to N such that

$$a \equiv u_a d_a \pmod N, \quad b \equiv u_b d_b \pmod N.$$

Setting u_a^* to be the modulo-N inverse of u_a, Eq.(9) is equivalent to

$$d_a x \equiv u_a^* u_b d_a q \pmod N$$

which is again equivalent to

$$x \equiv u_a^* u_b q \pmod{N/d_a}.$$

That is to say, the solutions to Eq.(9) are precisely the preimage of $[u_a^* u_b q]_{N/d_a}$ along the homomorphism $\mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/(N/d_a)\mathbb{Z}$. Since this homomorphism is surjective, we conclude that there are d_a-many solutions, given by

$$u_a^* u_b q + (N/d_a)\mathbb{Z} \pmod N.$$

□

2. Sum of two squares

Fermat considered the following question:

Question 2.1. *Which prime number can be represented as x^2+y^2 for some $x, y \in \mathbb{Z}$?*

By explicit calculation:

$$2 = 1^2+1^2, \quad 3 \neq x^2+y^2, \quad 5 = 1^2+2^2, \quad 7 \neq x^2+y^2, \quad 11 \neq x^2+y^2, \quad 13 = 2^2+3^2, \dots$$

2.1. **Necessary congruence conditions.** Here is a necessary congruence condition for p being a sum of squares:

Lemma 2.2. *Let p be an odd prime with $p = x^2+y^2$ for some $x, y \in \mathbb{Z}$. Then $p \equiv 1 \pmod 4$.*

Proof. Since p is odd, one of x, y is even and the other is odd. Say $x = 2m$, $y = 2n+1$. Then:

$$p = 4m^2 + 4n^2 + 4n + 1 \implies p \equiv 1 \pmod 4.$$

□

Fermat claimed the following. Euler wrote down a proof.

Theorem 2.3. *Let p be an odd prime. Then the following are equivalent:*

1. *$p = x^2+y^2$ for some $x, y \in \mathbb{Z}$.*
2. *$p \mid x^2+y^2$ for some $x, y \in \mathbb{Z}$ with $\gcd(x, y) = 1$.*
3. *$p \equiv 1 \pmod 4$.*

Proof of $1 \implies 2$. Since p is odd, one of x, y is even and the other is odd. Say $x = 2m$, $y = 2n+1$. Then:

$$p = 4m^2 + 4n^2 + 4n + 1 \implies p \equiv 1 \pmod 4.$$

□

The following can be deduced from Lemma 1.5: $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.

Lemma 2.4. *Assume $p = 4k+1$ for some $k \in \mathbb{Z}$ is a prime. There exists $x \in \mathbb{Z}$ coprime to p such that*

$$x^{2k} - 1 \not\equiv 0 \pmod p.$$

Proof of $3 \implies 2$. Write $p = 4k+1$ for some $k \in \mathbb{Z}$.

Since $(\mathbb{Z}/p\mathbb{Z})^\times$ has order $p-1 = 4k$, we have

$$x^{4k} \equiv 1 \pmod p$$

for all integers x that are coprime to p. Hence,

$$(x^{2k}-1)(x^{2k}+1) \equiv 0 \pmod p.$$

Now take x as in the corollary. Then,

$$x^{2k} + 1 \equiv 0 \pmod p, \quad \text{i.e., } p \mid (x^k)^2 + 1^2.$$

□

2.2. **Congruence condition is sufficient: $2 \implies 1$.** Let p be an odd prime number, we show by induction that

$$p \mid (x^2+y^2),\ \exists\, x, y \in \mathbb{Z},\ \gcd(x, y) = 1 \implies p = x'^2 + y'^2,\ \exists\, x', y' \in \mathbb{Z}.$$

Replacing x by $x + n_x p$, y by $y + n_y p$, for suitable $n_x, n_y \in \mathbb{Z}$, we assume

$$|x| \leq \frac{p}{2}, \quad |y| \leq \frac{p}{2}.$$

So

$$x^2 + y^2 \leq \frac{p^2}{2}. \tag{10}$$

Let

$$x^2 + y^2 = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$$

be the factorization into primes, with $p_1 > p_2 > p_3 > \cdots$. We have $p_1 = p$, $d_1 = 1$ by Eq.(10). If $k = 1$, then we are done.

Otherwise, we have $p_2 \mid (x^2+y^2)$, $\gcd(x, y) = 1$. By induction hypothesis, $p_2 = a^2+b^2$ for some $a, b \in \mathbb{Z}$. It only remains to show the following:

Lemma 2.5. *Let q be a prime number that can be written as a sum of squares:*

$$q = a^2 + b^2, \quad a, b \in \mathbb{Z}.$$

Assume that q divides $x^2 + y^2$ for some $x, y \in \mathbb{Z}$. Then there exist $c, d \in \mathbb{Z}$ such that

$$x^2 + y^2 = (a^2 + b^2)(c^2 + d^2).$$

Proof. Let i be a solution to $x^2 + 1 = 0$. Then the desired conclusion suggests:

$$x + iy = (a + ib)(c + id) \quad \text{or} \quad x + iy = (a - ib)(c + id).$$

So we are led to compute:

$$\frac{x + iy}{a + ib} = \frac{(x + iy)(a - ib)}{a^2 + b^2} = \frac{(ax + by) + i(ay - bx)}{q},$$
$$\frac{x + iy}{a - ib} = \frac{(x + iy)(a + ib)}{a^2 + b^2} = \frac{(ax - by) + i(ay + bx)}{q}.$$

Since

$$(ax + by)(ax - by) = a^2x^2 - b^2y^2 = a^2x^2 + (a^2 - q)y^2 \equiv a^2(x^2 + y^2) - qy^2 \equiv 0 \pmod{q},$$

one of $q \mid (ax + by)$ and $q \mid ax - by$ must be true. WLOG, assume the former holds. Then

$$(ay - bx)^2 \equiv (ay - bx)^2 + (ax + by)^2 = a^2(x^2 + y^2) + b^2(x^2 + y^2) \equiv 0 \pmod{q}.$$

So

$$x + iy = (a + ib)(c + id) \quad \text{with } c = \frac{ax + by}{q},\ d = \frac{ay - bx}{q} \in \mathbb{Z}.$$

Calculating $(x + iy)(x - iy)$ proves the lemma. □

3. Quadratic reciprocity law

3.1. Square root of -2 mod p.

Let us observe the following

Lemma 3.1. *Let p be an odd prime and n be an integer with $p \nmid n$. TFAE*

- *$p \mid x^2 + ny^2$ for a pair of coprime integers (x, y);*
- *$x^2 + ny^2 \equiv 0 \pmod{p}$ has a nonzero solution;*
- *there exists $x \in \mathbb{Z}/p\mathbb{Z}$ such that $x^2 = [-n]_p$, i.e., $-n$ has a square rood modulo p.*

When $n = 1$ we know the above is equivalent to $p \equiv 1 \pmod{4}$. Can this be generalized? Let us take the second example $n = 2$. Does $\sqrt{-2}$ exist in $\mathbb{Z}/p\mathbb{Z}$?

Well by the group isomorphism

$$\mathrm{U}(\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/(p - 1)\mathbb{Z}$$

an element in $\mathrm{U}(\mathbb{Z}/p\mathbb{Z})$ has a square root iff the order of this element divides $\frac{p-1}{2}$, that is

$$\sqrt{-2} \text{ exist in } \mathbb{Z}/p\mathbb{Z} \iff (-2)^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

On the other hand, we have another expression for $\sqrt{-2}$:

$$\zeta_8 - \zeta_8^{-1} = \sqrt{-2}.$$

From here we already see that if $p \equiv 1 \pmod{8}$, then ζ_8, and hence $\sqrt{-2}$ exists in $\mathbb{Z}/p\mathbb{Z}$. We still need to worry about the case $p \equiv 3, 5, 7 \pmod{8}$.

So we have

$$(-2)^{\frac{p-1}{2}} = (\zeta_8 + \zeta_8^{-1})^{p-1}.$$

We know that raising to p-th power is easy modulo p:

$$(\zeta_8 - \zeta_8^{-1})^p \equiv \zeta_8^p - \zeta_8^{-p} \pmod{p}$$

whose value is determined by the residue class of p modulo 8. Indeed

$$\zeta_8^p - \zeta_8^{-p} \pmod{p} \equiv \begin{cases} \zeta_8 - \zeta_8^{-1} & \text{if } p \equiv 1, 3 \pmod{8} \\ -\zeta_8 + \zeta_8^{-1} & \text{if } p \equiv 5, 7 \pmod{8} \end{cases}$$

This implies that

$$(-2)^{\frac{p-1}{2}} = (\zeta_8 + \zeta_8^{-1})^{p-1} \equiv \begin{cases} 1 & \text{if } p \equiv 1, 3 \pmod{8} \\ -1 & \text{if } p \equiv 5, 7 \pmod{8} \end{cases}$$

In other words,

$$\sqrt{-2} \text{ exists in } \mathbb{Z}/p\mathbb{Z} \iff p \equiv 1, 3 \pmod{8}.$$

3.1.1. *Square root of* -5. As one notes, in the above process, the key is to find an expression for $\sqrt{-n}$ using roots of unity. When $n = 5$, one can apply some clever trigonometry.

By staring at the triangle with inner angles $36°, 72°, 72°$. One finds

- $\sin 36° = \dfrac{\sin 72°}{(1+\sqrt{5})/2} \implies \cos 36° = \dfrac{1+\sqrt{5}}{4}$
- $\cos 72° = \dfrac{-1+\sqrt{5}}{4}$.
- the above two implies that

$$\zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4 = \sqrt{5}$$

Now we can again repeat the argument before to conclude that

$$\sqrt{5} \text{ exists modulo } p \iff p \equiv \pm 1 \pmod 5.$$

which is equivalent to $p \equiv \pm 1, \pm 9 \pmod{20}$.

One may continue to $\sqrt{-7}$, but ζ_7 is not easy to explicitly compute. Indeed, one can prove that ζ_7 is not expressible as finite combinations of rational numbers and square root and $+, -, \times, \div$ (known as constructible numbers).

3.2. **Euler's conjecture: quadratic reciprocity.** Though we get stuck in generalizing the proof. It is possible to do a few calculations:

quadratic_residues_p1mod4

p\q	5	13	17	29	37	41	53	61	73	89	97
5		0	0	1	0	1	0	1	0	1	0
13	0		1	1	0	0	1	1	0	0	0
17	0	1		0	0	0	1	0	0	1	0
29	1	1	0		0	0	1	0	0	0	0
37	0	0	0	0		1	1	0	1	0	0
41	1	0	0	0	1		0	1	1	0	0
53	0	1	1	1	1	0		0	0	1	1
61	1	1	0	0	0	1	0		1	0	1
73	0	0	0	0	1	1	0	1		1	1
89	1	0	1	0	0	0	1	0	1		1
97	0	0	0	0	0	0	1	1	1	1	

In the table above, the column primes are called p, row primes are called q. The (p, q)-th entry is 1 iff p is a quadratic modulo q and is 0 otherwise. In the table only primes that are 1 modulo 4 are listed. One notices that this is a symmetric matrix. Euler conjectured this is always the case. More generally, Euler made the following conjecture, proved later by Gauss. This is now known as quadratic reciprocity law.

Definition 3.2 (Legendre symbol)**.** *For $a \in \mathbb{Z}$ and an odd prime p,*

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{if } a \equiv 0 \pmod p, \\ 1 & \text{if } \gcd(a,p) = 1,\ a \text{ is a quadratic modulo } p, \\ -1 & \text{if } \gcd(a,p) = 1,\ a \text{ is not a quadratic modulo } p. \end{cases}$$

Theorem 3.3. *Let p and q be two distinct odd primes.*

1. $$\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod 4, \quad \text{or } \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}};$$
2. $$\left(\frac{2}{p}\right) = 1 \iff p \equiv 1, 7 \pmod 8, \quad \text{or } \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}};$$

3. (1) *if* $q \equiv 1 \pmod 4$ *or* $p \equiv 1 \pmod 4$*, then*

$$\left(\frac{q}{p}\right) = 1 \iff \left(\frac{p}{q}\right) = 1.$$

(2) *If* $p \equiv 3 \pmod 4$*, then*

$$\left(\frac{q}{p}\right) = 1 \iff \left(\frac{p}{q}\right) = -1.$$

In other words,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

We have seen the (rough) proof of the first two. Here are some explicit corollaries:

$$\left(\frac{3}{p}\right) = 1 \iff p \equiv \pm 1 \pmod{12}$$
$$\left(\frac{5}{p}\right) = 1 \iff p \equiv \pm 1, \pm 9 \pmod{20}$$
$$\left(\frac{7}{p}\right) = 1 \iff p \equiv \pm 1, \pm 25, \pm 9 \pmod{28}$$
$$\left(\frac{6}{p}\right) = 1 \iff p \equiv \pm 1, \pm 5 \pmod{24}$$

3.3. **Modulo p in ring extensions.** Here we resolve a technical issue that would arise in the proof.

Given an integer n, we write $\zeta_n := e^{\frac{2\pi i}{n}}$ and let $\mathbb{Z}[\zeta_n]$ be the subring of $\mathbb{C}$ generated by $\mathbb{Z}$ and ζ_n. So it consists of all $f(\zeta_n)$ as f ranges over all polynomials with integer coefficients.

Lemma 3.4. $\mathbb{Z}[\zeta_n] \cap \mathbb{Q} = \mathbb{Z}$.

The proof will be delayed to a later subsection.

Definition 3.5. *Let I be an additive subgroup (so that the being congruent is an equivalence relation) of $\mathbb{C}$, two complex numbers x, y are said to be congruent modulo I, written as $x \equiv y \pmod I$, iff $x - y \in I$.*

So for two integers a, b and a nonzero integer N,

$$a \equiv b \pmod N \iff a \equiv b \pmod{N\mathbb{Z}}.$$

As a corollary, we have

Corollary 3.6. *Let p, n be two integers. Then $p\mathbb{Z}[\zeta_n] \cap \mathbb{Q} = p\mathbb{Z}$. Consequently, for two rational numbers x, y, we have the following equivalence:*

$$x \equiv y \pmod p \iff x \equiv y \pmod{p\mathbb{Z}[\zeta_n]}$$

Proof. It is direct to see that $p\mathbb{Z}[\zeta_n] \cap \mathbb{Q} \supset p\mathbb{Z}$. Conversely, suppose $x \in p\mathbb{Z}[\zeta_n] \cap \mathbb{Q}$, then $x/p \in \mathbb{Z}[\zeta_n] \cap \mathbb{Q} = \mathbb{Z}$ by Lemma 3.4. Thus $x \in p\mathbb{Z}$.

Once this is done, that $x - y \in p\mathbb{Z} \iff x - y \in p\mathbb{Z}[\zeta_n]$ follows. □

So the proof of can be rigorously completed as follows.

$$2^{\frac{p-1}{2}} \cdot (\zeta_8 + \zeta_8^{-1}) = (\zeta_8 + \zeta_8^{-1})^p \equiv \zeta_8^p + \zeta_8^{-p} \pmod{p\mathbb{Z}[\zeta_8]} \tag{11}$$

A direct computation shows that $p \equiv \pm 1 \pmod 8$ iff $(-1)^{\frac{p^2-1}{8}} = 1$. First assume that $p \equiv 1 \pmod 8$ and we need to show $2^{\frac{p-1}{2}} \equiv 1 \pmod p$. From Eq.(11) and the assumption we have

$$\begin{aligned}
& 2^{\frac{p-1}{2}}(\zeta_8 + \zeta_8^{-1}) \equiv \zeta_8 + \zeta_8^{-1} \pmod{p\mathbb{Z}[\zeta_8]} \\
\implies & (2^{\frac{p-1}{2}} - 1)(\zeta_8 + \zeta_8^{-1}) \equiv 0 \pmod{p\mathbb{Z}[\zeta_8]} \\
\implies & (2^{\frac{p-1}{2}} - 1)(\zeta_8 + \zeta_8^{-1})^2 = (2^{\frac{p-1}{2}} - 1) \cdot 2 \equiv 0 \pmod{p\mathbb{Z}[\zeta_8]} \\
(\text{Coro } 3.6) \implies & (2^{\frac{p-1}{2}} - 1) \cdot 2 \equiv 0 \pmod p. \\
(\gcd(2, p) = 1) \implies & 2^{\frac{p-1}{2}} - 1 \equiv 0 \pmod p
\end{aligned}$$

In the other case when $p \equiv \pm 3 \pmod 8$, we have $\zeta_8^3 + \zeta_8^{-3} = -(\zeta_8 + \zeta_8^{-1})$. Similar arguments as above then imply that $2^{\frac{p-1}{2}} \equiv -1 \pmod p$. This completes the proof of part 2.

3.4. **Gauss sum and the proof of quadratic reciprocity law.** Define $g_q := \sum_{a \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{a}{q}\right) \zeta_q^a$.

Lemma 3.7. *Let q be a positive odd prime number, then $g_q^2 = \left(\frac{-1}{q}\right) \cdot q$.*

Proof. We start with a series of change of variables

$$\begin{aligned}
g_q^2 &= \left(\sum_{a \in (\mathbb{Z}/q\mathbb{Z})^\times} \left(\frac{a}{q}\right) \zeta_q^a\right)^2 = \sum_{a,b \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{ab}{q}\right) \zeta_q^{a+b} \\
&= \sum_{t \in (\mathbb{Z}/q\mathbb{Z})^\times} \sum_{a \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{a(t-a)}{q}\right) \zeta_q^t + \sum_{a \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{-a^2}{q}\right) \\
&= \sum_{t \in (\mathbb{Z}/q\mathbb{Z})^\times} \zeta_q^t \sum_{a \in (\mathbb{Z}/q\mathbb{Z})^\times} \left(\frac{a(t-a)a^{-2}}{q}\right) + \left(\frac{-1}{q}\right)(q-1) \\
&= \sum_{t \in (\mathbb{Z}/q\mathbb{Z})^\times} \zeta_q^t \sum_{a \in (\mathbb{Z}/q\mathbb{Z})^\times} \left(\frac{ta^{-1}-1}{q}\right) + \left(\frac{-1}{q}\right)(q-1) \\
&= \sum_{t \in (\mathbb{Z}/q\mathbb{Z})^\times} \zeta_q^t \sum_{a \in (\mathbb{Z}/q\mathbb{Z})^\times} \left(\frac{b-1}{q}\right) + \left(\frac{-1}{q}\right)(q-1) \\
&= \sum_{t \in (\mathbb{Z}/q\mathbb{Z})^\times} \zeta_q^t(-1)\left(\frac{-1}{q}\right) + (q-1)\left(\frac{-1}{q}\right) = q\left(\frac{-1}{q}\right).
\end{aligned}$$

□

Once this lemma is verified, the remaining proof is similar as before

$$\begin{aligned}
&\left(\left(\frac{-1}{q}\right) q\right)^{\frac{p-1}{2}} \cdot \left(\sum \left(\frac{a}{p}\right) \zeta_q^a\right) \\
&= \left(\sum \left(\frac{a}{p}\right) \zeta_q^a\right)^p \equiv \sum \left(\frac{a}{p}\right) \zeta_q^{ap} \equiv \left(\frac{p}{q}\right) \cdot \sum \left(\frac{a}{p}\right) \zeta_q^a \pmod{p\mathbb{Z}[\zeta_q]} \\
&\implies (-1)^{\frac{q-1}{2}\frac{p-1}{2}} q^{\frac{p-1}{2}} \equiv \left(\frac{p}{q}\right) \pmod p.
\end{aligned}$$

This completes the proof.

3.5. **Proof of Lemma 3.4.** We need Gauss' lemma. For a polynomial $f(x) = a_0 x^N + ... + a_N$ in $\mathbb{Z}[X]$, let $\mathrm{coeff}(f)$ be the set of non-zero coefficients $\{a_i\}$.

Lemma 3.8. *For $g, h \in \mathbb{Z}[X]$ with $\gcd(\mathrm{coeff}(g)) = \gcd(\mathrm{coeff}(h)) = 1$, we have $\gcd(\mathrm{coeff}(g \cdot h)) = 1$.*

Proof. We write

$$\begin{aligned}
g(x) &= b_0 x^m + b_1 x^{m-1} + ... + b_m, \\
h(x) &= c_0 x^l + c_1 x^{l-1} + ... + c_l, \\
g \cdot h(x) &= a_0 x^n + a_1 x^{n-1} + ... + a_n.
\end{aligned}$$

By convention a_i, b_i or c_i is set to be 0 if it does not appear.

Now assume the conclusion is false and we seek for a contradiction. Find a prime p dividing all $a_i's$. Choose k (resp. r) to be the smallest non-negative integer such that

$$\begin{aligned}
&p \mid b_0, b_1, ..., b_{k-1} \text{ but } p \nmid b_k \\
&\text{resp. } p \mid c_0, b_1, ..., c_{r-1} \text{ but } p \nmid c_r.
\end{aligned}$$

Consider

$$a_{k+r} = b_0 c_{k+r} + ... + b_{k-1} c_{r+1} + b_k c_r + b_{k+1} c_{r-1} + ... + b_{k+r} c_0.$$

For instance, $k = 0, r = 2$, we are looking at $a_2 = b_0 c_2 + b_1 c_1 + b_2 c_0$. Then $p \mid b_k c_r$, which is a contradiction.

□

Remark 3.9. *This lemma is a simple consequence of: for each field F, $F[X]$ is an integral ring.*

Now we go back to Lemma 3.4. We are actually going to show that $\mathbb{Z}[\alpha] \cap \mathbb{Q} = \mathbb{Z}$ whenever α is an algebraic integer, i.e., there exists a **monic** $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$. Assume $\deg f$ is as small as possible.

(1) We claim that f is the minimal polynomial for α in $\mathbb{Q}[x]$ (that is, $f(\alpha) = 0$, $f \in \mathbb{Q}[x]$ is monic and $\deg f$ is as small as possible). Otherwise, choose $g(x) \in \mathbb{Q}[x]$ monic whose degree is strictly smaller than f and $g(\alpha) = 0$. Write

$$f = g \cdot h + r$$

for some $g, r \in \mathbb{Q}[x]$ with $\deg r \lneq \deg g$. So $r(\alpha) = 0$. By minimality of $\deg g$, $r = 0$. Let M_1, M_2 be the smallest integers such that $M_1 g(x), M_2 h(x)$ have $\mathbb{Z}$-coefficients. Then $\gcd(\text{coeff}(M_1 g(x)) = \gcd(\text{coeff}(M_2 h(x)) = 1$. By Gauss' Lemma,

$$\gcd(\text{coeff}(M_1 g(x) M_2 h(x)) = \gcd(\text{coeff}(M_1 M_2 f(x)) = 1.$$

Thus $M_1 M_2 = 1$, implying $g \in \mathbb{Z}[x]$ and hence is equal to f.

(2) Let $N = \deg f$. Let W be the $\mathbb{Z}$-module spanned by $\{1, \alpha, \ldots, \alpha^{N-1}\}$. Using the fact that f is monic, for all $m \in \mathbb{Z}$, $\alpha^m \in W$. Thus, W is a ring and is equal to $\mathbb{Z}[\alpha]$.

(3) So any element $q \in \mathbb{Q} \cap \mathbb{Z}[\alpha]$ can be written as $\lambda_0 + \lambda_1 \alpha + \cdots + \lambda_{N-1}\alpha^{N-1}$ for some $\lambda_i \in \mathbb{Z}$, then

$$\varphi(x) = \lambda_0 - q + \lambda_1 x + \cdots + \lambda_N x^{N-1} \text{ annihilates } \alpha.$$

This contradicts against the minimality of f.

3.6. **An alternative way of concluding the proof: finite fields.** Rather than using $\mathbb{Z}[\alpha] \cap \mathbb{Q} = \mathbb{Z}$, we can use finite fields to conclude the proof.

Lemma 3.10. *Let $p \neq q$ be two distinct prime numbers. There exists a field extension F of $\mathbb{Z}/q\mathbb{Z}$ and $x_p \in F$ such that $x_p \neq 1$, $x_p^p = 1$.*

Proof. Write $F_q := \mathbb{Z}/q\mathbb{Z}$. We say a polynomial $\varphi \in F_q[X]$ is irreducible iff whenever $\varphi = f_1 \cdot f_2$ for some $f_1, f_2 \in F_q[X]$, one has f_1 or f_2 is contained in F_q.

Similar to Bezout's theorem, one can prove here that for any two $\varphi, \psi \in F_q[X]$, the ideal $\langle \varphi, \psi \rangle$ generated by them is a principal ideal, that is, there exists $\alpha, \beta \in F_q[X]$ such that $\alpha\varphi + \beta\psi =: f$ divides both φ and ψ. As a consequence, one can show that the ideal generated by an irreducible polynomial is a prime ideal.

Now let $\Phi_p(X) := 1 + X + X^2 + ... + X^{p-1} \in F_q[X]$. Let $\varphi \in F_q[X]$ be an irreducible factor of Φ_p. Then $F_q[X]/\langle \varphi(X) \rangle$ is an integral domain containing F_q. It is also finite, so must be a field. And the image x_p of X in the quotient is an element satisfying $x_p^p = 1$, $x_p \neq 1$.

□

Fix $x_p \in F$ as above. Note that in F we have $(x+y)^q = x^q + y^q$ for every $x, y \in F$. Similar to g_p, we now let $\tau_p := \displaystyle\sum_{a=0}^{p-1} \left(\frac{a}{p}\right) x_p^a \in F$. Just as before, we can show

- $\tau_p^2 = \left[\left(\frac{-1}{p}\right)\right]_q \cdot [p]_q$;
- $\tau_p^q = \tau_p \cdot \left[\left(\frac{q}{p}\right)\right]_q \implies \tau_p^{q-1} = \left[\left(\frac{q}{p}\right)\right]_q$.

and the above two imply that

- $\tau_p^{2\cdot(q-1)/2} = \left[\left(\frac{-1}{p}\right)\right]_q^{\frac{q-1}{2}} \cdot [p]_q^{\frac{q-1}{2}} = \left[\left(\frac{q}{p}\right)\right]_q$.

In other words,

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

which proves a major part of quadratic reciprocity law. The rest can be handled in a similar manner.

3.7. **Jacobi symbol.**

Definition 3.11 (Jacobi symbol)**.** *Let $M \in \mathbb{Z}$ and m be an odd positive integer. Let $m = \prod_{i=1}^{k} p_i^{a_i}$ be the prime decomposition of m. Define the Jacobi symbols:*

$$\left(\frac{M}{m}\right) := \prod_{i=1}^{k} \left(\frac{M}{p_i}\right)^{a_i}; \quad \left(\frac{M}{1}\right) := 1, \ M \neq 0; \quad \left(\frac{0}{1}\right) := 0.$$

It follows from the definition that

$$\left(\frac{M_1 M_2}{m}\right) = \left(\frac{M_1}{m}\right)\left(\frac{M_2}{m}\right).$$

That is, $M \mapsto \left(\frac{M}{m}\right)$ may be viewed as a homomorphism from the (multiplicative) semigroup $\mathbb{Z}/m\mathbb{Z}$ to $\{0, -1, 1\}$. Also,

$$\left(\frac{M}{m_1 m_2}\right) = \left(\frac{M}{m_1}\right)\left(\frac{M}{m_2}\right).$$

But it is not clear from the definition that whether $\left(\frac{M}{m}\right)$ only depends on $m \pmod M$.

We extend quadratic reciprocity to positive odd integers.

Lemma 3.12. *Let M, m be two positive odd integers. Then*

1. $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$;
2. $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$;
3. $\left(\frac{M}{m}\right) = \left(\frac{m}{M}\right)(-1)^{\frac{(M-1)(m-1)}{4}}$.

Remark 3.13. $\left(\frac{M}{m}\right) = 1$ *does not mean M is a square modulo m.*

To prove this lemma, let us assume their prime decompositions are $M = \prod_{i=1}^{r} q_j^{b_j}$ and $m = \prod_{i=1}^{l} p_i^{a_i}$.

Proof of 1. By definition and Theorem 3.3,

$$\left(\frac{-1}{m}\right) = \prod \left(\frac{-1}{p_i}\right)^{a_i} = \prod \left((-1)^{\frac{p_i-1}{2}}\right)^{a_i} = (-1)^{\sum a_i \cdot \frac{p_i-1}{2}} = (-1)^{\frac{\prod p_i^{a_i}-1}{2}} = (-1)^{\frac{m-1}{2}}.$$

The last two equalities come from the fact that for two odd integers x, y we have

$$\frac{x-1}{2} + \frac{y-1}{2} \equiv \frac{xy-1}{2} \pmod 2.$$

And we are done. □

Proof of 2. This is the same as above except that one needs

$$\frac{x^2-1}{8} + \frac{y^2-1}{8} \equiv \frac{x^2y^2-1}{8} \pmod 2$$

for two odd integers x, y. □

Proof of 3. The proof is also similar:

$$\left(\frac{M}{m}\right) = \prod_{i,j} \left(\frac{q_j}{p_i}\right)^{b_j a_i} = \left(\frac{m}{M}\right)(-1)^{\left(\sum a_i \frac{p_i-1}{2}\right)\cdot\left(\sum b_j \frac{q_j-1}{2}\right)} = \left(\frac{m}{M}\right)(-1)^{\frac{m-1}{2}\cdot\frac{M-1}{2}}.$$

□

Lemma 3.14. *Let m, n be two positive odd integers. Let D be an integer satisfying $D \equiv 0, 1 \pmod 4$. Assume $m \equiv n \pmod D$, then $\left(\frac{D}{m}\right) = \left(\frac{D}{n}\right)$.*

Proof when $D \equiv 1 \pmod 4$. If $D > 0$ and $D \equiv 1 \pmod 4$, then by Lemma 3.12,

$$\left(\frac{D}{m}\right) = \left(\frac{m}{D}\right) = \left(\frac{n}{D}\right) = \left(\frac{D}{n}\right).$$

If $D < 0$ and $D \equiv 1 \pmod 4$, then $-D \equiv 3 \pmod 4$. Thus

$$\left(\frac{D}{n}\right) = (-1)^{\frac{n-1}{2}}\left(\frac{-D}{n}\right) = (-1)^{\frac{n-1}{2}}\left(\frac{n}{-D}\right)(-1)^{\frac{n-1}{2}} = \left(\frac{n}{-D}\right) = \left(\frac{m}{-D}\right) = \left(\frac{D}{m}\right).$$

□

Proof when $D \equiv 0 \pmod 4$. Now assume $D \equiv 0 \pmod 4$ and we write $D = 4^r d$ for some positive integer r and some integer d not divisible by 4. In this case m is congruent to n modulo 4. Thus $\left(\frac{-1}{m}\right) = \left(\frac{-1}{n}\right)$. Therefore the case when $D < 0$ follows from the case when $D > 0$. So from now on assume $D > 0$.

If d is even, then $d = 2^l d'$ for some odd integer d' and $l \in \mathbb{Z}^+$. Now $m \equiv n \pmod 8$, implying that $\left(\frac{2}{m}\right) = \left(\frac{2}{n}\right)$. Since $m \equiv n \pmod{d'}$, we know by Lemma 3.14 that $\left(\frac{d'}{m}\right) = \left(\frac{d'}{n}\right)$. Therefore,

$$\left(\frac{D}{m}\right) = \left(\frac{2}{m}\right)^l \cdot \left(\frac{d'}{m}\right) = \left(\frac{2}{n}\right)^l \cdot \left(\frac{d'}{n}\right) = \left(\frac{D}{n}\right).$$

The last case when d is odd directly follows from Lemma 3.14. □

3.8. **The associated character.** We will prove later in Lemma 4.9 that the iff condition for an integer m coprime to D to be represented by some other quadratic form of the same discriminant:

$$D \equiv x^2 \pmod m \quad \exists\, x \in \mathbb{Z}.$$

Now we specialize to the case when m is a prime number p. Using quadratic reciprocity, we explain that this condition defines a subgroup of $(\mathbb{Z}/D\mathbb{Z})^\times$. Indeed, we will define a group homomorphism $\chi_D : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}$ such that p satisfies the above condition iff $[p]_D \in \ker \chi_D$.

Theorem 3.15. *Given a nonzero integer D satisfying $D \equiv 0, 1 \pmod 4$, there exists a unique homomorphism*

$$\chi_D : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}$$

such that

$$\chi_D([p]) = \left(\frac{D}{p}\right) \quad \textit{for every odd prime } p \textit{ not dividing } D.$$

Moreover,

$$\chi_D([-1]) = \begin{cases} 1 & D > 0 \\ -1 & D < 0 \end{cases}.$$

Proof. For $x \in (\mathbb{Z}/D\mathbb{Z})^\times$, choose $m_x \in \mathbb{Z}$ such that $[m_x] = x$ and m_x is positive and odd. Define $\chi_D(x) := \left(\frac{D}{m_x}\right)$. It follows from Lemma 3.14 that this is independent from the choice of m_x.

For $x, y \in (\mathbb{Z}/D\mathbb{Z})^\times$, $m_x m_y \equiv m_{xy} \pmod D$. Thus

$$\chi_D(xy) = \left(\frac{D}{m_{xy}}\right) = \left(\frac{D}{m_x m_y}\right) = \chi_D(x)\chi_D(y),$$

showing that χ_D is indeed a group homomorphism. It only remains to calculate $\chi_D([-1])$, which is a case-by-case analysis.

Case 1.1, $D > 0$, odd.

$$\chi_D([-1]) = \left(\frac{D}{2D-1}\right) = \left(\frac{2D-1}{D}\right) = \left(\frac{-1}{D}\right) = (-1)^{\frac{D-1}{2}} = 1.$$

Case 1.2, $D > 0$, even. Write $D = 4^r d$ and $4 \nmid d$. Note that $D - 1 \equiv 3 \pmod 4$. If d is even, write $d = 2d'$. In this case $D - 1 \equiv -1 \pmod 8$, so $\left(\frac{2}{D-1}\right) = 1$.

$$\chi_D([-1]) = \left(\frac{D}{D-1}\right) = \left(\frac{d'}{D-1}\right) = \left(\frac{D-1}{d'}\right)(-1)^{\frac{d'-1}{2}} = \left(\frac{-1}{d'}\right)(-1)^{\frac{d'-1}{2}} = 1.$$

The case when d is odd is easier.

Case 2.1, $D < 0$, odd. Note that $-2D - 1 \equiv 1 \pmod 4$.

$$\chi_D([-1]) = \left(\frac{D}{-1-2D}\right) = \left(\frac{-1-2D}{-D}\right) = \left(\frac{-1}{-D}\right) = -1.$$

Case 2.2, $D<0$, even. We only treat the case when $D=-4^r\cdot 2\cdot d'$ for some positive odd d'. Here $-1-D\equiv -1 \pmod 8$.

$$\begin{aligned}\chi_D([-1]) = \left(\frac{D}{-1-D}\right) &= \left(\frac{d'}{-1-D}\right)\left(\frac{-1}{-1-D}\right)\left(\frac{2}{-1-D}\right)\\ &= \left(\frac{-1-D}{d'}\right)(-1)^{\frac{d'-1}{2}}(-1)\\ &= \left(\frac{-1}{d'}\right)(-1)^{\frac{d'-1}{2}}(-1) = -1.\end{aligned}$$

□

4. Reduction theory and the descent step

Let p be an odd prime. We want to know when the implication

$$p \mid x^2+ny^2, \quad \gcd(x,y)=1 \implies p = x^2+ny^2$$

holds. We will define a number $h(-4n)$: implication always holds iff $h(-4n)=1$. To define this number, we need an important conceptual transition: from considering individual quadratic forms one by one to considering all/many of them at the same time – emphasizing their interconnections.

4.1. Space of quadratic forms.

We start with several definitions.

Definition 4.1. *An integral quadratic form Q is a nondegenerate homogeneous polynomial of degree two in two variables with $\mathbb{Z}$-coefficients. Explicitly, $Q(x,y)=ax^2+bxy+cy^2$, with $a,b,c\in\mathbb{Z}$ and $b^2-4ac\neq 0$. It is said to be **primitive** iff $\gcd(a,b,c)=1$. Unless otherwise specified, a **quadratic form** is a binary nondegenerate primitive integral quadratic form by default.*

Given a quadratic form Q, we let

$$\mathrm{Rep}(Q) := \{Q(x,y) \mid x,y\in\mathbb{Z}\}, \quad \mathrm{Rep}^{\mathrm{prim}}(Q) := \{Q(x,y)\mid x,y\in\mathbb{Z},\ \gcd(x,y)=1\}.$$

Definition 4.2. *Two quadratic forms Q and Q' are said to be **properly equivalent** if*

$$Q(x,y) = Q'(px+qy, rx+sy) = Q\left((x,y)\begin{bmatrix}p & r\\ q & s\end{bmatrix}\right)$$

for some $p,q,r,s\in\mathbb{Z}$ satisfying $ps-qr=1$. Sometimes we abbreviate this equivalence relation as $Q\sim Q'$.

Remark 4.3. *Observe that $Q\sim Q' \implies \mathrm{Rep}(Q)=\mathrm{Rep}(Q')$, $\mathrm{Rep}^{\mathrm{prim}}(Q)=\mathrm{Rep}^{\mathrm{prim}}(Q')$.*

Notation 4.4. *Given $\gamma=\begin{pmatrix}p & q\\ r & s\end{pmatrix}$ and a quadratic form Q, let ${}^\gamma Q$ be a new quadratic form defined by*

$${}^\gamma Q(x,y) := Q((x,y)\gamma) = Q(px+ry, qx+sy).$$

Let M_Q denotes the symmetric matrix representing Q, i.e.,

$$Q(x,y) = (x,y)M_Q\begin{pmatrix}x\\ y\end{pmatrix}.$$

Then $M_{{}^\gamma Q} = \gamma M_Q \gamma^{\mathrm{tr}}$.

Lemma 4.5. *Let $Q(x,y):=ax^2+bxy+cy^2$ be a quadratic form and $\gamma\in \mathrm{SL}_2(\mathbb{Z})$, then ${}^\gamma Q(x,y)$ just defined is still quadratic form. Namely, if $Q' := {}^\gamma Q = a'x^2+b'xy+c'y^2$. then $a',b',c'\in\mathbb{Z}$, $\gcd(a',b',c')=1$ and $b'^2-4a'c'\neq 0$.*

Proof. From the definition, one sees that $a',b',c'\in\mathbb{Z}$. Also, that $b'^2-4a'c'\neq 0$ will follow from Lemma 4.7 below and we do not repeat the proof here.

To see $\gcd(a',b',c')=1$, let us assume the converse: for certain prime p, one has $p\mid a',b',c'$. Then $p\mid Q'(x,y)$ for all integers x,y. Or in other words, $p\mid \mathrm{Rep}(Q')$, which is equal to $\mathrm{Rep}(Q)$.

Now let us observe that $a=Q(1,0)$, $b=Q(0,1)$ and $c=Q(1,1)-Q(1,0)-Q(0,1)$. Therefore $1=\gcd(a,b,c)=\gcd(Q(1,0),Q(0,1),Q(1,1))$. But this contradicts against the assertion that $p\mid \mathrm{Rep}(Q)$. □

4.2. **Discriminant friends.** Besides $\mathrm{Rep}(-)$, there is another invariant with respect to this relation:

Definition 4.6. *The **discriminant** of a quadratic form $Q(x,y) = ax^2 + bxy + cy^2$ is defined by $\mathrm{disc}(Q) := b^2 - 4ac$.*

Lemma 4.7. *If $Q \sim Q'$, then $\mathrm{disc}(Q) = \mathrm{disc}(Q')$.*

Proof. Note that $M_Q = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$ and hence $\mathrm{disc}(Q) = -4\det(M_Q)$. If $Q \sim Q'$, then we find $\gamma \in \mathrm{SL}(2,\mathbb{Z})$ such that $Q = {}^{\gamma}Q'$. So $M_{Q'} = \gamma M_Q \gamma^{\mathrm{tr}}$. Hence

$$\det(M_{Q'}) = \det(M_Q), \text{ implying } \mathrm{disc}(Q') = \mathrm{disc}(Q).$$

□

Notation 4.8. *We denote by $\mathcal{M}_D$ the space of quadratic forms of discriminant D. When $D < 0$, we let $\mathcal{M}_D^+ \subset \mathcal{M}_D$ collect positive definite forms. Let $\mathcal{M}_D(\mathbb{R})$ (resp. $\mathcal{M}_D^+(\mathbb{R})$) be the space of (resp. positive definition) real quadratic forms of discriminant D.*

Note that a necessary condition for $\mathcal{M}_D \neq \emptyset$ is that $D \equiv 0, 1 \pmod 4$.

Lemma 4.9. *Assume D is a nonzero integer with $D \equiv 0, 1 \pmod 4$. Then $\mathcal{M}_D \neq \emptyset$. And if m is an odd number coprime to D, then*

$$D \equiv x^2 \pmod m \quad \exists\, x \in \mathbb{Z} \iff m \in \mathrm{Rep}^{\mathrm{prim}}(Q),\ \exists\, Q \in \mathcal{M}_D.$$

Since the first half of the statement is implied by the second half, we focus on proving the latter.

Proof of $\Longleftarrow$. Find $Q(x,y) = ax^2 + bxy + cy^2$ and coprime integers p, q such that $m = Q(p,q)$. By Bezout theorem, find $t, s \in \mathbb{Z}$ such that $pt - qs = 1$. Let $M_Q = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$. Then we can find integer n, l such that

$$AM_QA^{\mathrm{tr}} = \begin{pmatrix} m & \frac{n}{2} \\ \frac{n}{2} & l \end{pmatrix}, \text{ where } A := \begin{pmatrix} p & q \\ s & t \end{pmatrix}.$$

Taking determinants of both sides:

$$-\frac{D}{4} = ml - \frac{n^2}{4} \implies D = -4ml + n^2 \implies D \equiv n^2 \pmod m.$$

This finishes the proof. □

Proof of $\Longrightarrow$. We first note that

$$m = m \cdot 1^2 + b \cdot 1 \cdot 0 + c \cdot 0^2 \quad \forall\, b, c \in \mathbb{Z}.$$

That is, if $Q_{b,c}(x,y) = mx^2 + bxy + cy^2$, then $m = Q_{b,c}(1,0) \in \mathrm{Rep}^{\mathrm{prim}}(Q_{b,c})$. We hope to find $b, c \in \mathbb{Z}$ such that

$$\mathrm{disc}(Q_{b,c}) = b^2 - 4mc = D \tag{12}$$

Since $D \equiv \square \pmod m$, there exist $s, t \in \mathbb{Z}$ such that $D = s^2 - tm$. Thus

$$D = (s+m)^2 - 2sm - m^2 - tm = (s+m)^2 - (2s + m + t)m.$$

We let $t' := 2s + m + t$. Since m is odd, one of t or t' must be even. WLOG, we assume t is even.

We then make use of the condition $D \equiv 0, 1 \pmod 4$. Also note that $s^2 \equiv 0, 1 \pmod 4$. Thus

$$tm = s^2 - D \equiv 0, 1 - 0, 1 \equiv -1, 0, 1 \pmod 4.$$

But t is even, so we are forced to have $tm \equiv 0 \pmod 4$. As m is odd, $t \equiv 0 \pmod 4$. So we can write $t = 4r$ for some $r \in \mathbb{Z}$.

Thus $b := s$, $c := r$ is a solution to Eq.(12) and the proof is complete.

□

We are interested in the quadratic form $x^2 + ny^2$, which has discriminant $-4n$. Apply the lemma in the case $D = -4n$ and $m = p$ is a prime here.

Corollary 4.10. *Let $n_{\neq 0} \in \mathbb{Z}$ and p be an odd prime not dividing n, then*

$$\left(\frac{-n}{p}\right) = 1 \iff p \in \mathrm{Rep}^{\mathrm{prim}}(Q),\ \exists\, Q \in \mathcal{M}_{-4n}.$$

Summary

Let me summarize the situation so far. Using change of coordinates, we defined an action of $\mathrm{SL}_2(\mathbb{Z})$ on the set of quadratic forms. And we find that discriminant is an invariant for this action. So we end up with actions of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{M}_D$ for each D. And it turns out that, for an integer m corpime to $4D$, the congruence condition[1] D being a square modulo m is equivalent to m being representable by one of the quadratic forms of discriminant D. In the next section, we will find a representative for each $\mathrm{SL}_2(\mathbb{Z})$-orbit, so that we will have a finite list of quadratic forms, one of which can represent the given m under congruence conditions. This method is now called "reduction theory".

4.3. **Reduced form.** So now we know that either one of the equivalent conditions

$$p \mid x^2 + ny^2 \iff \left(\frac{-n}{p}\right) = 1$$

implies that p is primitively represented by some "discriminant-friend" Q of $x^2 + ny^2$. Then p is also primitively represented by any $Q' \sim Q$. The question is, when can we find $Q' = x^2 + ny^2$? So we need find a way to determine whether two given quadratic forms are properly equivalent or not.

Definition 4.11. *Assume $D < 0$. A positive definite quadratic form $Q(x, y) = ax^2 + bxy + cy^2$ of discriminant D is said to be **reduced** if $0 \le b \le a \le c$ and if $|b| = a$ or $a = c$, then $b \ge 0$. We let $\mathcal{M}_D^{+,\mathrm{red}}$ collect all reduced positive definite quadratic forms of discriminant D.*

Theorem 4.12 (Lagrange)**.** *Every positive definite quadratic form Q is properly equivalent to a unique reduced form.*

4.4. **Proof of Existence.** Given $Q(x, y) = a_Q x^2 + b_Q xy + c_Q y^2$, by choosing special p, q, r, s, we find that the following two forms are properly equivalent to Q:

$$\mathcal{U}(Q)(x, y) = Q(x - y, y) = a_Q x^2 + (b_Q - 2a_Q)xy + (c_Q + a_Q - b_Q)y^2$$
$$\mathcal{T}(Q)(x, y) = Q(-y, x) = c_Q x^2 - b_Q xy + a_Q y^2.$$

Also note that Q being positive definite implies that

$$\mathrm{disc}(Q) = b_Q^2 - 4a_Q c_Q < 0, \quad a_Q, c_Q > 0.$$

The idea is to apply $\mathcal{U}$ and $\mathcal{T}$ repeatedly to reduce the size of $|b_Q|$. For convenience, let us assume that we have already arrived at Q_0 such that

(1) $Q_0 \sim Q$,
(2) $|b_0| := |b_{Q_0}|$ is as small as possible.

Applying $\mathcal{T}$ if necessary, we further assume that

(3) $a_0 \le c_0$.

Now, we show that $|b_0| \le a_0$. Indeed if this were not true, the b-coefficient of $\mathcal{U}(Q)$ or $\mathcal{U}^{-1}(Q)$ (which is $|b_0 - 2a_0|$, $|b_0 + 2a_0|$ respectively) would be strictly smaller than $|b_0|$, a contradiction against (2).

So we have $|b_0| \le a_0 \le c_0$. If both inequalities are strict, then we are done.

Next, we consider the case when $a_0 = c_0$. If $b_0 \ge 0$ then we are done. Otherwise $Q_1 := \mathcal{T}(Q_0)$ would have the required property.

Last, assume $|b_0| = a_0$. If $b_0 \ge 0$ then we are done. If not, $Q_1 := \mathcal{U}^{-1}(Q_0)$ meets our requirement.

4.5. **Finiteness of class number.** The existence part already leads to some interesting corollaries.

Definition 4.13. *Given an integer $D \equiv 0, 1 \pmod 4$ and $D < 0$, we define the **form class number***

$$h(D) := \#\{\text{proper equivalence classes of positive definite quadratic forms of discriminant } D\}$$
$$= \#\mathcal{M}_D^+ / \mathrm{SL}_2(\mathbb{Z}) = \#\mathcal{M}_D^{+,\mathrm{red}}.$$

Corollary 4.14. *Given $D \in \mathbb{Z}_{<0}$ and $D \equiv 0, 1 \pmod 4$. Let $Q(x, y) = ax^2 + bxy + cy^2$ be a reduced positive definite quadratic form with discriminant D. Then $|b| \le a \le \sqrt{\frac{-D}{4}}$ and $c \le \frac{-D}{4a} \le \frac{-D}{4}$. Consequently $h(D) \le \frac{D^2}{8}$.*

[1] That this is a congruence condition in m follows from quadratic reciprocity law.

Proof. Note that $|b| \le a \le c$.

$$-D = 4ac - b^2 \implies 4ac \le -D \implies c \le \frac{-D}{4a} \le \frac{-D}{4}, a \le \sqrt{\frac{-D}{4}}.$$

□

Remark 4.15. *One (Siegel) can show, for any $\varepsilon \in (0,1)$, there exists $C_\varepsilon > 1$ such that $C_\varepsilon^{-1} D^{1/2-\varepsilon} < h(D) < C_\varepsilon D^{1/2+\varepsilon}$.*

4.6. **Proof of Uniqueness.** The key to the proof is the following observation (due to Lagrange):

Lemma 4.16. *Let $Q(x,y) = ax^2+bxy+cy^2$ is a reduced positive definite quadratic form. Then $|Q(x,y)| \ge c$ (hence $\ge a$) if $x, y \ne 0$. Moreover, if $Q(x,y) = a$, then one of the following holds:*

1. $(x,y) = \pm(1,0)$;
2. $(x,y) = \pm(0,1)$ *and* $a = c$;
3. $(x,y) = \pm(1,-1)$ *and* $a = b = c$, *that is,* $Q(x,y) = x^2 + xy + y^2$.

Proof. We take $x \ne 0$ and $y \ne 0$. We need to show $Q(x,y) \ge c$ and if $Q(x,y) = a$ then $(x,y) = \pm(1,-1)$, $a = b = c$.

The proof is divided into two cases: $|x| \ge |y|$ or $|x| \le |y| - 1$. In either case we have $Q(x,y) \ge ax^2 + cy^2 - |bxy|$ with equality holds iff $xy \le 0$.

In the 1st case, we have

$$\begin{aligned} Q(x,y) &\ge ax^2 + cy^2 - |bxy| \\ (\text{use } |x| \ge |y|) \quad &= |x|\,||ax| - |by|| + cy^2 \\ &\ge cy^2 \ge c \ge a \end{aligned}$$

with $Q(x,y) = a$ iff

$$c = a,\ y^2 = 1,\ a|x| = |b|\,,\ xy \le 0 \implies a = b = c, (x,y) = (1,-1), \text{ or } (-1,1).$$

In the 2nd case, we have

$$\begin{aligned} Q(x,y) &\ge ax^2 + cy^2 - |bxy| \\ (\text{use } |x| \le |y| - 1) \quad &= ax^2 + |y|\,||cy| - |bx|| \\ (\text{use } |x| \le |y| - 1 \text{ again}) \quad &\ge ax^2 + c\,|y| \\ &\gneq c \ge a. \end{aligned}$$

Note that $Q(x,y) = a$ is impossible to hold in this case. □

Now we are ready to prove the uniqueness. Let Q, Q' be two reduced (positive definite) quadratic forms that are properly equivalent and we need to show $Q = Q'$. We first note that by the lemma above,

$$a_Q = \min \mathrm{Rep}^{\mathrm{prim}}(Q) = \min \mathrm{Rep}^{\mathrm{prim}}(Q') = a_{Q'}.$$

By the definition of proper equivalence,

$$Q(x,y) = Q'\left((x,y).\gamma\right), \quad \exists\, \gamma = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

In particular,

$$a'_Q = a_Q = Q(1,0) = (1,0) M_Q \begin{pmatrix} 1 \\ 0 \end{pmatrix} = Q'(p,q).$$

By Lemma 4.16, there are three cases

(a) $(p,q) = \pm(1,0)$
(b) $(p,q) = \pm(0,1)$ and $a'_Q = c'_Q$;
(c) $(p,q) = \pm(1,-1)$ and $a'_Q = b'_Q = c'_Q = 1$.

Case (a). We have

$$\gamma = \pm \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix}, \quad \exists\, r \in \mathbb{Z}.$$

Then

$$\begin{aligned} Q'(x,y) &= a_Q x^2 + (b_Q + 2ra_Q)xy + c_{Q'} y^2 \\ \implies a_Q &\geq |b_Q + 2ra_Q| \geq 2\,|r|\, a_Q - b_Q \geq (2\,|r| - 1)a_Q \end{aligned}$$

Therefore $r = 0, 1, -1$. If $r = 0$, then $Q = Q'$ and we are done. Otherwise $r = \pm 1$, and all inequalities above must be equalities and hence $a_Q = |b_Q|$ and the signs of b_Q and r are different, implying $b_Q = a_Q \geq 0$ and $r = -1$. But now $Q' = a_Q x^2 - a_Q xy + c_Q y^2$ is not reduced, a contradiction.

Case (b). Now $\gamma = \pm \begin{pmatrix} 0 & -1 \\ 1 & s \end{pmatrix}$ and

$$\begin{aligned} Q'(x,y) &= a_Q y^2 + b_Q y(-x + sy) + c_Q(-x + sy)^2 \\ &= c_Q x^2 + (-b_Q - 2sc_Q)xy + (a_Q + sb_Q + s^2 c_Q)y^2 \\ \implies a_Q = c_Q = a'_Q,\ a_Q &\geq |-b_Q - 2sa_Q| \geq |2s|\, a_Q - |b_Q| \geq (2\,|s| - 1)a_Q \end{aligned}$$

So $s = 0, 1, -1$. If $s = 0$, then the above equation implies $b'_Q = -b_Q$ hence $b_Q = b'_Q = 0$ and $Q = Q' = x^2 + y^2$.

If $s = \pm 1$, then all the inequalities above become equalities. So s and b_Q have different signs and $a_Q = |b_Q| \implies a_Q = b_Q$. Hence $s = -1$ and $Q' = Q = x^2 + xy + y^2$.

Case (c). Here we have $Q'(x,y) = x^2 + xy + y^2$. So $a_Q = a'_Q = 1$ and $b_Q = 0, 1, -1$. Inserting into $b_Q^2 - 4c_Q = -3$, we get $b_Q = \pm 1$ and $c_Q = 1$. So $Q = x^2 + xy + y^2 = Q'$.

4.7. **Class number 1 and representation of quadratic forms.**

Definition 4.17. *Given an integer $D \equiv 0, 1 \pmod 4$, We define the principal quadratic form (will be abbreviated as the **principal form**) to be*

$$Q_D^{\text{prin}}(x,y) := \begin{cases} x^2 - \frac{D}{4} y^2 & \text{if } D \equiv 0 \pmod 4 \\ x^2 + xy + \frac{-D+1}{4} y^2 & \text{if } D \equiv 1 \pmod 4 \end{cases}.$$

*The proper equivalence class that Q_D^{prin} belongs to is called the **principal class**.*

Corollary 4.18. *Given a negative integer $D \equiv 0, 1 \pmod 4$ such that $h(D) = 1$. Let p be an odd prime number coprime to D. Then TFAE*

1. *D is a square modulo p;*
2. *$p \in \text{Rep}^{\text{prim}}(Q_D^{\text{prin}})$;*
3. *$Q_D^{\text{prin}}(x,y) \equiv 0 \pmod p$ for some $\gcd(x,y) = 1$.*

In the special case when $D = -4n$ for some $n \in \mathbb{Z}^+$, we have the following equivalences

1. $\left(\dfrac{-n}{p}\right) = 1$;
2. *$p = x^2 + ny^2$ for some $x, y \in \mathbb{Z}$;*
3. *$p \mid x^2 + ny^2$ for some $\gcd(x,y) = 1$.*

4.8. **Examples of class numbers.** Corollary 4.14 yields an algorithm to calculate class numbers. Let us do a few examples by hand.

Example 4.19. $h(-4) = 1$, $\quad \mathcal{M}_D^{+,\text{red}} = \{x^2 + y^2\}$.

Example 4.20. $h(-3) = 1$, $\quad \mathcal{M}_D^{+,\text{red}} = \{x^2 + xy + y^2\}$.

Example 4.21. $h(-12) = 1$, $\quad \mathcal{M}_D^{+,\text{red}} = \{x^2 + 3y^2\}$.

Example 4.22. $h(-16) = 1$, $\quad \mathcal{M}_D^{+,\text{red}} = \{x^2 + 4y^2\}$.

Example 4.23. $h(-20) = 2$, $\quad \mathcal{M}_D^{+,\text{red}} = \{x^2 + 5y^2,\ 2x^2 + 2xy + 3y^2\}$.

Example 4.24. $h(-24) = 2$, $\quad \mathcal{M}_D^{+,\text{red}} = \{2x^2 + 3y^2,\ x^2 + 6y^2\}$.

Example 4.25. $h(-28) = 1$, $\quad \mathcal{M}_D^{+,\text{red}} = \{x^2 + 7y^2\}$.

As a corollary of this example, one obtains

Theorem 4.26. *Let $p \neq 7$ be an odd prime, then*

$$p = x^2 + 7y^2,\ \exists\, x, y \in \mathbb{Z} \iff p \equiv 1, 2, 4 \pmod 7.$$

One may wonder whether there are other examples of class number one.

Theorem 4.27 (Gauss conjecture, Landau theorem)**.** *If $n \in \mathbb{Z}^+$, then $h(-4n) = 1$ iff $n = 1, 2, 3, 4, 7$.*

See Cox's book for a short proof.

4.9. **Relation with hyperbolic geometry.** Let $D < 0$ be fixed. Given $Q = ax^2+bxy+cy^2 \in \mathcal{M}_D^+$, the equation $Q(x, 1) := ax^2 + bx + c = 0$ has a pair of conjugate solutions in $\mathbb{C}$: one has positive imaginary part, the other has negative imaginary part. Let z_Q be the root with positive imaginary part. This construction can be done more generally for

$$Q \in \mathcal{M}_D^+(\mathbb{R}) := \left\{ax^2 + bxy + cy^2 \;\middle|\; a, b, c \in \mathbb{R},\ b^2 - 4ac = D,\ a > 0\right\}.$$

Similar arguments as above show that $\mathrm{SL}_2(\mathbb{R})$ acts on $\mathcal{M}_D^+(\mathbb{R})$ and each orbit of $\mathrm{SL}_2(\mathbb{Z})$ contains one unique element in

$$\mathcal{M}_D^{+,\mathrm{red}}(\mathbb{R}) := \left\{ax^2 + bxy + cy^2 \in \mathcal{M}_D^+(\mathbb{R}) \;\middle|\; 0 \le b \le a \le c,\ \text{ if } |b| = a \text{ or } a = c, \text{ then } b \ge 0\right\}.$$

Taking $Q \mapsto z_Q$ defines a map

$$\mathcal{M}_D^+(\mathbb{R}) \to \mathbb{H}^2 := \{x + iy \in \mathbb{C} \mid y > 0\}$$
$$Q = ax^2 + bxy + cy^2 \mapsto z_Q := \frac{-b + \sqrt{D}}{2a}.$$

Exercise 4.1. *Show that indeed this is a homeomorphism $\mathcal{M}_D^+(\mathbb{R}) \cong \mathbb{H}^2$.*

There is a natural $\mathrm{SL}_2(\mathbb{R})$-action on $\mathbb{H}^2$ (known as fractional transformations):

$$\mathrm{SL}_2(\mathbb{R}) \times \mathbb{H}^2 \to \mathbb{H}^2$$
$$(\gamma, z) = \left(\begin{bmatrix} p & q \\ r & s \end{bmatrix}, z\right) \mapsto \gamma.z := \frac{pz + q}{rz + s}.$$

Exercise 4.2. *Show that this is indeed a group action.*

We temporarily write $\gamma.Q$ for our old notation ${}^{\gamma}Q$.

Lemma 4.28. *Let notations be as above. For $\gamma \in \mathrm{SL}_2(\mathbb{R})$ and $Q \in \mathcal{M}_D^+$, we have $z_{\gamma.Q} = \gamma^{-tr}.z_Q$.*

This is rather direct and the details are left to you. So for each $\gamma \in \mathrm{SL}_2(\mathbb{R})$, we get a commutative diagram:

$$\begin{array}{ccc} \mathcal{M}_D^+(\mathbb{R}) & \xrightarrow{\cong} & \mathbb{H}^2 \\ \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \gamma^{-tr}} \\ \mathcal{M}_D^+(\mathbb{R}) & \xrightarrow{\cong} & \mathbb{H}^2 \end{array}.$$

By transporting $\mathcal{M}_D^{+,\mathrm{red}}$ and Theorem 4.12 (the version for $\mathcal{M}_D^+(\mathbb{R})$) to the right, we have

Lemma 4.29. *Each $\mathrm{SL}_2(\mathbb{Z})$-orbit on $\mathbb{H}^2$ contains a unique element in the region*

$$R = \left\{x + iy \;\middle|\; |x| \le 1/2,\ x^2 + y^2 \ge 1,\ \text{if } |x| = 1/2 \text{ or } x^2 + y^2 = 1 \text{ then } x \ge 0\right\}.$$

Proof. Indeed, given $z = x+iy$, the coefficients a, b, c of the corresponding quadratic form are given by

$$a = \frac{1}{2y} \cdot \sqrt{-D},\ b = -\frac{x^2}{y} \cdot \sqrt{-D},\ c = \frac{y}{2}(1 + \frac{x^2}{y^2}) \cdot \sqrt{-D}.$$

It remains to apply the definition of $\mathcal{M}_D^{+,\mathrm{red}}(\mathbb{R})$. □

For this reason we call R a *strict fundamental domain* for the action $\mathrm{SL}_2(\mathbb{Z}) \curvearrowright \mathbb{H}^2$.

This action is related to hyperbolic geometry. Consider the metric on $\mathbb{H}^2$ defined by $\frac{\mathrm{d}x^2+\mathrm{d}y^2}{y^2}$ (this is called the hyperbolic metric). This means that for each $z = x + iy \in \mathbb{H}^2$, we have an Euclidean metric on $\mathbb{C} \cong \mathbb{R}^2$ (we should think of this $\mathbb{C}$ being rooted at z, and we will call this $\mathbb{C}$ to be T_z, the tangent plane at z) defined by the symmetric matrix

$$\frac{1}{y^2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Given $z_1, z_2 \in \mathbb{H}^2$ and $\gamma \in \mathrm{SL}_2(\mathbb{R})$ satisfying $\gamma.z_1 = z_2$, we associate it a map

$$\mathrm{d}\gamma_{z_1} : T_{z_1} \to T_{z_2}$$
$$u = v + iw \mapsto \mathrm{d}\gamma_{z_1}(u) := \gamma'(z_1) \cdot u.$$

This is compatible with the differential map from multivariable calculus.

Exercise 4.3. $\mathrm{d}\gamma_{z_1}$ *preserves the Euclidean metrics induced by* $\frac{\mathrm{d}x^2+\mathrm{d}y^2}{y^2}$.

Given a metric, one can talk about the area of $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^2$, which is nothing but the area of R as in the lemma above.

Exercise 4.4. *The area of* R *is* $\frac{\pi}{3}$.

Hint: evaluate the integral:

$$\int_{-1/2}^{1/2} \int_{\sqrt{1-x^2}}^{+\infty} \frac{\mathrm{d}x\mathrm{d}y}{y^2}.$$

One may view R as a triangle with one corner sitting at the "infinity". Then its inner angles are $\pi/3, \pi/3, 0$. So we find that

$$\mathrm{Area}(R) = \pi - \pi/3 - \pi/3 - 0$$

which is true for other (hyperbolic) triangles! This is related to Gauss-Bonnet.

5. Local Representation and Genus

Notation.

- A quadratic form refers to some $Q(x, y) = ax^2 + bxy + cy^2$ with $a, b, c \in \mathbb{Z}$ and $\gcd(a, b, c) = 1$.
- $[x]_N$ is the image of an integer x in $\mathbb{Z}/N\mathbb{Z}$.

5.1. **Genus, prelude.** Since $\mathcal{M}_{-20}^{+,\mathrm{red}} = \{x^2 + 5y^2, 2x^2 + 2xy + 3y^2\}$, reduction theory + quadratic reciprocity show that

$$p \equiv 1, 3, 7, 9 \pmod{20} \iff \left(\frac{-5}{p}\right) = 1 \iff p = x^2 + 5y^2 \text{ or } 2x^2 + 2xy + 3y^2. \quad (13)$$

These two forms, however, can be distinguished by calculating their values modulo 20:

$$\{1, 9 \pmod{20}\} = \left\{m \in (\mathbb{Z}/20\mathbb{Z})^\times \;\middle|\; m \equiv x^2 + 5y^2 \pmod{20}\right\}$$
$$\{3, 7 \pmod{20}\} = \left\{m \in (\mathbb{Z}/20\mathbb{Z})^\times \;\middle|\; m \equiv 2x^2 + 2xy + 3y^2 \pmod{20}\right\}.$$

Together with Eq.(13) we deduce that

Theorem 5.1. *Let* p *be an odd prime,* $p \neq 5$. *Then*

$$p \equiv 1, 9 \pmod{20} \iff p = x^2 + 5y^2$$
$$p \equiv 3, 7 \pmod{20} \iff p = 2x^2 + 2xy + 3y^2.$$

Our example suggests that

- the modulo-D-invertible numbers that are represented by $x^2 + ny^2$ is a group;
- for different quadratic forms, the set of invertible-modulo-D representations are either the same or disjoint.

A calculation with $D = -56$ is also in support of this, indeed,

$$p \equiv 1, 9, 15, 23, 25, 39 \pmod{56} \iff p = x^2 + 14y^2 \text{ or } 2x^2 + 7y^2$$
$$p \equiv 3, 5, 13, 19, 27, 45 \pmod{56} \iff p = 3x^2 + 2xy + 5y^2 \text{ or } 3x^2 - 2xy + 5y^2.$$

Definition 5.2. *Given a quadratic form* Q *of discriminant* $D < 0$, *let* $\mathrm{Rep}(Q, \mathrm{mod})$ *be the image of* $\mathrm{Rep}(Q)$ *in* $\mathbb{Z}/D\mathbb{Z}$. *An integer* m *is said to be* ***locally represented by*** Q *if* $[m]_D \in \mathrm{Rep}(Q, \mathrm{mod})$. *Let* $\mathrm{Rep}^\times(Q, \mathrm{mod}) := \mathrm{Rep}(Q, \mathrm{mod}) \cap (\mathbb{Z}/D\mathbb{Z})^\times$. *Also, we define*

$$\mathrm{Genus}(Q) := \left\{Q' \in \mathcal{M}_D^+ \;\middle|\; \mathrm{Rep}^\times(Q', \mathrm{mod}) = \mathrm{Rep}^\times(Q, \mathrm{mod})\right\}$$

to be the **genus** *containing* Q. *The special genus* $\mathrm{Genus}(Q_D^{\mathrm{prin}})$ *containing the principal form is called the* **principal genus**.

We will show that if a prime p coprime to D is locally represented by Q, then it is "globally represented" by one of its genus friend $Q' \in \mathrm{Genus}(Q)$. We use the character $\chi_D : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}$, appearing as corollary to the quadratic reciprocity law.

5.2. **Genus theory.** Caution: though the statement is general, currently the proof is only given in the case $D = -4n$, where $Q_D^{\text{prin}} = x^2 + ny^2$.

Theorem 5.3. *Let $D \equiv 0, 1 \pmod 4$ be a negative integer and $\chi_D : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}$ be the associated character. Then*

(1) *$H_D := \mathrm{Rep}^\times(Q_D^{\text{prin}}, \mathrm{mod})$ is a subgroup of $\ker(\chi_D)$.*

Let Q be a positive definite quadratic form of discriminant D, then

(2) *$\mathrm{Rep}^\times(Q, \mathrm{mod})$ is a coset of H_D in $\ker(\chi_D)$.*

Let $p \nmid D$ be a prime number in $\ker(\chi_D)$.

(3) *If p is locally represented by Q (i.e. $[p]_D \in \mathrm{Rep}^\times(Q, \mathrm{mod})$), then p is globally represented by some genus-friend of Q (i.e. $p \in \mathrm{Rep}(Q')$, for some $Q' \in \mathrm{Genus}(Q)$).*

In part (3), it suffices that p is an integer coprime to D that vanishes along χ_D.

Remark 5.4. *Part (2) of the above theorem shows that $Q \sim_{\text{Genus}} Q' \iff Q' \in \mathrm{Genus}(Q)$ defines an equivalence relation, which is coarser than proper equivalence, on $\mathcal{M}_D^+$. Since every congruence class in $(\mathbb{Z}/D\mathbb{Z})^\times$ contains one prime number (by Dirichlet's theorem on primes in arithmetic progressions, which we do not prove), the above theorem establishes a bijection*

$$\mathcal{M}_D^+/\sim_{\text{Genus}} \cong \ker(\chi_D)/H_D.$$

Since RHS is a group, this suggests a group structure on the left hand side. We will actually construct a group structure on $\mathcal{M}_D^+/\mathrm{SL}_2(\mathbb{Z})$ in the next section, making $[Q] \mapsto \mathrm{Rep}^\times(Q, \mathrm{mod})$ a group homomorphism onto $\ker(\chi_D)/H_D$. The principal genus is nothing but the kernel of this homomorphism:

$$\begin{array}{ccc} \mathcal{M}_D^+/\sim & & \\ \downarrow & \searrow & \\ \mathcal{M}_D^+/\sim_{\text{Genus}} & \xrightarrow[\cong]{} & \ker(\chi_D)/H_D \end{array}$$

In the special case of $D = -4n$, we draw the following corollary.

Corollary 5.5. *Let $n \in \mathbb{Z}^+$ and $p \nmid n$ be an odd prime number. Then ($D := -4n$)*

$$p \in \mathrm{Rep}(Q),\ \exists\, Q \in \mathrm{Genus}(Q_D^{\text{prin}}) \iff p \equiv \beta^2 \text{ or } \beta^2 + n \pmod D,\ \exists\, \beta \in \mathbb{Z}.$$

Proof of $\Longrightarrow$. Write $p \equiv x^2 + ny^2 \pmod D$ for some $x, y \in \mathbb{Z}$. Since

$$x^2 + ny^2 \equiv \begin{cases} x^2 \pmod D & \text{if } y \text{ is even} \\ x^2 + n \pmod D & \text{if } y \text{ is odd} \end{cases},$$

we are done. □

Proof of $\Longleftarrow$. Either case implies that $p \in \mathrm{Rep}(Q_D^{\text{prin}}, \mathrm{mod})$. It only remains to invoke Theorem 5.3.

□

For simplicity we only prove Theorem 5.3 in the special case $D \equiv 0 \pmod 4$. As usual, we write $D = -4n$.

5.2.1. *Proof of Theorem 5.3, (1).* It follows from

$$\begin{aligned} (x + ny^2)(z + nw^2) &= (x + \sqrt{-n}\, y)(x - \sqrt{-n}\, y)(z + \sqrt{-n}\, w)(z - \sqrt{-n}\, w) \\ &= \big((xz - nyw) + \sqrt{-n}\,(xw + yz)\big)\big((xz - nyw) - \sqrt{-n}\,(xw + yz)\big) \\ &= (xz - nyw)^2 + n(xw + yz)^2 \end{aligned}$$

that $\mathrm{Rep}(Q_D^{\text{prin}})$ is closed under multiplication. Therefore, H_D is a subgroup of $(\mathbb{Z}/D\mathbb{Z})^\times$. Next we explain that it is contained in $\ker(\chi_D)$.

Fix some element in H_D, written as $[x^2 + ny^2]_D \in (\mathbb{Z}/D\mathbb{Z})^\times$ for some $x, y \in \mathbb{Z}$ such that $x^2 + ny^2$ is coprime to D. Let $g := \gcd(x, y)$ and write $x = gx_1$, $y = gy_1$ for some coprime integers x_1, y_1. Then

$$\chi_D([x^2 + ny^2]) = \chi_D([x_1^2 + ny_1^2]). \tag{14}$$

Factorize $x_1^2 + ny_1^2 = \prod p_i^{r_i}$. Since D is even and $x^2 + ny^2$ is coprime to D, we have that each p_i is odd. Thus for each i, by Theorem 3.15,

$$p_i \mid x_1^2 + ny_1^2 \implies \left(\frac{-n}{p_i}\right) = 1 \implies \chi_D([p_i]) = 1.$$

Hence $\chi_D([x_1^2+ny_1^2]) = \prod \chi_D([p_i])^{r_i} = 1$. By Eq.(14), $\chi_D([x^2+ny^2]) = 1$ and the proof is complete.

5.2.2. *Proof of Theorem 5.3, (2).* The proof of (2) involves some clever algebra. Write $Q(x,y) = ax^2+bxy+cy^2$. Note that $D \equiv 0 \pmod 4 \implies b$ is an even number.

First we prove (2) under the assumption that c is coprime to D. Then we show that in general it is always possible to find Q' properly equivalent to Q such that the c-coefficient of Q' satisfies this assumption.

Step 1. Assume $\gcd(c,D) = 1$**.** We fix some $c^* \in \mathbb{Z}$ such that $cc^* \equiv 1 \pmod D$. For any $x, y \in \mathbb{Z}$,

$$\begin{aligned} 4c \cdot Q(x,y) &= 4acx^2 + 4bcxy + 4c^2y^2 = (4ac-b^2)x^2 + (b^2x^2+4bcxy+4c^2y^2) \\ &= (bx+2cy)^2 - Dx^2 \\ \implies c \cdot Q(x,y) &= \left(\frac{b}{2}x + cy\right)^2 + nx^2 \qquad (15) \\ \implies Q(x,y) &\equiv c^* \left(\left(\frac{b}{2}x+cy\right)^2 + nx^2\right) \pmod D. \end{aligned}$$

This shows that $\mathrm{Rep}^\times(Q, \mathrm{mod})$ is contained in the coset c^*H_D. To prove the reverse inclusion, fix $z, w \in \mathbb{Z}$ and note that $x := w$ and $y := (z - \frac{b}{2}w)c^*$ satisfy

$$\begin{cases} \frac{b}{2}x + cy \equiv z \pmod D \\ x \equiv w \pmod D \end{cases}.$$

Hence

$$z^2 + nw^2 \equiv cQ(x,y) \pmod D.$$

This shows that $H_D \subset [c] \cdot \mathrm{Rep}^\times(Q, \mathrm{mod})$. And thus $\mathrm{Rep}^\times(Q, \mathrm{mod}) = [c^*]H_D$ is a coset in $(\mathbb{Z}/D\mathbb{Z})^\times$. It only remains to check $\chi_D([c]) = 1$. Since c is positive and odd, we have

$$\chi_D([c]) = \left(\frac{D}{c}\right) = \left(\frac{b^2-4ac}{c}\right) = \left(\frac{b^2}{c}\right) = 1.$$

Step 2. It suffices to show (when $M := D$)

Lemma 5.6. *Let M be an integer. There exist $x, y \in \mathbb{Z}$ such that $Q(x,y)$ is coprime to M.*

Proof. Since $\gcd(a,b,c) = 1$, $Q(1,0) = a$, $Q(1,1) = a+b+c$ and $Q(0,1) = c$, for any prime p, there exists $(x_p, y_p) \in \{(1,0),(1,1),(0,1)\}$ such that $Q(x_p, y_p)$ is coprime to p. Let $p_1, ..., p_r$ be the distinct prime factors of M. By CRT, find $(x,y) \in \mathbb{Z}^2$ satisfying

$$x \equiv x_{p_i} \pmod{p_i}, \quad y \equiv y_{p_i} \pmod{p_i}, \quad \forall\, i = 1, ..., r.$$

Then $Q(x,y) \equiv Q(x_{p_i}, y_{p_i}) \pmod{p_i}$ for each i, implying that $Q(x,y)$ is coprime to each p_i and hence to M.

□

5.2.3. *Proof of Theorem 5.3, (3).* By Lemma 4.9, we can find $Q' \in \mathcal{M}_D^+$ representing p. Thus $p \in \mathrm{Rep}^\times(Q', \mathrm{mod})$. But any two $\mathrm{Rep}^\times(\bullet, \mathrm{mod})$ are either disjoint or the same by part (2) of the theorem. Therefore, $\mathrm{Rep}^\times(Q', \mathrm{mod}) = \mathrm{Rep}^\times(Q, \mathrm{mod})$ and $Q' \in \mathrm{Genus}(Q)$. So we are done.

5.3. **Why only modulo D?** We will explain the following in this subsection:

Theorem 5.7. *Let n be a positive integer and p be a prime number not dividing $4n$ that is represented by x^2+ny^2 modulo $-4n$ (i.e. $[p]_D \in \mathrm{Rep}^\times(x^2+ny^2, \mathrm{mod})$). Then there exists a sequence of $(x_N, y_N)_{N \in \mathbb{Z}^+} \subset \mathbb{Z}^2$ such that*[2]

$$Q(x_N, y_N) \equiv p \pmod N,\ \forall\, N \in \mathbb{Z}^+; \quad (x_N, y_N) \equiv (x_M, y_M) \pmod N,\ \forall\, N \mid M.$$

By Chinese remainder theorem, it suffices to show this for $N = q^k$ for every prime q and positive integer k. There are three types of q that require different treatment

- $q = 2$;
- $q \neq 2$ but $q \mid n$;
- $q \nmid 4n$.

[2] the first one is important, the second one about compatibilities of x_N, y_N can be implied by modifying x_N, y_N.

On the other hand, the proof when

- $k = 1$,
- $k > 1$.

is different.

5.3.1. *Hensel's lemma.* Hensel's lemma is similar to Newton's method of approximating the zero of a differentiable function. It allows us, under some condition, to "lift" modulo-q solutions to modulo-q^k solutions for any $k > 1$. Although this is general, and admittedly, the proof is essentially the same, we shall focus on the case of binary quadratic forms.

Lemma 5.8. *Let k be a positive integer. Q is a quadratic form and m is an integer. Assume $(x_k, y_k) \in \mathbb{Z}^2$ is given such that*

$$Q(x_k, y_k) - m \equiv 0 \pmod{q^k}, \quad \nabla Q(x_k, y_k) \not\equiv 0 \pmod{q}.$$

Then we can find $x_{k+1}, y_{k+1} \in \mathbb{Z}$ satisfying

$$Q(x_{k+1}, y_{k+1}) - m \equiv 0 \pmod{q^{k+1}}, \quad x_{k+1} \equiv x_k \pmod{q^k}, \quad y_{k+1} \equiv y_k \pmod{q^k}.$$

We note that

$$\nabla Q(x, y) = (\frac{\partial Q}{\partial x}(x, y), \frac{\partial Q}{\partial y}(x, y)) = (2ax + by, bx + 2cy).$$

By assumption we find $l \in \mathbb{Z}$ such that $Q(x_k, y_k) = m + q^k l$. For $\alpha \in \mathbb{Z}$,

$$\begin{aligned} Q(x_k + q^k\alpha, y_k) &= Q(x_k, y_k) + a\left((x_k + q^k\alpha)^2 - x_k^2\right) + bq^k\alpha y_k \\ &= m + q^k l + a(2x_k q^k\alpha + q^{2k}\alpha^2) + bq^k\alpha y_k \\ &\equiv m + (l + (2ax_k + by_k)\alpha)q^k \pmod{q^{k+1}} \\ &\equiv m + (l + \frac{\partial Q}{\partial x}(x_k, y_k) \cdot \alpha)q^k \pmod{q^{k+1}}. \end{aligned}$$

If

$$\frac{\partial Q}{\partial x}(x_k, y_k) \not\equiv 0 \pmod{q}$$

then there exists α (the inverse-mod-q of $\frac{\partial Q}{\partial x}(x_k, y_k)$ multiplied by $-l$) such that

$$l + (2ax_k + by_k)\alpha \equiv 0 \pmod{q},$$

implying that

$$Q(x_k + q^k\alpha, y_k) \equiv m \pmod{q^{k+1}}.$$

So we may choose $x_{k+1} := x_k + q^k\alpha$[3], $y_{k+1} := y_k$.

If

$$\frac{\partial Q}{\partial y}(x_k, y_k) \not\equiv 0 \pmod{q},$$

then similar considerations lead to the existence of $\beta \in \mathbb{Z}$ such that $x_{k+1} := x_k$, $y_{k+1} := y_k + q^k\beta$ fulfills the assumption.

Finally, note that at least one of $\frac{\partial Q}{\partial x}(x_k, y_k)$ or $\frac{\partial Q}{\partial y}(x_k, y_k)$ must be nonzero modulo q by assumption.

5.3.2. *Hensel's lemma in general.* We state Hensel's lemma in general here.

Theorem 5.9. *Let q be a prime number, $k \in \mathbb{Z}^+$ and $f \in \mathbb{Z}[X_1, ..., X_n]$ be a polynomial with integral coefficients. Assume that $(x_1, ..., x_n) \in \mathbb{Z}^n$ satisfies*

$$f(x_1, ..., x_n) \equiv 0 \pmod{q^k}, \quad \nabla f(x_1, ..., x_n) \not\equiv \vec{0} \pmod{q}.$$

Then there exists $(y_1, ..., y_n) \in \mathbb{Z}^n$ satisfying

$$f(y_1, ..., y_n) \equiv 0 \pmod{q^{k+1}}, \quad (x_1, ..., x_n) \equiv (y_1, ..., y_n) \pmod{q^k}.$$

Consequently, there exists a sequence of integral vectors $(w_1^j, ..., w_n^j)_{j \geq k} \subset \mathbb{Z}^n$ with

$$f(w_1^j, ..., w_n^j) \equiv 0 \pmod{q^j}, \quad (w_1^{j+1}, ..., w_n^{j+1}) \equiv (w_1^j, ..., w_n^j) \pmod{q^j}.$$

[3]Formally, $x_{k+1} = x_k - q^k \cdot \frac{l}{\frac{\partial Q}{\partial x}(x_k, y_k)} = x_k - \frac{Q(x_k, y_k) - m}{\frac{\partial Q}{\partial x}(x_k, y_k)}$.

5.3.3. *Apply Hensel's lemma.* In applying Lemma 5.8, the key observation is that

$$\nabla Q(x,y) = \begin{bmatrix} 2a & b \\ b & 2c \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = 2 \cdot M_Q \cdot \begin{bmatrix} x \\ y \end{bmatrix}.$$

We will use this in two ways.

Corollary 5.10. *Let n be a nonzero integer and $Q = ax^2 + bxy + cy^2 \in \mathcal{M}_{-4n}$. Take $m \in \mathbb{Z}$ and assume $q \nmid 4n$ is a prime number. Then for $(x_1, y_1) \in \mathbb{Z}^2$, the following implication holds*

$$\begin{aligned} &(x_1, y_1) \not\equiv (0,0) \pmod{q}, \quad Q(x_1, y_1) \equiv m \pmod{q} \\ \Longrightarrow &\exists \{(x_k, y_k)\}_{k \in \mathbb{Z}^+} \subset \mathbb{Z}^2,\ Q(x_k, y_k) \equiv m \pmod{q^k},\ (x_k, y_k) \equiv (x_{k+1}, y_{k+1}) \pmod{q^k}. \end{aligned}$$

Proof. In this case

$$\det \begin{bmatrix} 2a & b \\ b & 2c \end{bmatrix} = -4n$$

is coprime to q and hence this matrix is invertible modulo q. Consequently

$$\nabla Q(x,y) = \begin{bmatrix} 2a & b \\ b & 2c \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

is nonzero modulo q unless $(x, y) \equiv (0,0) \pmod{q}$. But this possibility has been excluded when $x = x_1, y = y_1$. So it remains to apply Hensel's lemma. □

Corollary 5.11. *Let n be a nonzero integer and $Q = ax^2 + bxy + cy^2 \in \mathcal{M}_{-4n}$. Take $m \in \mathbb{Z}$ and a prime number q. Assume m is coprime to $4n$. Then for $(x_1, y_1) \in \mathbb{Z}^2$, the following implication holds*

$$\begin{aligned} &Q(x_1, y_1) \equiv m \pmod{q} \\ \Longrightarrow &\exists \{(x_k, y_k)\}_{k \in \mathbb{Z}^+} \subset \mathbb{Z}^2,\ Q(x_k, y_k) \equiv m \pmod{q^k},\ (x_k, y_k) \equiv (x_{k+1}, y_{k+1}) \pmod{q^k}. \end{aligned}$$

Proof. Indeed

$$(x,y) \cdot \nabla Q(x,y) = (x,y) \cdot \begin{bmatrix} 2a & b \\ b & 2c \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = 2Q(x,y). \tag{16}$$

Thus when $x = x_1, y = y_1$, this is $2m$ modulo q, which is nonzero. So Hensel's lemma can be again applied. □

5.3.4. *The exceptional case $q = 2$.* Hensel's lemma, as stated, does not apply to the case $q = 2$ since $\nabla Q \equiv 0 \pmod{2}$. But it is nonzero (well, still not invertible) modulo higher powers of 2. We now modify the proof of Hensel's lemma to show

Lemma 5.12. *Assume m is coprime to 2 and k is an integer that is at least 3. Assume $(x_k, y_k) \in \mathbb{Z}^2$ satisfies $Q(x_k, y_k) \equiv m \pmod{2^k}$. Then there exists $(x_{k+1}, y_{k+1}) \in \mathbb{Z}^2$ such that*

$$(x_{k+1}, y_{k+1}) \equiv (x_k, y_k) \pmod{2^{k-1}}, \quad Q(x_{k+1}, y_{k+1}) \equiv m \pmod{2^{k+1}}.$$

If we shift the index and set $x'_k := x_{k+1}, y'_k := y_{k+1}$, then

$$Q(x'_k, y'_k) \equiv m \pmod{2^k}, \quad (x'_k, y'_k) \equiv (x'_{k+1}, y'_{k+1}) \pmod{2^k}$$

as before.

Proof. Note that $\nabla Q(x_k, y_k)$ is divisible by 2 and by Eq.(16)

$$\frac{1}{2} \nabla Q(x_k, y_k) \not\equiv (0,0) \pmod{2}.$$

Without loss of generality assume

$$\frac{1}{2} \frac{\partial Q}{\partial x}(x_k, y_k) \not\equiv 0 \pmod{2}.$$

Write $Q(x_k, y_k) = m + 2^k l$ and take $\alpha \in \mathbb{Z}$, then

$$Q(x_k + 2^{k-1}\alpha, y_k) \equiv m + 2^k \left(l + \frac{1}{2} \frac{\partial Q}{\partial x}(x_k, y_k) \cdot \alpha \right) \pmod{2^{k+1}}$$

So the proof is complete by analogous argument applied before. □

5.3.5. *Proof of Theorem 5.7.* Summarizing the efforts so far, we have shown (Lemma 5.12)

$$Q(x,y) \equiv m \pmod 8 \text{ has solution } \implies Q(x,y) \equiv m \pmod{8 \cdot 2^k} \text{ has solution } \forall\, k \in \mathbb{Z}_{\geq 0}$$

and for every odd prime q (Corollary 5.10, 5.11),

$$Q(x,y) \equiv m \pmod q \text{ has solution } \implies Q(x,y) \equiv m \pmod{q^k} \text{ has solution } \forall\, k \in \mathbb{Z}^+.$$

[4] Moreover, the solutions can be made to be compatible with $\mathbb{Z}/q^{k+1}\mathbb{Z} \to \mathbb{Z}/q^k\mathbb{Z}$.

To prove Theorem 5.7, we specialize to the case when $Q = x^2 + ny^2$, $m = p \nmid 4n$ is a prime and it remains to show

1. when n is odd, $x^2 + ny^2 \equiv p \pmod 8$ has a solution if it has a solution modulo 4;
2. for every prime $q \nmid 4n$, $x^2 + ny^2 \pmod q$ "can be any number" (see the precise statement below) in $\mathbb{Z}/q\mathbb{Z}$.

One should be able to do this for general Q, though maybe more complicated.

5.3.6. *Verify 1.* Note that when n is even, $x^2 + ny^2 \equiv p \pmod 8$ already has a solution if $[p] \in \mathrm{Rep}^\times(x^2 + ny^2, \mathrm{mod})$.

Lemma 5.13. *For an odd integer m satisfying $m \equiv x^2 + ny^2 \pmod 4$ for some $x, y \in \mathbb{Z}$, it also satisfies $m \equiv x^2 + ny^2 \pmod 8$ for some $x, y \in \mathbb{Z}$.*

Proof. This is by brutal force. There are only four possibilities for $x^2 + ny^2$ modulo 8:

$$x^2 + y^2,\ x^2 + 3y^2,\ x^2 + 5y^2,\ x^2 + 7y^2.$$

Then

- $\{x^2 + y^2 \pmod 8\}^\times = \{1, 5 \pmod 8\}$;
- $\{x^2 + 3y^2 \pmod 8\}^\times = \{x^2 + 5y^2 \pmod 8\}^\times = \{1, 3, 5, 7 \pmod 8\}$;
- $\{x^2 + 7y^2 \pmod 8\}^\times = (\mathbb{Z}/8\mathbb{Z})^\times$.

One sees that these sets are closed under modulo $4\mathbb{Z}$. □

5.3.7. *Verify 2.*

Lemma 5.14. *Take n to be a nonzero integer and q to be a prime number with $q \nmid D = -4n$, then every integer p is represented by $x^2 + ny^2$ modulo q. Moreover, if $p = q$ is a prime not dividing $4n$ and $[p]_D \in \mathrm{Rep}^\times(x^2 + ny^2, \mathrm{mod})$, then we may choose x, y such that $\gcd(x, y) = 1$.*

Proof. Certainly numbers divided by q are represented. So consider

$$\mathrm{Rep}_q := \left\{ [m] \in (\mathbb{Z}/q\mathbb{Z})^\times \;\middle|\; x^2 + ny^2 \equiv m \pmod q,\ \exists\, x, y \in \mathbb{Z} \right\}.$$

One can prove that Rep_q is a subgroup of $(\mathbb{Z}/q\mathbb{Z})^\times$. By definition, it contains all the quadratic residue modulo q. Thus it is the full $(\mathbb{Z}/q\mathbb{Z})^\times$ once we find some quadratic non-residue in Rep_q. If n is not a quadratic residue then we are done by taking $x = 0$, $y = 1$. Otherwise

$$\mathrm{Rep}_q := \left\{ [m] \in (\mathbb{Z}/q\mathbb{Z})^\times \;\middle|\; x^2 + y^2 \equiv m \pmod q,\ \exists\, x, y \in \mathbb{Z} \right\},$$

showing that $1^2 + 1^2 = 2$ is contained in Rep_q. If 2 is not a quadratic residue then we are done, otherwise (replacing y by $\sqrt{2}y$)

$$\mathrm{Rep}_q := \left\{ [m] \in (\mathbb{Z}/q\mathbb{Z})^\times \;\middle|\; x^2 + 2y^2 \equiv m \pmod q,\ \exists\, x, y \in \mathbb{Z} \right\}.$$

This shows that $1^2 + 2 \cdot 1^2 = 3$ is contained in Rep_q. Continuing this way we must arrive at some quadratic non-residue.

For the part "Moreover,....". Note that

$$x^2 + ny^2 \equiv 0 \pmod q \text{ has a coprime solution } \iff \left(\frac{-n}{q}\right) = 1.$$

But this is true since $[p]_D \in \mathrm{Rep}^\times(x^2 + ny^2, \mathrm{mod})$ (see Theorem 5.3). □

[4] when $q \mid m$, in "having a solution...." we additional require x, y is coprime.

5.3.8. *p-adic integers.* We introduce the notion of p-adic integers and state another equivalent form of Theorem 5.7 in this subsubsection. Such fields are sometimes referred to as local fields ($\mathbb{R}$ is also counted as a local field).

Given a prime number p, we have the following chain of ring homomorphisms

$$.... \to \mathbb{Z}/p^{k+1}\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z} \to .... \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}.$$

Define $\mathbb{Z}_p := \varprojlim(.... \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z})$ to be the inverse limit of this system. More concretely, if $\pi_k : \mathbb{Z}/p^{k+1}\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ denotes the natural projection, then

$$\mathbb{Z}_p = \left\{ (x_{p^k}) \in \prod_{k\in\mathbb{Z}^+} \mathbb{Z}/p^k\mathbb{Z} \;\middle|\; \pi_k(x_{p^{k+1}}) = x_{p^k},\ \forall\, k \in \mathbb{Z}^+ \right\}$$

equipped with the coordinate-wise addition and multiplication. So $\mathbb{Z}_p$ is a ring. Let $\mathbb{Z}_p$ inherit the subspace topology from $\prod_{k\in\mathbb{Z}^+} \mathbb{Z}/p^k\mathbb{Z}$, equipped with the product topology. Each $\mathbb{Z}/p^k\mathbb{Z}$ is assumed to be equipped with the discrete topology. Hence $\mathbb{Z}_p$ is compact. If we define a metric (check that this is indeed a metric!) on the set of integers by

$$|x|_p := p^{-v_p(x)}, \quad v_p(x) := \max\{v \in \mathbb{Z},\ p^v \mid x\}.$$

Then the metric induces the same topology as the inverse limit topology.

As a ring $\mathbb{Z}_p$ has a unique prime ideal $p\mathbb{Z}_p$. If one embeds $\mathbb{Z}$ into $\mathbb{Z}_p$, then the residue field $\mathbb{Z}_p/p\mathbb{Z}_p$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. All ideals of $\mathbb{Z}_p$ are of the form $p^k\mathbb{Z}_p$ whose residue ring is $\mathbb{Z}/p^k\mathbb{Z}$.

Each p-adic integer $x = (x_{p^k}) \in \mathbb{Z}_p$ can be uniquely represented as

$$x = a_0 + a_1 p + a_2 p^2 + ...$$

with $a_i \in \{0, 1, ..., p-1\}$ for each i such that

$$x_{p^k} \equiv \sum_{j=1}^{k-1} a_j p^i \pmod{p^k}.$$

Conversely, given a sequence $(a_k)_{k=0,1,...}$ of $\{0, 1, ..., p-1\}$, the sequence

$$x_{p^k} := \sum_{j=1}^{k-1} a_j p^i \pmod{p^k}$$

satisfies $\pi_k(x_{p^{k+1}}) = x_{p^k}$. And hence it defines a p-adic integer.

Finally, by taking the product space $\mathbb{Z}_f := \prod_{p \text{ primes}} \mathbb{Z}_p$, we get a compact topological ring called "finite integral adele"[5]. Take $\mathbb{Q}_p$ to be the fraction field (which is equipped with a natural topology) of $\mathbb{Z}_p$, one arrives at the topological field: p-adic rationals. By taking the "restricted product space" $\prod'_{p \text{ primes}} \mathbb{Q}_p$ with respect to $\mathbb{Z}_f$, one gets a topological ring $\mathbb{A}_f$ containing $\mathbb{Z}_f$, called "finite adele". The topological ring "adele" $\mathbb{A}_\mathbb{Q}$ is nothing but $\mathbb{R} \times \mathbb{A}_f$.

Theorem 5.7 can be restated as

Theorem 5.15. *Let n be a positive integer and p be a prime number not dividing $4n$ that is represented by $x^2 + ny^2$ modulo $-4n$ (i.e. $[p]_D \in \mathrm{Rep}^\times(x^2 + ny^2, \mathrm{mod})$). Then p is represented by $x^2 + ny^2$ in $\mathbb{Z}_f$.*

6. Composition of quadratic forms

Notation. Although much of the theory generalizes without difficulty to $D \equiv 1 \pmod 4$, we have chosen to focus on the case $D \equiv 0 \pmod 4$, where the b-coefficient is even.

From this subsection on we will fix $n \in \mathbb{Z}^+$, $D := -4n$ and a quadratic form $Q \in \mathcal{M}_D$ will be written as $ax^2 + 2bxy + cy^2$ with $\gcd(a, 2b, c) = 1$ and $ac - b^2 = n$.

6.1. Naive composition of quadratic forms.

Definition 6.1. *Given two quadratic forms $P, Q \in \mathcal{M}_D$, a third quadratic form $R \in \mathcal{M}_D$ is said to be a **naive composition** of P and Q iff there exist two $\mathbb{Z}$-bilinear forms B_1, B_2 on $\mathbb{Z}^2$ such that*

$$P(x, y) \cdot Q(z, w) = R\left(B_1((x, y), (z, w)), B_2((x, y), (z, w))\right).$$

Explicitly, for some $\alpha_i, \beta_i, \eta_i, \theta_i \in \mathbb{Z}$ $(i = 1, 2)$,

$$P(x, y) \cdot Q(z, w) = R\left(\alpha_1 xz + \beta_1 xw + \eta_1 yz + \theta_1 yw, \alpha_2 xz + \beta_2 xw + \eta_2 yz + \theta_2 yw\right). \quad (17)$$

[5] Alternatively, define it to be the inverse limit of $\mathbb{Z}/M\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ as $N \mid M$ varies.

We now show that x^2+ny^2 is a naive composition of Q with itself for any $Q\in\mathcal{M}_D$.

Lemma 6.2. *We have the following identity:*

$$(ax^2+2bxy+cy^2)(az^2+2bzw+cw^2)=(axz+bxw+byz+cyw)^2+n(xw-yz)^2 \tag{18}$$

if $n=ac-b^2$.

Proof. Recall that we showed in last lecture (replace ac by $n+b^2$)

$$(ax^2+2bxy+cy^2)\cdot cw^2=(bx+cy)^2w^2+nx^2w^2.$$

By symmetry

$$(ax^2+2bxy+cy^2)\cdot az^2=(by+ax)^2z^2+ny^2z^2.$$

We also have (split $4b^2$ as $2b^2+(2ac-2n)$)

$$\begin{aligned}(ax^2+2bxy+cy^2)\cdot 2bzw&=\left(2abx^2+(2ac-2n+2b^2)xy+2cby^2\right)\cdot zw\\&=2zw\cdot(ax\cdot bx+ax\cdot cy+bx\cdot by+by\cdot cy)+n\cdot(-2xyzw)\\&=2zw\cdot(ax+by)(bx+cy)+n\cdot(-2xyzw)\end{aligned}$$

Adding them together completes the proof. □

Corollary 6.3. *Let p,q be two prime numbers. Then*

(1) $p,q\equiv 3,\ 7\pmod{20}\implies pq=x^2+5y^2$ *for some* $x,y\in\mathbb{Z}$;
(2) $p\equiv 3\pmod{20}\implies 2p=x^2+5y^2$ *for some* $x,y\in\mathbb{Z}$.

Proof. We have shown that

$$p,q\equiv 3,\ 7\pmod{20}\implies\begin{cases}p=2x^2+2xy+3y^2\\q=2z^2+2zw+3w^2\end{cases}$$

for some $x,y,z,w\in\mathbb{Z}$. Also $2=2\cdot1^2+2\cdot1\cdot0+3\cdot0^2$. It only remains to invoke Lemma 6.2. □

6.2. **Direct composition.** With a little more care, we define

Definition 6.4. *Notation as in Definition 6.1. We say that Q_3 is a* ***direct composition*** *of Q_1,Q_2 provided B_i's can be chosen such that*

$$Q_1(1,0)=\det\begin{pmatrix}\alpha_1&\alpha_2\\\beta_1&\beta_2\end{pmatrix},\quad Q_2(1,0)=\det\begin{pmatrix}\alpha_1&\alpha_2\\\eta_1&\eta_2\end{pmatrix}. \tag{19}$$

We let $\mathrm{Comp}^+(Q_1,Q_2)\subset\mathcal{M}_D$ *collect all possible direct compositions.*

Exercise 6.1. *Check that the composition in Lemma 6.2 is not a direct composition.*

To understand the condition (19), we need

Lemma 6.5. *Notation as in Definition 6.1. In particular $P,Q,R\in\mathcal{M}_D$ with $D=-4n$ for some $n\in\mathbb{Z}^+$. For $i=1,2$, there exists a constant map* $\mathrm{sgn}_i:\mathbb{R}^2\setminus\{(0,0)\}\to\{1,-1\}$ *such that*

$$\begin{aligned}P(x,y)&=\mathrm{sgn}_1(x,y)\det\begin{pmatrix}\alpha_1x+\eta_1y&\alpha_2x+\eta_2y\\\beta_1x+\theta_1y&\beta_2x+\theta_2y\end{pmatrix}.\\Q(z,w)&=\mathrm{sgn}_2(z,w)\det\begin{pmatrix}\alpha_1z+\beta_1w&\alpha_2z+\beta_2w\\\eta_1z+\theta_1w&\eta_2z+\theta_2w\end{pmatrix}.\end{aligned} \tag{20}$$

Proof. Let M_i be the symmetric matrix corresponding to Q_i. Fix x,y and view both sides of Eq.(17) as quadratic forms in z,w. Calculate the discriminant of this quadratic form. By the left hand side we get

$$\mathrm{disc}=Q_1(x,y)^2\cdot\mathrm{disc}(Q_2).$$

From the right hand side we get

$$\begin{aligned}\mathrm{RHS}&=(z,w)\begin{pmatrix}\alpha_1x+\eta_1y&\alpha_2x+\eta_2y\\\beta_1x+\theta_1y&\beta_2x+\theta_2y\end{pmatrix}M_{Q_3}\begin{pmatrix}\alpha_1x+\eta_1y&\alpha_2x+\eta_2y\\\beta_1x+\theta_1y&\beta_2x+\theta_2y\end{pmatrix}^{\mathrm{tr}}\begin{pmatrix}z\\w\end{pmatrix}\\\implies\mathrm{disc}&=\det\begin{pmatrix}\alpha_1x+\eta_1y&\alpha_2x+\eta_2y\\\beta_1x+\theta_1y&\beta_2x+\theta_2y\end{pmatrix}^2\cdot\mathrm{disc}(Q_3)\end{aligned} \tag{21}$$

This proves the first half of Eq.(20) and the second half follows from a similar argument.

To show that $\mathrm{sgn}_i(x,y)$ is independence of (x,y), it suffices to note that $(x,y)\mapsto\mathrm{sgn}_i(x,y)$ is a continuous map from $\mathbb{R}^2\setminus\{(0,0)\}$ to $\{-1,1\}$: the domain being connected forces the image to be connected. □

Lemma 6.6. *Direct compositions are* $\mathrm{SL}_2(\mathbb{Z})$*-stable. More precisely,*

(1) *If* $Q_3 \in \mathrm{Comp}^+(Q_1, Q_2)$ *and* $Q_3' \sim Q_3$ *then* $Q_3' \in \mathrm{Comp}^+(Q_1, Q_2)$*;*
(2) *If* $Q_1' \sim Q_1,\ Q_2' \sim Q_2$*, then* $\mathrm{Comp}^+(Q_1', Q_2') = \mathrm{Comp}^+(Q_1, Q_2)$*.*

Proof of (1). Thanks to Eq.(21), if $Q_3' = {}^{\gamma}Q_3$, then Eq.(17) holds for Q_3 replaced by Q_3' and (B_1, B_2) replaced by

$$(B_1'((x,y),(z,w)), B_2'((x,y),(z,w))) = (z,w)\begin{pmatrix}\alpha_1 x+\eta_1 y & \alpha_2 x+\eta_2 y\\ \beta_1 x+\theta_1 y & \beta_2 x+\theta_2 y\end{pmatrix}\cdot\gamma^{-1}$$

One can verify that B_1', B_2' are still bilinear and the signature stays positive. □

Proof of (2). Say $Q_i' = {}^{\gamma_i}Q_i$ $(i = 1, 2)$ for some $\gamma_i \in \mathrm{SL}_2(\mathbb{Z})$. And Q_3 satisfies Eq.(17) with the correct signature.

One simply replace B_i by

$$B_1'((x,y),(z,w)) := B_1((x,y)\gamma_1,(z,w)\gamma_2), \quad B_2'((x,y),(z,w)) := B_2((x,y)\gamma_1,(z,w)\gamma_2).$$

□

It is a fact that $\mathrm{Comp}^+(Q_1, Q_2)$ consists of a single proper equivalence class. We shall not prove it here and will not use it.

6.3. **Explicit composition.**

Lemma 6.7. *When the middle coefficients coincide, we have the following identity:*

$$(ax^2+2bxy+cy^2)(dz^2+2bzw+fw^2) = adX^2+2bXY+\frac{f}{a}Y^2 \quad \text{if } ac = df$$

where $X := xz - \frac{f}{a}yw$ *and* $Y := axw + dyz + 2byw$*.*

In light of this lemma, we make the following definition.

Definition 6.8. *A pair* (P, Q) *of quadratic forms in* $\mathcal{M}_D$ *is said to be* ***Lagrange-great*** *iff their* a*-coefficients are coprime and* b*-coefficients are the same. Write* $P(x,y) := ax^2+2bxy+cy^2$ *and* $Q(z,w) := dz^2+2bzw+fw^2$*. Then* $a \mid f$ *and we define the* ***explicit composition*** $P \star Q \in \mathcal{M}_D$ *by*

$$P\star Q(x,y) := adx^2+2bxy+\frac{f}{a}y^2.$$

One can check that $P \star Q$ indeed lives in $\mathcal{M}_D$.

Remark 6.9. *By Lemma 6.8,*

$$P\star Q\left(xz+0xw+0yz-\frac{f}{a}yw, 0xz+axw+dyz+byw\right) = P(x,y)\cdot Q(z,w).$$

which shows that $P \star Q$ *is a naive composition since* $a \mid f$*. Since*

$$a = P(1,0) = \det\begin{pmatrix}1&0\\0&a\end{pmatrix},\ d = Q(1,0) = \det\begin{pmatrix}1&0\\0&d\end{pmatrix}$$

the explicit composition is a direct composition.

6.4. **Proof of Lemma 6.8.**

We always replace c by $d\cdot\frac{f}{a}$; f by $a\cdot\frac{f}{a}$ in the proof.

Let us first treat a special case when $b = 0$:

$$\begin{aligned}(ax^2+cy^2)(az^2+fw^2) &= adx^2z^2+afx^2w^2+cdy^2z^2+cfy^2w^2\\ &= adx^2z^2+a^2\frac{f}{a}x^2w^2+d^2\frac{f}{a}y^2z^2+ad\left(\frac{f}{a}\right)^2y^2w^2\\ &= ad(xz-\frac{f}{a}yw)^2+\frac{f}{a}(axw+dyz)^2.\end{aligned}$$

Now we add b-terms into the formula.

$$\begin{aligned}&(ax^2+2bxy+cy^2)(dz^2+2bzw+fw^2)\\ =&ad(xz-\frac{f}{a}yw)^2+\frac{f}{a}(axw+dyz)^2+2bdxyz^2+2ab\frac{f}{a}xyw^2+2abx^2zw+2bd\frac{f}{a}y^2zw+4b^2xyzw\end{aligned}$$

Certainly we expect a middle term $2b(xz-\frac{f}{a}yw)(axw+dyz)$ here. So we continue the above as

$$\begin{aligned}=&ad(xz-\frac{f}{a}yw)^2+\frac{f}{a}(axw+dyz)^2+\cancel{2bdxyz^2}+2ab\frac{f}{a}xyw^2+\cancel{2abx^2zw}+2bd\frac{f}{a}y^2zw+4b^2xyzw\\&+2b(xz-\frac{f}{a}yw)(axw+dyz)\\&\cancel{-2abx^2zw}+2ab\frac{f}{a}xyw^2-\cancel{2bdxyz^2}+2b\frac{f}{a}dy^2zw.\end{aligned}$$

The terms in red and pink are cancelled and we can combine blue terms. We get the above continues as

$$\begin{aligned}=&ad(xz-\frac{f}{a}yw)^2+\frac{f}{a}(axw+dyz)^2+2b(xz-\frac{f}{a}yw)(axw+dyz)\\&+4ab\frac{f}{a}xyw^2+4bd\frac{f}{a}y^2zw+4b^2xyzw\end{aligned}$$

We then hope to add something to $xz-\frac{f}{a}yw$ or $axw+dyz$ so that the blue terms can be absorbed. To obtain the $4b^2xyzw$-term, it seems (to me) a natural choice to replace $axw+dyz$ by $axw+dyz+2byw$. So

$$\begin{aligned}=&ad(xz-\frac{f}{a}yw)^2+\frac{f}{a}(axw+dyz+2byw)^2+2b(xz-\frac{f}{a}yw)(axw+dyz+2byw)\\&-4ab\frac{f}{a}xyw^2-4bd\frac{f}{a}y^2zw-\cancel{4b^2\frac{f}{a}y^2w^2}-4b^2xzyw+\cancel{4b^2\frac{f}{a}y^2w^2}\\&+4ab\frac{f}{a}xyw^2+4bd\frac{f}{a}y^2zw+4b^2xyzw\end{aligned}$$

It turns out that everything is cancelled. So we are done.

6.5. **Form class groups.**

Theorem 6.10. *Fix $n\in\mathbb{Z}^+$ and let $D:=-4n$. For any $[P],[Q]\in\mathcal{M}_D^+/\sim$, choose $P_1\in[P]$ and $Q_1\in[Q]$ such that (P_1,Q_1) is Lagrange-great. We define a map:*

$$\cdot:\mathcal{M}_D^+/\sim\ \times\mathcal{M}_D^+/\sim\to\ \mathcal{M}_D^+/\sim,\quad [P]\cdot[Q]:=[P_1\star Q_1]$$

Then $[P_1\star Q_1]$ is independent of the choice of Lagrange-great pair (P_1,Q_1) and makes $\mathcal{M}_D^+/\sim$ into an abelian group.

Definition 6.11. *Henceforth (when $D=-4n$, $n\in\mathbb{Z}^+$) the set $\mathcal{M}_D^+/\sim$ together with this group structure is referred to as the **form class group** (of discriminant D), denoted as* $\mathbf{Cl}(D)$.

The definition is independent of the choice of (P_1,Q_1).

Lemma 6.12. *Given two Lagrange-great pairs of quadratic form (P_1,Q_1) and (P_2,Q_2) satisfying $P_1\sim P_2$ and $Q_1\sim Q_2$, we have $P_1\star Q_1\sim P_2\star Q_2$.*

6.6. **Proof of Lemma 6.13.** Take P_1,P_2,Q_1,Q_2 as in the lemma. Assume they are given by

$$\begin{aligned}P_1(x,y)=a_1x^2+2b_1xy+c_1y^2,\quad Q_1(z,w)=d_1z^2+2b_1zw+f_1w^2;\\P_2(x,y)=a_2x^2+2b_2xy+c_2y^2,\quad Q_2(z,w)=d_2z^2+2b_2zw+f_2w^2.\end{aligned}$$

By assumption we find $\begin{pmatrix}p&q\\r&s\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z})$ such that

$$\begin{pmatrix}p&q\\r&s\end{pmatrix}\begin{pmatrix}d_2&b_2\\b_2&f_2\end{pmatrix}\begin{pmatrix}p&r\\q&s\end{pmatrix}=\begin{pmatrix}d_1&b_1\\b_1&f_1\end{pmatrix}$$

and we wish to find a conjugation between $\begin{pmatrix}a_1d_1&b_1\\b_1&{a_1}^{-1}f_1\end{pmatrix}$ and $\begin{pmatrix}a_2d_2&b_2\\b_2&{a_2}^{-1}f_2\end{pmatrix}$. This is easy if we allow the transition matrix to be non-integral:

$$\begin{aligned}\begin{pmatrix}a_1d_1&b_1\\b_1&{a_1}^{-1}f_1\end{pmatrix}&=\begin{pmatrix}\sqrt{a_1}&0\\0&\sqrt{a_1}^{-1}\end{pmatrix}\begin{pmatrix}d_1&b_1\\b_1&f_1\end{pmatrix}\begin{pmatrix}\sqrt{a_1}&0\\0&\sqrt{a_1}^{-1}\end{pmatrix}\\&=\begin{pmatrix}\sqrt{a_1}&0\\0&\sqrt{a_1}^{-1}\end{pmatrix}\begin{pmatrix}p&q\\r&s\end{pmatrix}\begin{pmatrix}d_2&b_2\\b_2&f_2\end{pmatrix}\begin{pmatrix}p&r\\q&s\end{pmatrix}\begin{pmatrix}\sqrt{a_1}&0\\0&\sqrt{a_1}^{-1}\end{pmatrix}\\&=\begin{pmatrix}\sqrt{a_1/a_2}p&\sqrt{a_1a_2}q\\\sqrt{a_1a_2}^{-1}r&\sqrt{a_2/a_1}s\end{pmatrix}\begin{pmatrix}a_2d_2&b_2\\b_2&a_2^{-1}f_2\end{pmatrix}\begin{pmatrix}\sqrt{a_1/a_2}p&\sqrt{a_1a_2}q\\\sqrt{a_1a_2}^{-1}r&\sqrt{a_2/a_1}s\end{pmatrix}^{tr}.\end{aligned}$$

We are more likely to succeed provided $a = a_1 = a_2$ where one has

$$\begin{pmatrix} ad_1 & b_1 \\ b_1 & a^{-1}f_1 \end{pmatrix} = \begin{pmatrix} p & aq \\ a^{-1}r & s \end{pmatrix} \begin{pmatrix} ad_2 & b_2 \\ b_2 & a^{-1}f_2 \end{pmatrix} \begin{pmatrix} p & aq \\ a^{-1}r & s \end{pmatrix}^{tr}. \tag{22}$$

This would be a conjugation in $\mathrm{SL}_2(\mathbb{Z})$ if $a \mid r$.

Step 1: the lemma holds assuming $P_1 = P_2$. In this case, $a = a_1 = a_2$, $b = b_1 = b_2$ and $c = c_1 = c_2$. By Eq.(22), it only remains to show $a \mid r$.

To verify this,

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} d_2 & b \\ b & f_2 \end{pmatrix} \begin{pmatrix} p & r \\ q & s \end{pmatrix} = \begin{pmatrix} d_1 & b \\ b & f_1 \end{pmatrix}$$
$$\Longrightarrow \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} d_2 & b \\ b & f_2 \end{pmatrix} = \begin{pmatrix} d_1 & b \\ b & f_1 \end{pmatrix} \begin{pmatrix} s & -r \\ -q & p \end{pmatrix}$$
$$\Longrightarrow \begin{pmatrix} pd_2 + qb & pb + qf_2 \\ rd_2 + sb & rb + sf_2 \end{pmatrix} = \begin{pmatrix} sd_1 - qb & -rd_1 + pb \\ sb - qf_1 & -rb + pf_1 \end{pmatrix}$$

By comparing the $(1,2)$-th entry:

$$qf_2 = -rd_1.$$

Since $a \mid f_2$ and $\gcd(a, d_1) = 1$, we have the required

$$a \mid r.$$

If the proper equivalence takes a special form, we can also construct the desired equivalence.

Notation 6.13. *Given two quadratic forms P_1, P_2, we write $P_1 \sim_{\mathcal{U}} P_2$ iff*

$$P_2(x, y) = P_1\left((x, y)\begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix}\right) \text{ for some } \lambda \in \mathbb{Z}.$$

Concretely, if $P_i = a_i x^2 + 2b_i xy + c_i y^2$ $(i = 1, 2)$, then

$$P_1 \sim_{\mathcal{U}} P_2 \iff a_2 = a_1,\ b_2 = b_1 + a_1\lambda,\ c_2 = c_1 + 2b_1\lambda + a_1\lambda^2,\ \exists\, \lambda \in \mathbb{Z}.$$

Step 2: the lemma holds assuming $P_1 \sim_{\mathcal{U}} P_2$ and $Q_1 \sim_{\mathcal{U}} Q_2$.

So we are assuming there exist $\alpha, \beta \in \mathbb{Z}$ such that

$$b_2 = b_1 + a_1\alpha = b_1 + d_1\beta, \quad c_2 = c_1 + 2b_1\alpha + a_1\alpha^2,\ f_2 = f_1 + 2b_1\beta + d_1\beta^2.$$

Since $\gcd(a_1, d_1) = 1$, by Chinese remainder theorem, there exists $\theta \in \mathbb{Z}$ such that

$$b_2 = b_1 + \theta a_1 d_1.$$

Well, one immediately sees that $\beta = a_1\theta$. We claim that

$$P_2 \star Q_2(x, y) = P_1 \star Q_1\left((x, y)\begin{bmatrix} 1 & 0 \\ \theta & 1 \end{bmatrix}\right),$$

or equivalently and concretely,

$$a_2 d_2 = a_1 d_1, \quad b_2 = b_1 + a_1 d_1 \theta, \quad \frac{f_2}{a_2} = \frac{f_1}{a_1} + 2b_1\theta + a_1 d_1 \theta^2.$$

The first two are already there. The third one follows by noting that $\beta/a_1 = \theta$.

Step 3: the lemma holds assuming a_1, a_2, d_1, d_2 are pairwise coprime. Here we combine the previous two steps.

By Chinese remainder theorem and the coprime assumption, there exist P_i', Q_i' $(i = 1, 2)$ such that

- $P_i \sim_{\mathcal{U}} P_i'$, $Q_i \sim_{\mathcal{U}} Q_i'$ for $i = 1, 2$;
- All P_i', Q_i' $(i = 1, 2)$ have the same b-coefficient;
- the a-coefficients of P_1', P_2', Q_1' and Q_2' are pairwise coprime.

By step 2,

$$P_1 \star Q_1 \sim P_1' \star Q_1', \quad P_2 \star Q_2 \sim P_2' \star Q_2'.$$

By step 1,

$$P_1' \star Q_1' \sim P_1' \star Q_2' \sim Q_1' \star Q_2'.$$

So we are done.

Step 4. The general case.

Arguing in the same way as Lemma 6.15, we can find quadratic forms $P_3(x, y) = a_3 x^2 + 2b_3 xy + c_3 y^2$, $Q_3(z, w) = d_3 z^2 + 2b_3 zw + f_3 w^2$ such that

(1) $P_3 \sim P_1$ and $Q_3 \sim Q_1$;
(2) $\gcd(a_3, a_1 a_2 d_1 d_2) = 1$ and $\gcd(d_3, a_3 a_1 a_2 d_1 d_2) = 1$;

(3) (P_3, Q_3) is a Lagrange-great pair.

Step 3, then, can be applied to the quadruple (P_1, P_3, Q_1, Q_3) and (P_2, P_3, Q_2, Q_3) respectively. Thus,

$$P_1 \star Q_1 \sim P_3 \star Q_3 \sim P_2 \star Q_2.$$

The proof is now complete.

6.6.1. *Associativity.* The existence of Lagrange-great pair and associativity law can be deduced from the following

Lemma 6.14. *Given a triple (P, Q, R) of quadratic forms with the same discriminants, there exist $P_1 \sim P$, $Q_1 \sim Q$, $R_1 \sim R$ that are pairwise Lagrange-great.*

Proof. By Lemma 5.6, we can find $P' \sim P$, $Q' \sim Q$, $R' \sim R$ with pairwise coprime a-coefficients. By performing coordinate change under $x \mapsto x + \lambda y$ and $y \mapsto y$ for suitable $\lambda \in \mathbb{Z}$, we find:

- Each pair $P_1 \sim P$, $Q_1 \sim Q$, $R_1 \sim R$ is proper equivalent and shares the same a-coefficients;
- P_1, Q_1, R_1 have the same b-coefficients.

This completes the proof. □

6.6.2. *Inverse element.*

Lemma 6.15. *Let $Q = ax^2+2bxy+cy^2$ be a quadratic form of discriminant $D = -4n < 0$ and $[Q]$ be its image in $\mathrm{Cl}(D)$. Then $[Q]^{-1} = [Q^-]$ where $Q^- := ax^2 - 2bxy + cy^2$.*

Proof. We can select $Q_1 = a_1x^2+2b_1xy+c_1y^2 \in [Q]$ such that $\gcd(a_1, c_1) = 1$. Indeed, we take $Q_1(x, y) := Q(x+\alpha y, y) = ax^2+2(b+\alpha a)xy+(c+2b\alpha+a\alpha^2)y^2$ for suitable α. Since $\gcd(a, 2b, c) = 1$, there exists $\alpha \in \mathbb{Z}$ such that $\gcd(a, c+2b\alpha+a\alpha^2) = \gcd(a, c+2b\alpha) = 1$.

Thus $Q_2 := \mathcal{T}(Q_1) = c_1x^2 - 2b_1xy + a_1y^2 \in [Q]$ and $Q_1^- = a_1x^2 - 2b_1xy + c_1y^2 \in [Q^-]$.

The pair (Q_1^-, Q_2) is Lagrange-great and their explicit composition $Q_1^- \star Q_1$ is

$$Q_3(x, y) = a_1c_1x^2 - 2b_1xy + y^2,$$

showing that $[Q_3] = [x^2 + ny^2] = \mathrm{id}$. □

6.7. **Example.** $n = 14$. We first list the reduced forms $\mathcal{M}_{-56}^{+,\mathrm{red}}$:

$$A := x^2 + 14y^2,\ B := 2x^2 + 7y^2,\ C := 3x^2 + 2xy + 5y^2,\ D := 3x^2 - 2xy + 5y^2.$$

One notes that $[Q]^{-1}$ can be obtained by negating the signature of b. Thus $[A] = \mathrm{id}$, $[B]^2 = [A]$ and $[C][D] = \mathrm{id}$.

$$\begin{aligned} &3x^2 + 2xy + 5y^2 \sim 5x^2 - 2xy + 3y^2 \sim 3x^2 + 8xy + 10y^2 =: C', \\ &3x^2 + 2xy + 5y^2 \sim 3x^2 + 10xy + 10y^2 =: C'' \\ \Longrightarrow\ &C' \star C'' = 15x^2 + 8xy + 2y^2 \sim 2x^2 - 8xy + 15y^2 \sim 2x^2 + 7y^2. \end{aligned}$$

	[A]	[B]	[C]	[D]
[A]	[A]	[B]	[C]	[D]
[B]	\	[A]	[D]	[C]
[C]	\	\	[B]	[A]
[D]	\	\	\	[B]

TABLE 1. Multiplication table of $\mathbf{Cl}(-56)$

$\mathbf{Cl}(-56)$ is a cyclic group of order 4.

6.8. **[Not discussed in the lecture]Dirichlet composition.** In the rest of this lecture, we will use a slight extension, called Dirichlet composition, of the Lagrange composition. With little extra work, many analogous properties can be established for Dirichlet compositions. More importantly, we will show that up to proper equivalence, direct composition is obtained by Dirichlet composition. This will complete Gauss' claim that any direct composition consists of only one proper equivalence class (see Corollary 6.23).

Definition 6.16. *A pair of quadratic forms $Q_1 = a_1x^2 + 2b_1xy + c_1y^2$ and $Q_2 = a_2x^2 + 2b_2xy + c_2y^2$ is said to be **Dirichlet-good** iff they have the same discriminant $-4n$ for some $n \in \mathbb{Z}^+$ and $\gcd(a_1, a_2, b_1 + b_2) = 1$. If moreover, $b_1 = b_2$ and $a_1 \mid c_2$, $a_2 \mid c_1$, then we say this pair is **Dirichlet-great**.*

Proposition 6.17. *Given a Dirichlet-good pair (Q_1, Q_2), there exists a unique $[B]_{a_1a_2} \in \mathbb{Z}/a_1a_2\mathbb{Z}$ such that*

$$\begin{cases} B \equiv b_1 & (\mathrm{mod}\ a_1) \\ B \equiv b_2 & (\mathrm{mod}\ a_2) \\ B^2 \equiv -n & (\mathrm{mod}\ a_1a_2). \end{cases}$$

For such a $B \in \mathbb{Z}$, we define

$$Q_1 \star_B Q_2 := a_1a_2x^2 + 2Bxy + \frac{B^2 + n}{a_1a_2}y^2.$$

*This is called the **Dirichlet composition** of (Q_1, Q_2).*

Proof will be presented in the next subsection.

Corollary 6.18. *If the pair (Q_1, Q_2) is Dirichlet-good, then there exist $Q_1 \sim_{\mathcal{U}} P_1$ and $Q_2 \sim_{\mathcal{U}} P_2$ such that (P_1, P_2) is Dirichlet-great.*

Proof. Choose B as in Proposition 6.18. Write $B = b_1 + \lambda_1a_1 = b_2 + \lambda_2a_2$ for some $\lambda_i \in \mathbb{Z}$. Then

$$\mathcal{U}^{\lambda_1}(Q_1) = a_1x^2 + 2Bxy + (c_1 + 2b_1\lambda_1 + a_1\lambda_1^2)y^2;$$
$$\mathcal{U}^{\lambda_2}(Q_2) = a_2x^2 + 2Bxy + (c_2 + 2b_2\lambda_2 + a_2\lambda_2^2)y^2.$$
$$\gcd(a_1, a_2, 2B) = \gcd(g, b_1 + \lambda_1a_1 + b_2 + \lambda_2a_2) = \gcd(g, b_1 + b_2) = 1.$$

That $a_2 \mid c_1 + 2b_1\lambda_1 + a_1\lambda_1^2$ follows from the proof of Proposition 6.18. See Eq.(24). □

For a Dirichlet-great pair (Q_1, Q_2), one may simply take $B := b_1 = b_2$ write $Q_1 \star Q_2$, dropping the dependence on B

$$Q_1 \star Q_2 := Q_1 \star_B Q_2 = a_1a_2x^2 + 2Bxy + \frac{c_2}{a_1}y^2.$$

6.9. [Not discussed in the lecture]Proof of Proposition 6.18.

Lemma 6.19. *Given $m, l \in \mathbb{Z}$, write $m = gm'$ and $l = gl'$ where $g := \gcd(m, l)$. Then we have the following exact sequence:*

$$1 \longrightarrow \mathbb{Z}/l'm'g \xrightarrow{\varphi} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z} \xrightarrow{\psi} \mathbb{Z}/g\mathbb{Z} \to 1$$

where $\varphi : [x]_{l'm'g} \to ([x]_m, [x]_l)$ and $\psi : ([x]_m, [y]_l) \mapsto [x - y]_g$.

Proof. It is rather direct to show that $\psi \circ \varphi = 1$. It remains to show $\ker\psi \subset \mathrm{Im}\,\varphi$. Say $[x]_m, [y]_l$ is such that $[x]_g = [y]_g$, we must show $([x], [y]) \in \mathrm{Im}\,\varphi$.

Since $\gcd(m', l') = 1$, we can find $\lambda \in \mathbb{Z}$ such that

$$m'\lambda \equiv \frac{y - x}{g} \pmod{l'}.$$

Multiplying by g, we get

$$m\lambda \equiv y - x \pmod{l}.$$

Setting $z := m\lambda + x$, we get $\varphi([z]_L) = ([x], [y])$. □

We turn to the proof of Proposition 6.18. Let $g := \gcd(a_1, a_2)$ and write $a_1 = ga_1'$, $a_2 = ga_2'$. Since both forms have the same discriminant:

$$a_1c_2 - b_1^2 = a_2c_2 - b_2^2 \implies (b_1 - b_2)(b_1 + b_2) \equiv 0 \pmod{g} \implies b_1 - b_2 \equiv 0 \pmod{g}.$$

The last implication is due to $\gcd(a_1, a_2, b_1 + b_2) = 1$. By Lemma 6.20, we find $B_1 \in \mathbb{Z}$ such that

$$B_1 \equiv b_1 \pmod{a_1}, \quad B_1 \equiv b_2 \pmod{a_2}.$$

It remains to find $\lambda \in \mathbb{Z}$ such that

$$(B_1 + \lambda g a_1' a_2')^2 = -n \pmod{a_1a_2}. \tag{23}$$

We write $B_1 = b_1 + \lambda_1a_1$, then[6]

$$-n = B_1^2 - a_1(c_1 + \lambda_1 2b_1 + \lambda_1^2 a_1).$$

[6]This is computing the discriminant of $\mathcal{U}^{\lambda_1}(Q_1)$.

Therefore,

$$\begin{aligned} -b &\equiv b_2^2 - a_1(c_1 + \lambda_1 2b_1 + \lambda_1^2 a_1) \pmod{a_2} \\ \implies 0 &\equiv a_2 c_2 \equiv -a_1(c_1 + \lambda_1 2b_1 + \lambda_1^2 a_1) \pmod{a_2} \\ \implies 0 &\equiv -a_1'(c_1 + \lambda_1 2b_1 + \lambda_1^2 a_1) \pmod{a_2'} \\ \implies 0 &\equiv c_1 + \lambda_1 2b_1 + \lambda_1^2 a_1 \pmod{a_2'}. \end{aligned} \tag{24}$$

Replacing $-n$ in Eq.(23) by $B_1^2 - a_1(c_1 + \lambda_1 2b_1 + \lambda_1^2 a_1)$, it only remains to show

$$2B_1 \lambda g a_1' a_2' \equiv -a_1(c_1 + \lambda_1 2b_1 + \lambda_1^2 a_1) \pmod{a_1 a_2}$$

Dividing both sides by a_1, this would be a consequence of

$$2B_1 \lambda a_2' \equiv -(c_1 + \lambda_1 2b_1 + \lambda_1^2 a_1) \pmod{a_2}$$

Thanks to Eq.(24), we can divide by a_2' on both sides and this is further reduced to

$$2B_1 \lambda \equiv -\frac{c_1 + \lambda_1 2b_1 + \lambda_1^2 a_1}{a_2'} \pmod{g}$$

which can be solved because $\gcd(2B_1, g) = \gcd(b_1 + b_2, a_1, a_2) = 1$. This completes the proof of existence of B.

Proof of Uniqueness. It is likely that the uniqueness can already be extracted from the proof above. Or, if B' has the same properties as B, then

$$B' \equiv B \pmod{g a_1' a_2'}, \quad B'^2 \equiv -n \pmod{a_1 a_2}.$$

Write $B' := B + \lambda g a_1' a_2'$ and we need to show $g \mid \lambda$.

$$\begin{aligned} &(B + \lambda g a_1' a_2')^2 \equiv -n \pmod{a_1 a_2} \\ \implies &2B\lambda g a_1' a_2' \equiv 0 \pmod{a_1 a_2} \\ \implies &2B\lambda \equiv 0 \pmod{g}. \end{aligned}$$

But $\gcd(g, 2B) = 1$, so $\lambda \equiv 0 \pmod{g}$ as desired. □

6.10. **[Not discussed in the lecture]Proper equivalence between Dirichlet compositions.** Similar to Lagrange compositions, we have

Lemma 6.20. *For two Dirichlet-great pairs (P_1, P_2) and (Q_1, Q_2), if $P_1 \sim Q_1$ and $P_2 \sim Q_2$, then $P_1 \star_B P_2 = Q_1 \star_{B'} Q_2$ for any choices of B, B' as in the definition of Dirichlet compositions.*

This follows from the same proof of Lemma 6.13. The proof of $a_1 \mid r$ causes a little more trouble, but the rest remains the same.

6.11. **[Not discussed in the lecture]Direct compositions and Dirichlet composition.**

Theorem 6.21. *Let $n \in \mathbb{Z}^+$ and $D = -4n$. Take $P_1, P_2 \in \mathcal{M}_D$ and $P_3 \in \mathrm{Comp}^+(P_1, P_2)$. Then there exists $Q_1 \sim P_1$, $Q_2 \sim P_2$, $Q_3 \sim P_3$ such that (Q_1, Q_2) is Dirichlet-great and $Q_3 = Q_1 \star Q_2$.*

Corollary 6.22. *Let $n \in \mathbb{Z}^+$ and $D = -4n$. For every pair $P_1, P_2 \in \mathcal{M}_D$, $\mathrm{Comp}^+(P_1, P_2)$ consists of exactly one proper equivalence class.*

6.12. **[Not discussed in the lecture]Proof of Theorem 6.22.** By assumption, there is an integral matrix

$$\mathscr{B} = \begin{pmatrix} \alpha_1 & \beta_1 & \eta_1 & \theta_1 \\ \alpha_2 & \beta_2 & \eta_2 & \theta_2 \end{pmatrix}$$

such that

$$\begin{aligned} P_1(x,y)P_2(z,w) &= P_3\left((\alpha_1 xz + \beta_1 xw + \eta_1 yz + \theta_1 yw, \alpha_2 xz + \beta_2 xw + \eta_2 yz + \theta_2 yw)\right) \\ &= P_3\left((z,w)\left(\begin{pmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{pmatrix} x + \begin{pmatrix} \eta_1 & \eta_2 \\ \theta_1 & \theta_2 \end{pmatrix} y\right)\right) \\ &= P_3\left((x,y)\left(\begin{pmatrix} \alpha_1 & \alpha_2 \\ \eta_1 & \eta_2 \end{pmatrix} z + \begin{pmatrix} \beta_1 & \beta_2 \\ \theta_1 & \theta_2 \end{pmatrix} w\right)\right). \end{aligned}$$

Also, recall that if $\gamma_1, \gamma_2, \gamma_3 \in \mathrm{SL}_2(\mathbb{Z})$, then ${}^{\gamma_3}P_3 \in \mathrm{Comp}^+({}^{\gamma_1}P_1, {}^{\gamma_2}P_2)$ and the $\mathscr{B}$ is transformed by[7]

$$(\gamma_1, \gamma_3): \ \gamma_1 \begin{pmatrix} \alpha_1 & \alpha_2 \\ \eta_1 & \eta_2 \end{pmatrix} \gamma_3, \ \gamma_1 \begin{pmatrix} \beta_1 & \beta_2 \\ \theta_1 & \theta_2 \end{pmatrix} \gamma_3;$$
$$(\gamma_2, \gamma_3): \ \gamma_2 \begin{pmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{pmatrix} \gamma_3, \ \gamma_2 \begin{pmatrix} \eta_1 & \eta_2 \\ \theta_1 & \theta_2 \end{pmatrix} \gamma_3.$$

We denote by ${}^{\gamma}\mathcal{B}$ the resulting (coefficients of the) bilinear form. Choose $\gamma_1, \gamma_2, \gamma_3$ such that

- $\min\{|\alpha_1|, |\alpha_2|, ..., |\theta_2|\}$ is as small as possible.

Modifying γ_i's by certain permutations we can further arrange that

- $\alpha_1 > 0$ and $\alpha_1 = \min\{|\alpha_1|, ..., |\theta_2|\}$.

Claim 6.23. $\alpha_1 = 1$.

Proof. Some immediate observation:

- $\alpha_1 \mid \eta_1$: otherwise we apply suitable γ_1 to get something strictly smaller;
- $\alpha_1 \mid \beta_1$: otherwise apply γ_2;
- $\alpha_1 \mid \alpha_2$: otherwise apply γ_3.

Actually we may and do modify $\gamma_1, \gamma_2, \gamma_3$ by certain unipotent matrices such that $\eta_1 = \beta_1 = \alpha_2 = 0$.

It is also not hard to see that $\alpha_1 \mid \eta_1$ via (γ_1, γ_3)-action and $\alpha_1 \mid \beta_2$ via (γ_2, γ_3)-action.

Recall that, by the definition of direct composition and Lemma 6.6, we have (write $Q_i := {}^{\gamma_i}P_i$)

$$Q_2(1,0) = \alpha_1\eta_2, \ Q_2(0,1) = -\theta_1\beta_2, \ Q_2(1,1) = \det \begin{pmatrix} \alpha_1 & \beta_2 \\ \theta_1 & \theta_2 + \eta_2 \end{pmatrix}.$$

Since Q_2 is primitive, the above three numbers must have $\gcd = 1$. But α_1 divides all of them, so $\alpha_1 = 1$.

□

If we write $Q_i = a_i x^2 + 2b_i xy + c_i y^2$, then we get

$$\eta_2 = Q_2(1,0) = a_2, \ -\beta_2\theta_1 = Q_2(0,1) = c_2, \ \beta_2 = Q_1(1,0) = a_1, \ -\eta_2\theta_1 = Q_1(0,1) = c_1.$$

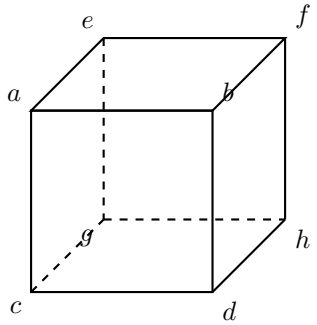
Thus $c_2 = -a_1\theta_1$ and $c_1 = -a_2\theta_1$. This shows that $a_1 \mid c_2$, $a_2 \mid c_1$ and

$$a_2 + 2b_2 + c_2 = P_2(1,1) = \det \begin{pmatrix} 1 & a_1 \\ \theta_1 & a_2 + \theta_2 \end{pmatrix} = a_2 + \theta_2 - a_1\theta_1$$
$$a_1 + 2b_1 + c_1 = P_2(1,1) = \det \begin{pmatrix} 1 & a_2 \\ \theta_1 & a_1 + \theta_2 \end{pmatrix} = a_1 + \theta_2 - a_2\theta_1$$
$$\Longrightarrow b_1 = b_2 =: b, \ \theta_2 = 2b.$$

This shows that (Q_1, Q_2) is Dirichlet-great and $Q_3 = Q_1 \star Q_2$ by Lemma 6.8 and

$${}^{\gamma}\mathcal{B} = \begin{pmatrix} 1 & 0 & 0 & -\frac{c_1}{a_1} \\ 0 & a_1 & a_2 & 2b \end{pmatrix}.$$

6.13. **Bhargava's cube.** Bhargava found yet another way of understanding composition law. He associates three quadratic forms to a cube with labelled vertices. Let us be given a cube $\mathcal{C}$ (which is really eight integers arranged in a special way):

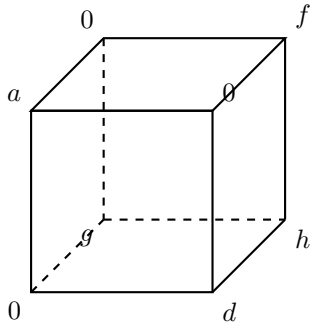


[7] Though it is not necessary to know this, but the action of γ_1 and γ_2 commutes.

By slicing the cube in different ways, define

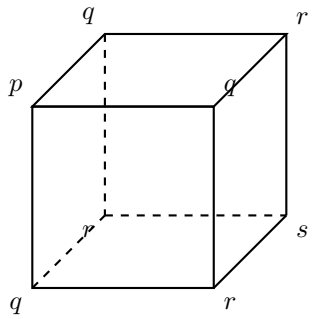
$$\begin{aligned}
\text{front-back}: &\quad P_{\mathcal{C}}(x,y) := -\det\left(x\begin{bmatrix}a & b\\ c & d\end{bmatrix} - y\begin{bmatrix}e & f\\ g & h\end{bmatrix}\right)\\
\text{left-right}: &\quad Q_{\mathcal{C}}(x,y) := -\det\left(x\begin{bmatrix}a & e\\ c & g\end{bmatrix} - y\begin{bmatrix}b & f\\ d & h\end{bmatrix}\right)\\
\text{top-bottom}: &\quad R_{\mathcal{C}}(x,y) := -\det\left(x\begin{bmatrix}a & b\\ e & f\end{bmatrix} - y\begin{bmatrix}c & d\\ g & h\end{bmatrix}\right)
\end{aligned}$$

A few examples: take $\mathcal{C}$ to be



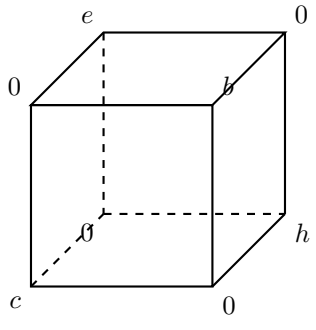
$$\begin{aligned}
\text{front-back}: &\quad P_{\mathcal{C}}(x,y) := -\det\left(x\begin{bmatrix}a & 0\\ 0 & d\end{bmatrix} - y\begin{bmatrix}0 & f\\ g & h\end{bmatrix}\right) = -adx^2 + ahxy + gfy^2\\
\text{left-right}: &\quad Q_{\mathcal{C}}(x,y) := -\det\left(x\begin{bmatrix}a & 0\\ 0 & g\end{bmatrix} - y\begin{bmatrix}0 & f\\ d & h\end{bmatrix}\right) = -agx^2 + ahxy + dfy^2\\
\text{top-bottom}: &\quad R_{\mathcal{C}}(x,y) := -\det\left(x\begin{bmatrix}a & 0\\ 0 & f\end{bmatrix} - y\begin{bmatrix}0 & d\\ g & h\end{bmatrix}\right) = -afx^2 + ahxy + dgy^2.
\end{aligned}$$

Take $\mathcal{C}$ to be



$$\begin{aligned}
\text{front-back}: &\quad P_{\mathcal{C}}(x,y) := -\det\left(x\begin{bmatrix}p & q\\ q & r\end{bmatrix} - y\begin{bmatrix}q & r\\ r & s\end{bmatrix}\right)\\
\text{left-right}: &\quad Q_{\mathcal{C}}(x,y) := -\det\left(x\begin{bmatrix}p & q\\ q & r\end{bmatrix} - y\begin{bmatrix}q & r\\ r & s\end{bmatrix}\right)\\
\text{top-bottom}: &\quad R_{\mathcal{C}}(x,y) := -\det\left(x\begin{bmatrix}p & q\\ q & r\end{bmatrix} - y\begin{bmatrix}q & r\\ r & s\end{bmatrix}\right)\\
\text{All equal to} &\quad (q^2 - pr)x^2 + (ps - qr)xy + (r^2 - qs)y^2.
\end{aligned}$$

Last one. Take $\mathcal{C}$ to be:



Then

$$\begin{aligned}
\text{front-back}: \quad & P_{\mathcal{C}}(x,y) := -\det\left(x\begin{bmatrix}0 & b\\ c & 0\end{bmatrix} - y\begin{bmatrix}e & 0\\ 0 & h\end{bmatrix}\right) = bcx^2 - ehy^2\\
\text{left-right}: \quad & Q_{\mathcal{C}}(x,y) := -\det\left(x\begin{bmatrix}0 & e\\ c & 0\end{bmatrix} - y\begin{bmatrix}b & 0\\ 0 & h\end{bmatrix}\right) = cex^2 - bhy^2\\
\text{top-bottom}: \quad & R_{\mathcal{C}}(x,y) := -\det\left(x\begin{bmatrix}0 & b\\ e & 0\end{bmatrix} - y\begin{bmatrix}c & 0\\ 0 & h\end{bmatrix}\right) = bex^2 - chy^2
\end{aligned}$$

When $e = b = c = 1$, $h = -n$, we get

$$P_{\mathcal{C}} = Q_{\mathcal{C}} = R_{\mathcal{C}} = x^2 + ny^2.$$

6.13.1. *Group law.* The idea is that the proper equivalence class of $P + Q + R$ should be equal to the identify in the abelian group.

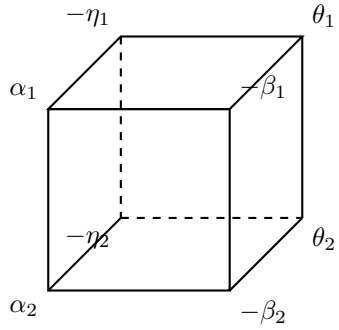
Definition 6.24. *Let $\mathbf{Cl}_{Bhar}(D)$ be the quotient of the free abelian group $\bigoplus_{Q\in\mathcal{M}_D^+}\mathbb{Z}.Q$ by the subgroup generated by $P_{\mathcal{C}}+Q_{\mathcal{C}}+R_{\mathcal{C}}$ as $\mathcal{C}$ varies such that all $P_{\mathcal{C}}$, $Q_{\mathcal{C}}$ and $R_{\mathcal{C}}$ belong to $\mathcal{M}_D^+$.*

Theorem 6.25. *The natural map from $\bigoplus_{Q\in\mathcal{M}_D^+}\mathbb{Z}.Q$ to $\mathbf{Cl}(D)$ descends to an isomorphism $\mathbf{Cl}_{Bhar}(D) \cong \mathbf{Cl}(D)$.*

6.13.2. *Hints from direct composition.* Recall that if R is a direct composition of P and Q, then by Lemma 6.6,

$$\begin{aligned}
P(x,y) &= \det\begin{pmatrix}\alpha_1 x + \eta_1 y & \alpha_2 x + \eta_2 y\\ \beta_1 x + \theta_1 y & \beta_2 x + \theta_2 y\end{pmatrix} = \det\left(x\begin{pmatrix}\alpha_1 & \alpha_2\\ \beta_1 & \beta_2\end{pmatrix} + y\begin{pmatrix}\eta_1 & \eta_2\\ \theta_1 & \theta_2\end{pmatrix}\right)\\
Q(z,w) &= \det\begin{pmatrix}\alpha_1 z + \beta_1 w & \alpha_2 z + \beta_2 w\\ \eta_1 z + \theta_1 w & \eta_2 z + \theta_2 w\end{pmatrix} = \det\left(z\begin{pmatrix}\alpha_1 & \alpha_2\\ \eta_1 & \eta_2\end{pmatrix} + w\begin{pmatrix}\beta_1 & \beta_2\\ \theta_1 & \theta_2\end{pmatrix}\right).
\end{aligned}$$

Thus if we consider the cube $\mathcal{C}$,



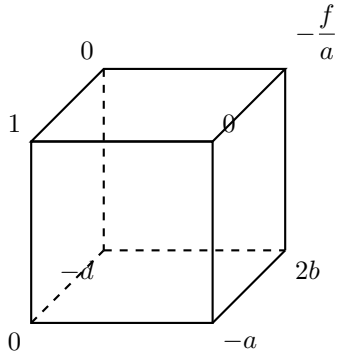
Then $P_{\mathcal{C}} = P$ and $Q_{\mathcal{C}} = Q$. Thus we expect that the proper equivalence class of $R_{\mathcal{C}}$ is $[R]^{-1}$. But it seems difficult to check.

6.13.3. *Explicit composition.* Working with explicit composition is much easier. Here we explain that for a Lagrange-great pair (P, Q), there exists a cube $\mathcal{C}$ such that

$$P = P_{\mathcal{C}}, \quad Q = Q_{\mathcal{C}}, \quad (P \star Q)^- \sim R_{\mathcal{C}}.$$

The notation $()^-$ means to negate the b-coefficient.

So this time our cube $\mathcal{C}$ is



$$\begin{aligned} R_{\mathcal{C}}(X,Y) &= -\det\left(X\begin{bmatrix}1 & 0\\ 0 & -f/a\end{bmatrix} - Y\begin{bmatrix}0 & -a\\ -d & 2b\end{bmatrix}\right)\\ &= -\det\begin{bmatrix}X & aY\\ dY & -\frac{f}{a}X - 2bY\end{bmatrix}\\ &= \frac{f}{a}X^2 + 2bXY + adY^2 \sim adX^2 - 2bXY + \frac{f}{a}Y^2, \end{aligned}$$

which is the negation of R.

6.13.4. $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$-*action on cubes.* Recall that we defined $\mathrm{SL}_2(\mathbb{Z})$-action on quadratic forms as follows. Let $\gamma = \begin{bmatrix}p & q\\ r & s\end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Then

$$(\gamma, Q) \mapsto (\gamma.Q)(x,y) := Q((x,y).\gamma) = Q(px+ry, qx+sy).$$

So when the quadratic from $Q = P_{\mathcal{C}}$ is coming from a cube, then

$$\begin{aligned} \gamma.P_{\mathcal{C}}(x,y) &:= -\det\left((px+ry)\begin{bmatrix}a & b\\ c & d\end{bmatrix} - (qx+sy)\begin{bmatrix}e & f\\ g & h\end{bmatrix}\right)\\ &= -\det\left(x\cdot\left(p\begin{bmatrix}a & b\\ c & d\end{bmatrix} + q\begin{bmatrix}e & f\\ g & h\end{bmatrix}\right) - y\cdot\left(r\begin{bmatrix}a & b\\ c & d\end{bmatrix} + s\begin{bmatrix}e & f\\ g & h\end{bmatrix}\right)\right) \end{aligned}$$

Inspired by this, define $\mathrm{SL}_2(\mathbb{Z})$-action on cubes by changing its front-back matrices:

$$\left(\begin{bmatrix}a & b\\ c & d\end{bmatrix}, \begin{bmatrix}e & f\\ g & h\end{bmatrix}\right) \mapsto \left(p\begin{bmatrix}a & b\\ c & d\end{bmatrix} + q\begin{bmatrix}e & f\\ g & h\end{bmatrix}, r\begin{bmatrix}a & b\\ c & d\end{bmatrix} + s\begin{bmatrix}e & f\\ g & h\end{bmatrix}\right)$$

and let $\gamma.\mathcal{C}$ be the new cube. Then $P_{\gamma.\mathcal{C}} = \gamma.P_{\mathcal{C}}$. It is also direct to check that $Q_{\gamma.\mathcal{C}} = Q_{\mathcal{C}}$ and $R_{\gamma.\mathcal{C}} = R_{\mathcal{C}}$. In particular, this shows that in $\mathbf{Cl}_{Bhar}(D)$, $[\gamma.P_{\mathcal{C}}] = [P_{\mathcal{C}}]$.[8]

Likewise, we define $\mathrm{SL}_2(\mathbb{Z})$-action by changing left-right or top-bottom matrices. These actions commute with each other, so we end up with a $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$-action on cubes.

Let me note that a proof of Theorem 6.26 can be obtained by combining discussions so far.

Sketch of proof of Theorem 6.26 . We need to check that for every " primitive cube" $\mathcal{C}$,

$$[P_{\mathcal{C}}] \cdot [Q_{\mathcal{C}}] \cdot [R_{\mathcal{C}}] = \text{identity} \tag{25}$$

in $\mathbf{Cl}(D)$. By discussion above, it suffices to check this for some $\mathcal{C}'$ in the $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$-orbit of $\mathcal{C}$. Since gcd of the eight integers must be 1, we can find $\mathcal{C}'$ such that its a equals 1. Then one can use this to eliminate adjacent vertices b, e, c. For such a cube, the verification of Eq.(25) requires a slight generalization of explicit composition, which is left to the reader.

Then it only remains to check the descending morphism is injective. This follows by noting that every P is of the form $P_{\mathcal{C}}$ for some $\mathcal{C}$ and for any γ,

$$\begin{aligned} &[P_{\mathcal{C}}]_{Bhar} + [Q_{\mathcal{C}}]_{Bhar} + [R_{\mathcal{C}}]_{Bhar} = 0, \quad [\gamma P_{\mathcal{C}}]_{Bhar} + [Q_{\mathcal{C}}]_{Bhar} + [R_{\mathcal{C}}]_{Bhar}\\ &\implies [P_{\mathcal{C}}]_{Bhar} = [\gamma P_{\mathcal{C}}]_{Bhar}. \end{aligned}$$

□

Finally,

Theorem 6.26. *There is a group law on* $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$*-orbits of primitive cubes (that is, the associated quadratic forms are primitive) such that if* $[\mathcal{C}_1] \cdot [\mathcal{C}_2] = [\mathcal{C}_3]$*, then*

$$[P_{\mathcal{C}_1}] \cdot [P_{\mathcal{C}_2}] = [P_{\mathcal{C}_3}], \quad [Q_{\mathcal{C}_1}] \cdot [Q_{\mathcal{C}_2}] = [Q_{\mathcal{C}_3}], \quad [R_{\mathcal{C}_1}] \cdot [R_{\mathcal{C}_2}] = [R_{\mathcal{C}_3}].$$

7. Genus theory II

Recall $\mathcal{M}_D^+/\sim$ equipped with the group structure is denoted as $\mathrm{Cl}(D)$.

[8] That every quadratic form P is of the form $P_{\mathcal{C}}$ can be deduced from results on Lagrange-great pairs.

7.1. **2-torsion elements in class groups.**

Lemma 7.1. *Let $D = -4n$ for some $n \in \mathbb{Z}^+$. Take $Q = ax^2 + 2bxy + cy^2 \in \mathcal{M}_D^{\mathrm{red},+}$. Then*

$$[Q] \in \mathbf{Cl}(D) \text{ has order } \leq 2 \iff b = 0 \text{ or } a = 2b \text{ or } a = c.$$

Proof. $[Q]$ has order ≤ 2 iff its inverse is equal to itself, that is, iff

$$Q = ax^2 + 2bxy + cy^2 \sim Q^- = ax^2 - 2bxy + cy^2.$$

Let us first assume $[Q] \in \mathbf{Cl}(D)$ has order two. If $|2b| < a < c$, then Q^- is reduced and hence $Q = Q^-$ by uniqueness of reduced forms, implying $b = 0$.

If $|2b| = a$, then $2b = a$ by the definition of reduced forms.

If $a = c$, then we are also done.

Conversely, we must show $Q \sim Q^-$ when $b = 0$ or $a = 2b$ or $a = c$. Indeed, $b = 0 \implies Q = Q^-$, $a = 2b \implies Q^- = \mathcal{U}^{-1}(Q)$ and $a = c \implies Q^- = \mathcal{T}(Q)$. So we have $Q \sim Q^-$ in each case. □

Notation 7.2. *Given an abelian group A, let $A[2]$ be the 2-torsion subgroup: $\{a \in A,\ a^2 = 1\}$.*

By Subsection 4.9, 2-torsion elements are those on the boundary of the fundamental domain or whose real parts are zero.

Using the above lemma, it's possible to obtain nontrivial information about $\mathbf{Cl}(D)$. Here is one example

Example 7.3. $\mathbf{Cl}(-164) \cong \mathbb{Z}/8\mathbb{Z}$.

Proof. By listing all reduced forms

$$1x^2 + 0xy + 41y^2;\ 2x^2 + 2xy + 21y^2;\ 3x^2 - 2xy + 14y^2;\ 3x^2 + 2xy + 14y^2;$$
$$5x^2 - 4xy + 9y^2;\ 5x^2 + 4xy + 9y^2;\ 6x^2 - 2xy + 7y^2;\ 6x^2 + 2xy + 7y^2,$$

we find $\#\,\mathbf{Cl}(-164) = 8$ and that there is only one element of order 2. This gives the conclusion. □

It is direct to see that $\#\,\mathbf{Cl}(D)[2]$ is a power of 2. By further computation, we can find

Proposition 7.4. *Let $D = -4n$ for some $n \in \mathbb{Z}^+$. Let r be the number of distinct odd prime numbers dividing D. Define*

$$\mu := \begin{cases} r & n \equiv 3 \pmod 4 \\ r+1 & n \equiv 1, 2 \pmod 4 \\ r+1 & n \equiv 4 \pmod 8 \\ r+2 & n \equiv 0 \pmod 8 \end{cases}.$$

Then $\#\,\mathbf{Cl}(D)[2] = 2^{\mu - 1}$.

7.2. **Proof of Proposition 7.4.** Without loss of generality, we shall assume $n \geq 2$. Elements in $\mathcal{M}_{-4n}^{\mathrm{red},+} \cap \mathbf{Cl}(D)[2]$ can be divided into three disjoint types by Lemma 7.1:

Type 1. $ax^2 + cy^2$ with $0 < a < c$, $a, c \in \mathbb{Z}$, $\gcd(a, c) = 1$, $ac = n$;
Type 2. $2bx^2 + 2bxy + cy^2$ with $b, c \in \mathbb{Z}^+$, $2b < c$, $\gcd(b, c) = 1$, c is odd and $(2c - b)b = n$;
Type 3. $ax^2 + 2bxy + ay^2$ with $a, b \in \mathbb{Z}^+$, $2b < a$, $\gcd(a, b) = 1$, a is odd and $a^2 - b^2 = n$.

Type 1 forms are in bijection with

$$\text{Type 1} \cong \left\{(a, c) \in \mathbb{Z}^2 \;\middle|\; 0 < a < c,\ \gcd(a, c) = 1,\ ac = n\right\}.$$

So its cardinality is nothing but all possible ways of dividing distinctive prime factors of n into two parts: allowing one of them to be empty. Thus,

$$\#\text{Type 1} = \begin{cases} 2^{r-1} & \text{if } n \text{ is odd.} \\ 2^r & \text{if } n \text{ is even.} \end{cases}$$

Type 2 and 3 elements are more complicated and will be considered together.

Note that sending $(b, c) \mapsto (l, m) := (b, 2c - b)$ gives a bijection (with the inverse being $(l, m) \mapsto (b, c) := (l, (l + m)/2)$) between

$$\left\{(b, c) \in \mathbb{R}^2 \;\middle|\; n = b(2c - b),\ 0 < 2b < c\ \right\} \cong \left\{(l, m) \in \mathbb{R}^2 \;\middle|\; n = lm,\ 0 < 3l < m\right\}. \quad (26)$$

Similarly $(a, b) \mapsto (l, m) := (a + b, a - b)$ gives a bijection (with inverse given by $(l, m) \mapsto (a, b) := ((l + m)/2, (m - l)/2)$) between

$$\left\{(a, b) \in \mathbb{R}^2 \mid 0 < 2b < a,\ n = a^2 - b^2\right\} \cong \left\{(l, m) \in \mathbb{R}^2 \mid n = lm,\ 0 < l < m < 3l\right\}. \quad (27)$$

Proof when $n \equiv 1 \pmod 4$

By restricting to suitable subsets, Type 2 elements are in bijection with:

$$\left\{(b,c)\in\mathbb{R}^2 \;\middle|\; \begin{array}{l} b,c\in\mathbb{Z}^2,\ c \text{ is odd},\ \gcd(b,c)=1,\\ n=b(2c-b),\ 0<2b<c \end{array}\right\} \cong \left\{(l,m)\in\mathbb{R}^2 \;\middle|\; \begin{array}{l} l,m\in\mathbb{Z},\ \ l+m\equiv 0 \pmod 2,\\ l+m\equiv 2 \pmod 4,\ \gcd(l,m)=1,\\ n=lm,\ 0<3l<m \end{array}\right\}. \tag{28}$$

Indeed,

$$b,c\in\mathbb{Z}^2 \iff l,\frac{l+m}{2}\in\mathbb{Z}^2 \iff l,m\in\mathbb{Z}^2,\ l+m\equiv 0 \pmod 2;$$

$$c \text{ is odd} \iff \frac{l+m}{2} \text{ is odd} \iff l+m\equiv 2 \pmod 4.$$

Finally, under the above conditions l must be odd. Thus

$$\gcd(b,c)=1 \iff \gcd(l,\frac{l+m}{2})=1 \iff \gcd(l,l+m)=1 \iff \gcd(l,m)=1.$$

This verifies Eq.(28).

The right hand side of Eq.(28) can be further simplified. Indeed, $n\equiv 1 \pmod 4$ implies that $l\equiv m \pmod 4$. Thus $l+m\equiv 0 \pmod 2$ and $l+m\equiv 2 \pmod 4$ automatically hold. So

$$\text{Type 2} \cong \left\{(l,m)\in\mathbb{Z}^2 \;\middle|\; \gcd(l,m)=1,\ n=lm,\ 0<3l<m\right\}. \tag{29}$$

Type 3 elements can be analyzed in a similar fashion:

$$\left\{(a,b)\in\mathbb{R}^2 \;\middle|\; \begin{array}{l} a,b\in\mathbb{Z}^2,\ a \text{ is odd},\ \gcd(a,b)=1,\\ n=(a-b)(a+b),\ 0<2b<a \end{array}\right\} \cong \left\{(l,m)\in\mathbb{R}^2 \;\middle|\; \begin{array}{l} l,m\in\mathbb{Z},\ \ l+m\equiv 0 \pmod 2,\\ l+m\equiv 2 \pmod 4,\ \gcd(l,m)=1,\\ n=lm,\ 0<l<m<3l \end{array}\right\}. \tag{30}$$

The blue and orange part is the same. The pink part is also similar

$$\gcd(a,b)=1 \iff \gcd(\frac{l+m}{2},\frac{-l+m}{2})=1 \iff \gcd(\frac{l+m}{2},m)=1 \iff \gcd(l+m,m)=\gcd(l,m)=1.$$

This verifies Eq.(30), which is further simplified as

$$\text{Type 3} \cong \left\{(l,m)\in\mathbb{Z}^2 \;\middle|\; \gcd(l,m)=1,\ n=lm,\ 0<l<m<3l\right\} \tag{31}$$

Combining Eq.(29) and (31), we get (note that $m=3l$ never happens)

$$\text{Type 2}\sqcup\text{Type 3} \cong \left\{(l,m)\in\mathbb{Z}^2 \;\middle|\; n=lm,\ \gcd(l,m)=1,\ 0<l<m\right\}$$

which is in bijection with partition of prime factors of n. So it has cardinality $2^r/2=2^{r-1}$. Thus

$$\#\text{Type 1} + \#\text{Type 2 or 3} = 2^{r-1}+2^{r-1}=2^r.$$

Proof when $n\equiv 2,3 \pmod 4$.

In this case, there are no Type 2 or 3 elements.

For type 2 forms, since c is odd, $2c\equiv 2 \pmod 4$ and

$$n=2cb-b^2\equiv 2b-b^2\equiv \begin{cases} 2-1\equiv 1 \pmod 4 & \text{if } b \text{ is odd},\\ 0-0\equiv 0 \pmod 4 & \text{if } b \text{ is even}. \end{cases}$$

For type 3 forms, since a is odd, we have $a^2\equiv 1 \pmod 4$, so

$$n=a^2-b^2\equiv 1-b^2\equiv \begin{cases} 0 \pmod 4 & \text{if } b \text{ is odd},\\ 1 \pmod 4 & \text{if } b \text{ is even}. \end{cases}$$

So we are also done in these two cases.

Proof when $n\equiv 4 \pmod 8$.

In this case there are also no type 2/3 forms.

For a type 2 form $2bx^2+2bxy+cy^2$, we have that c is odd. In order that $n=2bc-b^2\equiv 0 \pmod 4$, we must have b is even. Write $b=2b'$ for some $b'\in\mathbb{Z}$. So $n=4b'(b'-c)$. But one of b' or $b'-c$ has to be even, we have $n\equiv 0 \pmod 8$.

For a type 3 form $ax^2+2bxy+ay^2$, we have that a is odd. But $n=a^2-b^2$ is even, so b is also odd. But then $a^2\equiv b^2\equiv 1 \pmod 8$, showing that $n\equiv 0 \pmod 8$.

So the proof is complete in this case.

Proof when $n\equiv 0 \pmod 8$.

Sending $(b,c)\mapsto(l,m):=\left(\frac{b}{2},c-\frac{b}{2}\right)$ and $(a,b)\mapsto(l,m):=\left(\frac{a-b}{2},\frac{a+b}{2}\right)$ gives bijections between

$$\left\{(b,c)\in\mathbb{R}^2\;\middle|\;n=b(2c-b),0<2b<c\right\}\cong\left\{(l,m)\in\mathbb{R}^2\;\middle|\;n/4=lm,0<3l<m\right\}$$
$$\left\{(a,b)\in\mathbb{R}^2\;\middle|\;n=(a-b)(a+b),0<2b<a\right\}\cong\left\{(l,m)\in\mathbb{R}^2\;\middle|\;n/4=lm,0<l<m<3l\right\}.$$

Restricting to subsets, they induce bijections

$$\left\{(b,c)\in\mathbb{R}^2\;\middle|\;\begin{array}{l}b,c\in\mathbb{Z}^2,\ c\text{ is odd},\ \gcd(b,c)=1,\\ n=b(2c-b),\ 0<2b<c\end{array}\right\}\cong\left\{(l,m)\in\mathbb{R}^2\;\middle|\;\begin{array}{l}l,m\in\mathbb{Z},\ l+m\equiv 1\pmod 2,\\ \gcd(l,m)=1,\ n=lm,\ 0<3l<m\end{array}\right\}\tag{32}$$

and

$$\left\{(a,b)\in\mathbb{R}^2\;\middle|\;\begin{array}{l}a,b\in\mathbb{Z}^2,\ a\text{ is odd},\ \gcd(a,b)=1,\\ n=(a-b)(a+b),\ 0<2b<a\end{array}\right\}\cong\left\{(l,m)\in\mathbb{R}^2\;\middle|\;\begin{array}{l}l,m\in\mathbb{Z},\ l+m\equiv 1\pmod 2,\\ \gcd(l,m)=1,\ n=lm,\ 0<l<\\ m<3l\end{array}\right\}.\tag{33}$$

We explain why Eq.(32) holds and omit the proof for Eq.(33). Note that $\frac{n}{4}=lm$ excludes the possibility $l,m\in\frac{\mathbb{Z}}{2}\setminus\mathbb{Z}$.

$$b,c\in\mathbb{Z}\iff 2l,l+m\in\mathbb{Z}\iff l,m\in\mathbb{Z}.$$

$$c\text{ is odd}\iff l+m\equiv 1\pmod 2.$$

Finally, under the above conditions

$$\gcd(b,c)=1\iff\gcd(2l,l+m)=1\iff\gcd(l,l+m)=\gcd(l,m)=1.$$

One also observes that $l+m\equiv 1\pmod 2$ is redundant: it can be deduced from lm being even and $\gcd(l,m)=1$. Therefore,

$$\text{Type 2}\sqcup\text{Type 3}\cong\left\{(l,m)\in\mathbb{Z}^2\;\middle|\;\frac{n}{4}=lm,\ \gcd(l,m)=1,\ 0<l<m\right\},$$

which has cardinality 2^r. Combined with type 1 elements, there are $2^r+2^r=2^{r+1}$ in total. The proof of Proposition 7.4 is now complete.

7.3. **Genus number, I.** Let $n\in\mathbb{Z}^+$, $D=-4n$ and $Q\in\mathcal{M}_D^+$. We already knew that $\mathrm{Rep}^\times(Q,\mathrm{mod})$ is a coset of $H_D:=\mathrm{Rep}^\times(x^2+ny^2,\mathrm{mod})$, which is a subgroup of $\ker\chi_D$. Sending $[Q]$ to $\mathrm{Rep}^\times(Q,\mathrm{mod})$ gives us a map $\Phi:\mathbf{Cl}(D)\to\ker(\chi_D)/H_D$.

Lemma 7.5. *Φ is a group homomorphism.*

Proof. By definition, identity element is preserved.

Take $[Q_1],[Q_2]\in\mathbf{Cl}(D)$. Replacing by properly equivalent forms, we assume (Q_1,Q_2) is Lagrange-great and so $Q_3:=Q_1\star Q_2$ is a direct composition. Therefore,

$$\mathrm{Rep}^\times(Q_3,\mathrm{mod})\subset\mathrm{Rep}^\times(Q_1,\mathrm{mod})\cdot\mathrm{Rep}^\times(Q_2,\mathrm{mod}).$$

But they are cosets of H_D, so actually equality holds. This shows that $\Phi([Q_1]\cdot[Q_2])=\Phi([Q_1\star Q_2]))=\Phi([Q_1])\cdot\Phi([Q_2])$. □

Therefore, $\mathcal{M}_D^+/\sim_{\mathrm{Genus}}\cong\ker(\chi_D)/H_D$.

Lemma 7.6. *$\ker(\chi_D)/H_D$ is a 2-torsion abelian group. Hence $\#\mathcal{M}_D^+/\sim_{\mathrm{Genus}}$ is a power of 2.*

Proof. This comes from the fact that Q_D^{prin} is a naive composition of Q with itself for every $Q\in\mathcal{M}_D^+$. □

7.4. **Genus number, II.** Let $n\in\mathbb{Z}^+$ and $D:=-4n$ as usual. So far we know the following

- For every $Q\in\mathcal{M}_D^+$, $[Q]^2\in\mathrm{Genus}(x^2+ny^2)$ (see Lemma 6.2). That is, $\mathbf{Cl}(D)^2\subset\mathrm{Genus}(x^2+ny^2)/\sim$;
- Consider the endomorphism

$$\mathbf{Cl}(D)\to\mathbf{Cl}(D)^2$$
$$[Q]\mapsto[Q]^2.$$

We find that

$$\frac{\#\mathbf{Cl}(D)}{\#\mathbf{Cl}(D)[2]}=\#\mathbf{Cl}(D)^2\implies\#\mathbf{Cl}(D)/\mathbf{Cl}(D)^2=\#\mathbf{Cl}(D)[2]$$

- $[Q] \mapsto \mathrm{Rep}^\times([Q], \mathrm{mod})$ induces $\dfrac{\mathbf{Cl}(D)}{\mathrm{Genus}(x^2+ny^2)} \cong \dfrac{\ker(\chi_D)}{H_D}$.
- $\#\,\mathbf{Cl}(D)[2] = 2^{\mu-1}$.

We are now going to show

Theorem 7.7. *The index of H_D in $(\mathbb{Z}/D\mathbb{Z})^\times$ is 2^μ.*

Combining with the facts listed above, we obtain

Corollary 7.8. $\mathbf{Cl}(D)^2 = \mathrm{Genus}(x^2+ny^2)$ *and* $\mathbf{Cl}(D)/\mathbf{Cl}(D)^2 \cong \ker(\chi_D)/H_D$.

In words, every principal genus form arises from a duplication.

7.5. **Proof of Theorem 7.7.** In the proof, we adopt the shorthand notation that for a nonzero integer N,

$$\mathrm{Rep}^\times(N) := \left\{[x^2+ny^2]_N \;\middle|\; x, y \in \mathbb{Z}\right\} \cap \mathrm{U}(\mathbb{Z}/N\mathbb{Z}).$$

So $\mathrm{Rep}^\times(x^2+ny^2, \mod) = \mathrm{Rep}^\times(D)$. Write $n = 2^{a_0} \cdot p_1^{a_1} \cdot \ldots \cdot p_r^{a_r}$ for certain odd primes $p_1, ..., p_r$ with $a_0 \geq 0$, $a_1, ..., a_r \in \mathbb{Z}^+$. Note that

$$x^2 + ny^2 \equiv x^2 \pmod{p_i^{a_i}}, \quad i = 1, ..., r.$$

By Chinese remainder theorem,

$$\begin{aligned}\mathrm{Rep}^\times(D) &= \mathrm{Rep}^\times(4 \cdot 2^{a_0}) \times \mathrm{Rep}^\times(p_1^{a_1}) \times \ldots \times \mathrm{Rep}^\times(p_r^{a_r}) \\ &= \mathrm{Rep}^\times(4 \cdot 2^{a_0}) \times \mathrm{U}(\mathbb{Z}/p_1^{a_1}\mathbb{Z})^2 \times \ldots \times \mathrm{U}(\mathbb{Z}/p_r^{a_r}\mathbb{Z})^2.\end{aligned}$$

For the reader's convenience, let us recall the structure of unit groups: Lemma 1.10 and 1.13.

Lemma 7.9. *Let p be an odd prime and $r \in \mathbb{Z}^+$. Then as a group $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is isomorphic to $\mathbb{Z}/p^{r-1}\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^\times$.*

Lemma 7.10. *Let $r \geq 3$ be an integer. There is a canonical isomorphism $\{\pm 1\} \times \mathbb{Z}/2^{r-2}\mathbb{Z} \cong (\mathbb{Z}/2^r\mathbb{Z})^\times$ where ± 1 goes to $[\pm 1]_{2^r}$ and the $[1] \in \mathbb{Z}/2^{r-2}\mathbb{Z}$ is sent to $[5]_{2^r}$.*

Hence

$$\mathrm{Ind}\left(\mathrm{Rep}^\times(D), (\mathbb{Z}/D\mathbb{Z})^\times\right) = \mathrm{Ind}(\mathrm{Rep}^\times(4 \cdot 2^{a_0}), (\mathbb{Z}/2^{a_0+2}\mathbb{Z})^\times) \cdot 2^r.$$

It only remains to show that

$$\mathrm{Ind}(\mathrm{Rep}^\times(4 \cdot 2^{a_0}), (\mathbb{Z}/2^{a_0+2}\mathbb{Z})^\times) = \begin{cases} 1 & n \equiv 3 \pmod 4 \\ 2 & n \equiv 1, 2 \pmod 4 \\ 2 & n \equiv 4 \pmod 8 \\ 4 & n \equiv 0 \pmod 8 \end{cases}.$$

Case 1, n is odd. Here $a_0 = 0$.
If $n \equiv 1 \pmod 4$, then

$$\mathrm{Rep}^\times(4) = \left\{x^2 + y^2 \pmod 4\right\}^\times = \{[1]_4\},$$

which has index 2 in $(\mathbb{Z}/4\mathbb{Z})^\times$ as expected.
If $n \equiv 3 \pmod 4$, then

$$\mathrm{Rep}^\times(4) = \left\{x^2 - y^2 \pmod 4\right\}^\times = \{[1]_4, [3]_4\},$$

which has index 1 in $(\mathbb{Z}/4\mathbb{Z})^\times$ as expected.
Case 2, $n \equiv 2 \pmod 4$. Here $a_0 = 1$ and

$$\mathrm{Rep}^\times(8) = \{x^2 + ny^2 \pmod 8\}^\times.$$

Note that x has to be odd so $x^2 \equiv 1 \pmod 8$. If y is even, then $ny^2 \equiv 0 \pmod 8$. If y is odd, then $ny^2 \equiv n \pmod 8$. So

$$\mathrm{Rep}^\times(8) = \begin{cases} \{[1]_8, [3]_8\} & \text{if } n \equiv 2 \pmod 8 \\ \{[1]_8, [7]_8\} & \text{if } n \equiv 6 \pmod 8 \end{cases}.$$

In any case, the index in $(\mathbb{Z}/8\mathbb{Z})^\times$ is 2, as expected.
Case 3, $n \equiv 4 \pmod 8$.
Here $a_0 = 2$ and

$$\mathrm{Rep}^\times(16) = \{x^2 + ny^2 \pmod{16}\}^\times.$$

Note that x has to be odd so $x^2 \equiv 1, 9 \pmod{16}$. If y is even, then $ny^2 \equiv 0 \pmod{16}$. If $y = 2y' + 1$ is odd, then

$$ny^2 \equiv 4ny'^2 + 4ny' + n \equiv n \pmod{16}.$$

So there are two cases $n \equiv 4$ or $12 \pmod{16}$. In either case, one has

$$\mathrm{Rep}^\times(16) = \{[1]_{16}, [5]_{16}, [9]_{16}, [13]_{16}\},$$

with index 2 in $(\mathbb{Z}/16\mathbb{Z})^\times$.

Case 4, $n \equiv 0 \pmod{8}$**.**

Now $a_0 \geq 3$ and

$$\mathrm{Rep}^\times(2^{a_0+2}) = \{x^2 + ny^2 \pmod{2^{a_0+2}}\}^\times.$$

Recall $(\mathbb{Z}/2^{a_0+2}\mathbb{Z})^\times \cong \{\pm 1\} \times \langle [5] \rangle$. Thus, when y is even, $\{x^2 \pmod{2^{a_0+2}}\}^\times$ is equal to $\{1\} \times \langle [5]^2 \rangle$. But this is exactly the kernel of

$$(\mathbb{Z}/2^{a_0+2}\mathbb{Z})^\times \to (\mathbb{Z}/8\mathbb{Z})^\times.$$

and $x^2 + ny^2 \equiv x^2 \pmod{8}$. Therefore,

$$\mathrm{Rep}^\times(2^{a_0+2}) = \{1\} \times \langle [5]^2 \rangle$$

with index 4 in $(\mathbb{Z}/2^{a_0+2}\mathbb{Z})^\times$.

7.6. **When is genus = class?** Here is a summary on what we have done:

Theorem 7.11. *Let $n \in \mathbb{Z}^+$ and $D := -4n$. TFAE:*

1. $\mathrm{Genus}(Q)$ *consists of only one proper equivalence class $[Q]$ for every $Q \in \mathcal{M}_D^+$;*
2. *Every positive definite reduced quadratic form of discriminant D takes the form: $ax^2 + cy^2,\ 2bx^2 + 2bxy + cy^2,\ ax^2 + 2bxy + ay^2$;*
3. *The form class group is 2-torsion: $\mathbf{Cl}(D)[2] = \mathbf{Cl}(D)$;*
4. *The form class number is equal to $h(D) = 2^{\mu-1}$.*

Recall that there exists a necessary and sufficient congruence condition for $p = x^2 + ny^2$ (for $p \nmid -4n$) when each $\mathrm{Genus}(Q)$ consists of only one proper equivalence class. Euler listed 65 many n's such that $\sim \iff \sim_{\mathrm{Genus}}$ and Gauss conjectured that the list is complete, which is confirmed under GRH.

Let us end this lecture with such an example.

Example 7.12. *Take $n = 240$. It can be checked that $h(-4n) = 8$. On the other hand, $240 = 2^4 \cdot 3 \cdot 5$. So $r = 2$ and $\mu = r + 2 = 4$. So $2^{\mu-1} = 8 = h(-4n)$. Thus we have for a prime number $p \neq 2, 3, 5$,*

$$p = x^2 + 240y^2 \quad \exists\, x, y \in \mathbb{Z} \iff p \equiv x^2 + 240y^2 \pmod{960} \quad \exists\, x, y \in \mathbb{Z}.$$

Working out the latter condition explicitly (by computer) we obtain

$$p = x^2 + 240y^2 \quad \exists\, x, y \in \mathbb{Z} \iff$$
$$p \equiv 1, 289, 481, 769, 169, 361, 841, 409, 649, 601, 49, 529, 721, 241, 121, 889 \pmod{960}.$$

Note that there are exactly $\frac{32 \times 2 \times 4}{2 \times 8} = 16$ congruence classes as expected.

7.7. **[Not discussed in the class]Interpretation H_D as kernel of characters.** We define group homomorphisms[9]

- For $i = 1, ..., r$, $\chi_i([x]_D) := \left(\dfrac{x}{p_i}\right)$.
- $\delta([x]_D) := (-1)^{\frac{x-1}{2}}$;
- $\epsilon([x]_D) := (-1)^{\frac{x^2-1}{8}}$.

Since the targets are $\{\pm 1\}$, these characters are determined by the kernels, which admit a more concrete description. Note that if $n = 2^k \prod_{i=1}^r p_i^{a_i}$ where p_i's are distinct odd primes, then

$$(\mathbb{Z}/D\mathbb{Z})^\times = (\mathbb{Z}/2^{2+k}\mathbb{Z})^\times \times (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^\times \times ... \times (\mathbb{Z}/p_r^{a_r}\mathbb{Z})^\times$$

Also note that $(\mathbb{Z}/2^{k+2}\mathbb{Z})^\times \cong (\mathbb{Z}/4\mathbb{Z})^\times \times \mathbb{Z}/2^k\mathbb{Z}$ canonically.

- For each $i \in \{1, ..., r\}$,

$$x \equiv \square \pmod{p_i^{a_i}} \iff \chi_i([x]_D) = 1.$$

[9] In general, homomorphisms from a group to $\mathbb{C}^\times$ are referred to as **characters**. Finite abelian groups are determined up to isomorphism by its group of characters.

- $$\delta([x]_D) = 1 \iff \text{the image of } [x]_D \text{ in } (\mathbb{Z}/4\mathbb{Z})^\times \text{ is } [1]_4.$$
- $$\epsilon([x]_D) = 1 \iff \text{the image of } [x]_D \text{ in } \mathbb{Z}/2^k\mathbb{Z} \text{ lies in } 2\mathbb{Z}/2^k\mathbb{Z}.$$
- $$(\epsilon \cdot \delta)([x]_D) = 1 \iff \text{the image of } [x]_D \text{ in } (\mathbb{Z}/4\mathbb{Z})^\times \times \mathbb{Z}/2\mathbb{Z} \text{ lies in } \{(1,0),(-1,1)\}.$$

Let $\mathscr{A}_{D,\text{odd}} := \{\chi_1, ..., \chi_r\}$ and

$$\mathscr{A}_D := \begin{cases} \mathscr{A}_{D,\text{odd}} & n \equiv 3 \pmod 4 \\ \mathscr{A}_{D,\text{odd}} \cup \{\delta\} & n \equiv 1 \pmod 4 \\ \mathscr{A}_{D,\text{odd}} \cup \{\delta \cdot \epsilon\} & n \equiv 2 \pmod 8 \\ \mathscr{A}_{D,\text{odd}} \cup \{\epsilon\} & n \equiv 6 \pmod 8 \\ \mathscr{A}_{D,\text{odd}} \cup \{\delta\} & n \equiv 4 \pmod 8 \\ \mathscr{A}_{D,\text{odd}} \cup \{\delta, \epsilon\} & n \equiv 0 \pmod 8 \end{cases}$$

Note that $\#\mathscr{A}_D = \mu$. Finally, let $\Psi_D : (\mathbb{Z}/D\mathbb{Z})^\times \to (\mathbb{Z}/2\mathbb{Z})^\mu$ by $\Psi_D([x]_D) = \bigoplus_{\chi \in \mathscr{A}} \chi([x]_D)$. The proof presented below actually reveals the following:

Theorem 7.13. *Let $n \in \mathbb{Z}^+$ and $D = -4n$. Then $H_D = \ker \Psi_D$.*

8. $\mathbb{Z}[\omega]$

8.1. **Ring properties of $\mathbb{Z}[\omega]$.** Let $\omega := e^{2\pi i/3}$ be a cubic root of unity. Explicitly $\omega = \dfrac{-1+\sqrt{-3}}{2}$. It satisfies

$$\omega^2 + \omega + 1 = 0.$$

So ω is an algebraic integer and we let $\mathbb{Z}[\omega]$ be the subring of $\mathbb{C}$ generated by $\mathbb{Z}$ and ω. As an abelian group (or $\mathbb{Z}$-module) $\mathbb{Z}[\omega] \cong \mathbb{Z} \oplus \mathbb{Z}.\omega$. Every element $x \in \mathbb{Z}[\omega]$ can be uniquely written as $a + b\omega$ for some $a, b \in \mathbb{Z}$.

Just to recall the definition of rings and ideals

Definition 8.1. *Let R be a unital commutative ring, that is, R is equipped with two binary operations $+, \times$ and two distinguished elements $0, 1$ satisfying certain assumptions*[10]*. A subset $I \subset R$ is said to be an **ideal** iff*

(1) *I is an additive subgroup;*
(2) *$R \cdot I \subset I$.*

*Equivalently, an ideal is an R-submodule of R. For $x \in R$, $R \cdot x$ is an ideal and is called the ideal generated by x, denoted as $\langle x \rangle$. An ideal is said to be **principal** iff it is generated by a single element. If all ideals are principal, then we call R a **principal ideal domain**.*

Notation 8.2. *$I \trianglelefteq R$ means I is an ideal of R.*

We often use the fact that $\mathbb{Z}[\omega]$ is an integral domain: $xy = 0 \implies x$ or $y = 0$.

8.1.1. *Euclidean domain.* For $\alpha \in \mathbb{Z}[\omega]$, we let $\mathrm{Nm}(\alpha) := \alpha \cdot \overline{\alpha}$. It is a positive integer unless $\alpha = 0$. If $\alpha = a + b\omega$, then

$$\mathrm{Nm}(\alpha) = (a + b\omega)(a + b\overline{\omega}) = a^2 - ab + b^2.$$

Lemma 8.3. *For $x, y \in \mathbb{Z}[\omega]$ with $x \neq 0$, there exists $q, r \in \mathbb{Z}[\omega]$ such that $y = qx + r$ and $\mathrm{Nm}(r) \lneq \mathrm{Nm}(y)$.*

Proof. Find $\alpha, \beta \in \mathbb{Q}$ such that

$$\frac{y}{x} = \frac{y \cdot \overline{x}}{\mathrm{Nm}(x)} = \alpha + \beta\omega.$$

Choose $a, b \in \mathbb{Z}$ such that $|a - \alpha|, |b - \beta| \lneq \frac{1}{2}$. We let $q := a + b\omega$. Then

$$\mathrm{Nm}(y - qx) = \mathrm{Nm}(x) \cdot \mathrm{Nm}((\alpha - a) + (\beta - b)\omega) \leq \frac{3}{4}\mathrm{Nm}(x) \lneq \mathrm{Nm}(x).$$

□

This shows that $\mathbb{Z}[\omega]$ is an Euclidean domain with respect to $\mathrm{Nm}(\cdot)$[11].

[10] $(R, +, 0)$ is an Abelian group, $(R, \times, 1)$ is an Abelian semi-group and $(x + y) \times z = x \times z + y \times z$.

[11] For other number fields K, it is possible that the Euclidean property fails for $\mathcal{O}_K$ with respect to $\mathrm{Nm}(\cdot)$, but holds for some other function.

8.1.2. *Units.* One can characterize **units** ($x \in \mathbb{Z}[\omega]$ is said to be a unit iff $xy = 1$ for some $y \in \mathbb{Z}[\omega]$ and the set of units is denoted as $\mathbb{Z}[\omega]^\times$ or $\mathbf{U}(\mathbb{Z}[\omega])$) in terms of $\mathrm{Nm}\,(\cdot)$.

Lemma 8.4. $\mathbb{Z}[\omega]^\times = \{x \in \mathbb{Z}[\omega] \mid \mathrm{Nm}\,(x) = 1\} = \{1, -1, \omega, -\omega, \omega^2 = -1 - \omega, -\omega^2 = 1 + \omega\}$.

Proof. If $x \in \mathbb{Z}[\omega]^\times$, then $xy = 1$ for some $y \in \mathbb{Z}[\omega]$. So $\mathrm{Nm}\,(x)\,\mathrm{Nm}\,(y) = \mathrm{Nm}\,(1) = 1$, forcing $\mathrm{Nm}\,(x) = \mathrm{Nm}\,(y) = 1$. Conversely, if $\mathrm{Nm}\,(x) = 1$, then $\overline{x}$ is the inverse of x.

The list of units is obtained by solving the equation

$$\mathrm{Nm}\,(a + b\omega) = a^2 - ab + b^2 = (a - \frac{1}{2}b)^2 + \frac{3}{4}b^2 = 1.$$

The details are omitted. □

8.1.3. *PID.*

Lemma 8.5. *The ring $\mathbb{Z}[\omega]$ is a principal ideal domain.*

Proof. Let us assume $I \neq \{0\}$. Take $I \trianglelefteq \mathbb{Z}[\omega]$ and choose $x_0 \in I$ satisfying

$$\mathrm{Nm}\,(x_0) = \min\{\mathrm{Nm}\,(x) \mid x \in I,\ x \neq 0\}$$

We claim that $I = \langle x_0 \rangle$. Otherwise, take $y \in I \setminus \langle x_0 \rangle$. Then $y = z \cdot x_0 + r_0$ for some $\mathrm{Nm}\,(r_0) < \mathrm{Nm}\,(x_0)$. But $r_0 \in I$, leading to a contradiction. □

Notation 8.6. *For $x, y \in R$, write $x \mid y$ iff $\langle x \rangle \supset \langle y \rangle$ or equivalently, $y = xr$ for some $r \in R$.*

8.1.4. *UFD.* The notion of prime numbers can be generalized to rings in two ways.

Definition 8.7. *An element $\pi_{\neq 0} \in \mathbb{Z}[\omega]$ is said to be **prime** iff the ideal generated by π is a **prime ideal**, that is to say, if $xy \in \langle \pi \rangle$ for two elements $x, y \in \mathbb{Z}[\omega]$ then one of x, y has to be in $\langle \pi \rangle$. An element $\pi_{\neq 0} \in \mathbb{Z}[\omega]$ is said to be **irreducible** iff $\pi = xy$ for two elements $x, y \in \mathbb{Z}[\omega]$ implies one of x or y has to be a unit.*

By definition $\pi \in \mathbb{Z}[\omega]$ is prime iff $\pi \mid xy \implies \pi \mid x$ or $\pi \mid y$.

Lemma 8.8. *Let $\pi_{\neq 0} \in \mathbb{Z}[\omega]$. Then π a prime iff π is irreducible.*

Proof. First let us assume π is prime and suppose $\pi = xy$ for some $x, y \in \mathbb{Z}[\omega]$. We must show one of them is a unit. Indeed, we know that one of them belongs to $\langle \pi \rangle$. Say $x \in \langle \pi \rangle$, so $x = \pi x'$ for some $x' \in \mathbb{Z}[\omega]$. So $\pi = xy = \pi x' y \implies 1 = x'y$. So y is a unit.

On the other hand, suppose π is irreducible. Assume $x, y \notin \langle \pi \rangle$ and it suffices to show $xy \notin \langle \pi \rangle$. Since $\mathbb{Z}[\omega]$ is a PID, we find x' such that $\langle \pi, x \rangle = \langle x' \rangle$. Write $\pi = x' \cdot \pi'$. Since $\langle \pi, x \rangle \neq \langle \pi \rangle$, π' is not a unit. But π is irreducible, so x' must be a unit and $\langle x' \rangle = \mathbb{Z}[\omega]$ and we can find $a, b \in \mathbb{Z}[\omega]$ such that $ax + b\pi = 1$. Multiplying by y, we get $axy + b\pi y = y$. Since $y \notin \langle \pi \rangle$, we must have $xy \notin \langle \pi \rangle$. □

Lemma 8.9. *The ring $\mathbb{Z}[\omega]$ is a UFD (**Unique factorization domain**). Namely, the following two things hold:*

1. *For every nonzero $x \in \mathbb{Z}[\omega] \setminus \mathbb{Z}[\omega]^\times$, there exist irreducible and non-unital elements $(\pi_1, ..., \pi_l)$ in $\mathbb{Z}[\omega]$ such that $x = \prod_{i=1}^{l} \pi_i$.*
2. *If $x = \prod_{j=1}^{m} q_j$ is another factorization into irreducible non-unital elements, then $m = l$ and up to reordering, $q_i = p_i u_i$ for some units u_i.*

Proof of (1). If x is irreducible, then we are done. Otherwise, write $x = y \cdot z$, neither of which is a unit. If they are both irreducible then we are done, otherwise we could continue. Repeating this process, either we end up writing x as a product of irreducible elements, or we find a sequence $x_1, x_2, ...$ such that $x_n = x_{n+1} y_{n+1}$ for some non-unit $y_{n+1} \in \mathbb{Z}[\omega]$. So we get an increasing sequence of ideals

$$\langle x_1 \rangle \subsetneq \langle x_2 \rangle \subsetneq ...$$

This is strictly increasing since y_{n+1}'s are not unit. But this is a contradiction against the PID property. Indeed, let I be their union, then I is an ideal and hence generated by some z, but by definition $z \in \langle x_n \rangle$ for some n. So $I = \langle x_n \rangle = \langle x_{n+1} \rangle = ...$ □

Proof of (2). Say

$$x = q_1 \cdot ... \cdot q_l = \pi_1 \cdot .... \cdot \pi_k$$

Since irreducible = prime, we have

$$q_1 \mid \pi_1 \cdot .... \cdot \pi_k \implies q_1 \mid \pi_{\sigma_1}$$

for some $\sigma_1 \in \{1, ..., k\}$. But q_1, π_{σ_1} are both irreducible, so $\pi_{\sigma_1} = q_1 u_1$ for some unit u_1. By permuting, we assume $\sigma_1 = 1$ and we are left with

$$x/q_1 = q_2 \cdot ... \cdot q_l = u_1 \cdot \pi_2 \cdot ... \cdot \pi_k$$

It suffices to repeat the above process. □

We can also define the notion of coprime. Two elements are said to be coprime iff the primes dividing them are disjoint from each other.

Lemma 8.10. *If $x, y \in \mathbb{Z}[\omega]$ are coprime, then $\alpha x + \beta y = 1$ for some $\alpha, \beta \in \mathbb{Z}[\omega]$.*

Proof. Let z be such that $\langle z \rangle = \langle x, y \rangle$. Then any prime dividing z necessarily divides both x, y. By assumption, there are no such primes. That is to say, z is a unit. □

8.2. **Arithmetic of $\mathbb{Z}[\omega]$.**

Theorem 8.11. *Let $p \in \mathbb{Z}^+$ be a prime number, then*

$$\begin{cases} p = -\omega^2(1-\omega)^2 & p = 3. \\ p = \pi \cdot \overline{\pi} \text{ for some primes } \pi \in \mathbb{Z}[\omega] & p \equiv 1 \pmod 3 \\ p \text{ remains a prime in } \mathbb{Z}[\omega] & p \equiv 2 \pmod 3 \end{cases}$$

Moreover in the second case, $\langle \pi \rangle \neq \langle \overline{\pi} \rangle$.

Proof. That $3 = -\omega^2(1-\omega)^2$ can be checked directly.

So let $p_{\neq 3} \in \mathbb{Z}^+$ be a prime number, factorized as $p = \pi_1 \cdot ... \cdot \pi_l$ in $\mathbb{Z}[\omega]$. Then

$$p^2 = \mathrm{Nm}\,(p) = \prod \mathrm{Nm}\,(\pi_i) \implies l = 1, 2$$

When $l = 2$,

$$\pi_1 \cdot \pi_2 = p = \mathrm{Nm}\,(\pi_1) = \pi_1 \cdot \overline{\pi_1} = \mathrm{Nm}\,(\pi_2) = \pi_2 \cdot \overline{\pi_2}.$$

So $p = \pi_1 \cdot \overline{\pi_1}$ is the prime factorization. If $\pi_1 = x + y\omega$, then $p = x^2 - xy + y^2$. Modulo 3 implies that $p \equiv 1 \pmod 3$.

It remains to assume $l = 1$ and we are going to show $p \equiv 2 \pmod 3$. If not, then $p \equiv 1 \pmod 3$. By reduction theory, $p = x^2 - xy + y^2 = \mathrm{Nm}\,(x + y\omega)$ for some $x, y \in \mathbb{Z}$. One sees that $x + y\omega$ is not a unit so p is not a prime. This is a contradiction. □

Theorem 8.12. *Let π be a non-unital irreducible element in $\mathbb{Z}[\omega]$, then either $\pi = p$ is a prime number in $\mathbb{Z}$ with $p \equiv 2 \pmod 3$, or $\mathrm{Nm}\,(\pi) = p$ is a prime number in $\mathbb{Z}$ with $p \equiv 1 \pmod 3$, or $\langle \pi \rangle = \langle 1 - \omega \rangle$.*

Proof. Let π be a prime. Then $n = \pi \cdot \overline{\pi}$ is an integer in $\mathbb{Z}$. By uniqueness of prime factorization, n is either p or p^2 for some prime number p. Moreover, in the latter case, $p = \pi u$ for some unit u. This finishes the proof. □

Lemma 8.13. *Let $\langle \pi \rangle$ be a prime ideal of $\mathbb{Z}[\omega]$, then $\mathbb{Z}[\omega]/\langle \pi \rangle$ is a field consisting of $\mathrm{Nm}\,(\pi)$ elements.*

Proof. That it is a field follows from the fact that prime ideals are maximal.

If $\pi = p$ is a prime number in $\mathbb{Z}$, then $\mathbb{Z}[\omega]/\langle p \rangle \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}.\omega$ as an additive group. So it has $p^2 = \mathrm{Nm}\,(p)$ many elements.

Otherwise, $\pi \cdot \overline{\pi} = p$ for some prime number $p \in \mathbb{Z}$ and hence $\langle \pi \rangle \neq \langle p \rangle$. So $\mathbb{Z}[\omega]/p\mathbb{Z}[\omega] \to \mathbb{Z}[\omega]/\langle \pi \rangle$ is surjective homomorphism with nontrivial kernel, implying $\#\mathbb{Z}[\omega]/\langle \pi \rangle$ divides $\#\mathbb{Z}[\omega]/p\mathbb{Z}[\omega] = p^2$ and is not equal to it. Thus $\#\mathbb{Z}[\omega]/\langle \pi \rangle = p = \mathrm{Nm}\,(\pi)$. □

Also note that in whichever case $\langle \pi \rangle \cap \mathbb{Z} = p.\mathbb{Z}$. Indeed if an integer n is equal to $n = \pi \cdot x$ for some $x \in \mathbb{Z}[\omega]$, by taking norm on both sides we get

$$n^2 = p \cdot \mathrm{Nm}\,(x) \implies p \mid n.$$

Thus, the natural map $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}[\omega]/\langle \pi \rangle$ is injective, which may be viewed as a finite field extension.

8.3. **Associates and primary elements.**

Definition 8.14. *Given two elements $x, y \in R$, y is said to be an **associate** of x iff $y = ux$ for some unit u, or equivalently, iff $\langle x \rangle = \langle y \rangle$.*

Definition 8.15. *An element $\pi = a + b\omega \in \mathbb{Z}[\omega]$ is said to be **primary** iff $a \equiv -1 \pmod 3$ and $b \equiv 0 \pmod 3$.*

We record here an observation

Lemma 8.16. *Let $\pi_{\neq 0} = a + b\omega \in \mathbb{Z}[\omega]$. Then x has exactly six associates given by*

$$a + b\omega,\ -a - b\omega,\ -b + (a - b)\omega,\ b + (b - a)\omega,\ (b - a) - a\omega,\ (a - b) + a\omega.$$

If π is an irreducible element not dividing 3, then exactly one of the six associates is primary.

Proof. If $\pi = a + b\omega$ with $(a, b) = (-1, 0) \pmod 3$, then

$$(-a, -b) \equiv (1, 0) \quad (-b, a - b) \equiv (0, -1) \quad (b, b - a) \equiv (0, 1)$$
$$(b - a, -a) \equiv (1, 1) \quad (a - b, a) \equiv (-1, -1) \quad \pmod 3.$$

It thus suffices to show that (a, b) modulo 3 takes one of the forms $(\pm 1, 0), (0, \pm 1), \pm(1, 1)$ if $\pi \nmid 3$. If $\pi \in \mathbb{Z}$, then $b = 0$ and this is true. Otherwise $p := a^2 - ab + b^2$ is a prime number different from 3. If $(a, b) = \pm(1, -1)$ or $(0, 0)$, then $p \equiv 0 \pmod 3$, contradiction. So we are done. □

9. Cubic reciprocity law

We will present a cubic reciprocity law in this section. Whereas many ideas are borrowed from the quadratic case, the arithmetic of $\mathbb{Z}[\omega]$ is used in an essential way.

9.1. **Motivation of cubic reciprocity.** Let p, q be two different prime numbers, when does

$$x^3 \equiv q \pmod p$$

has a solution?

Well, equivalently, we are asking whether $[q]_p$ lies in $\mathbf{U}(\mathbb{Z}/p\mathbb{Z})^3$. Note that $\mathbf{U}(\mathbb{Z}/p\mathbb{Z})$ is a cyclic group of order $p - 1$.

9.1.1. *Trivial case: $p \equiv 2 \pmod 3$.* In this case, the order of $\mathbf{U}(\mathbb{Z}/p\mathbb{Z})$ is coprime to 3. Hence

$$x \mapsto x^3 \pmod p$$

induces an automorphism $\mathbf{U}(\mathbb{Z}/p\mathbb{Z}) \cong \mathbf{U}(\mathbb{Z}/p\mathbb{Z})$. The conclusion is

$$\text{for every integer } n,\ x^3 \equiv n \pmod p \text{ has exactly one solution.}$$

9.1.2. *Nontrivial case: $p \equiv 1 \pmod 3$.* In this case, exactly one thirds of $\mathbf{U}(\mathbb{Z}/p\mathbb{Z})$ has a cubic root modulo p.

Question 9.1. *Fix q, let $p \equiv 1 \pmod 3$ vary. Is it true that*

$$\textit{whether } \sqrt[3]{q} \textit{ exists modulo } p \textit{ depends on the congruence class of } p \textit{ modulo } q?$$

It turns out that the answer is surprisingly NO! There is a theorem in algebraic number theory implying that[12]

Theorem 9.2. *Let $M \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$ with $a \equiv 1 \pmod 3$ and $\gcd(a, M) = 1$. Consider the set of primes $\mathcal{P}_{a,M} := \{\, p \equiv 1 \pmod 3,\ p \equiv a \pmod M\}$. Then*

$$\#\{p \in \mathcal{P}_{a,m} \mid \sqrt[3]{q} \textit{ exists} \bmod p\} = \#\{p \in \mathcal{P}_{a,m} \mid \sqrt[3]{q} \textit{ does not exist} \bmod p\} = +\infty.$$

9.2. **Mimicking the quadratic case.** Let us recall some elements from the quadratic case

(1) there is a Legendre symbol $\left(\frac{q}{p}\right) \in \{\pm 1\}$ recording whether $\sqrt{q} \pmod p$ exists or not;
(2) there is certain law relating the value $\left(\frac{q}{p}\right)$ to $\left(\frac{p}{q}\right)$;
(3) in the process of establishing this law, we found an expression for $\sqrt{\pm q}$ using "Gauss sum" $g_q := \sum_{a \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{a}{q}\right) \zeta_q^a$ where $\zeta_q := e^{\frac{2\pi i}{q}}$.

[12] We are not going to prove this.

9.3. **Cubic residue character.** Since $\mathbb{Z}/p\mathbb{Z}$ has order $p-1$, for any integer n coprime to p, $n^{\frac{p-1}{3}}$ is a cubic root of unity modulo p. Thus we would like to say that $n^{\frac{p-1}{3}}$ is one of $\{1, \zeta_3, \zeta_3^2\}$ modulo p. But wait, what does this mean? How to put ζ_3 inside $\mathbb{Z}/p\mathbb{Z}$?

One could just consider[13] ω modulo $p\mathbb{Z}[\omega]$, namely $[\omega]_p \in \mathbb{Z}[\omega]/p\mathbb{Z}[\omega]$. It has been shown that $\mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbb{Z}[\omega]/p\mathbb{Z}[\omega]$ before. So we would be happy if $[\omega]_p$ just happens to lie in the image of $\mathbb{Z}/p\mathbb{Z}$, which is, of course, not true.

Luckily we have learned the arithmetic of $\mathbb{Z}[\omega]$, so we know how to remedy this[14]. Indeed, by Theorem 8.11, $p \equiv 1 \pmod 3 \implies p = \pi_p \cdot \overline{\pi_p}$ for some irreducible element $\pi_p \in \mathbb{Z}[\omega]$. Moreover, the natural map $\mathbb{Z} \to \mathbb{Z}[\omega]$ induces an *isomorphism* $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}[\omega]/\pi_p\mathbb{Z}[\omega]$ (cf. Lemma 8.13). So the analogue of Legendre symbol can be defined.

Although we initially care only about $n \in \mathbb{Z}$ coprime to p, it readily generalizes to all $x \in \mathbb{Z}[\omega]$ that is coprime to π_p:

Lemma 9.3. *Let $p \equiv 1 \pmod 3$ be a prime number in $\mathbb{Z}$, which factorizes as $p = \pi_p \cdot \overline{\pi_p}$ for some $\pi_p \in \mathbb{Z}[\omega]$. Then for each $x \in \mathbb{Z}[\omega]$ that is coprime to π_p, there exists a unique number in $\{1, \omega, \omega^2\}$, denoted as $\left(\frac{x}{\pi_p}\right)_3$, such that*

$$x^{\frac{p-1}{3}} \equiv \left(\frac{x}{\pi_p}\right)_3 \pmod{\pi_p\mathbb{Z}[\omega]}.$$

Proof. It remains to show that the images of $\{1, \omega, \omega^2\}$ in $\mathbb{Z}[\omega]/\pi_p\mathbb{Z}[\omega]$ are different from each other. Indeed, $\mathrm{Nm}\left(1-\omega^2\right) = \mathrm{Nm}\left(1-\omega\right) = \mathrm{Nm}\left(\omega-\omega^2\right) = 3$ is corpime to p and hence $1-\omega^2$, $1-\omega$ and $\omega-\omega^2$ are coprime to π_p. □

Remark 9.4. *Let us note that*

$$x^3 \equiv q \pmod p \text{ has a solution} \iff \left(\frac{q}{\pi_p}\right)_3 = 1.$$

Remark 9.5. *Given p, one does not have a preference of π_p over $\overline{\pi_p}$, so let us note that*

$$\overline{\left(\frac{x}{\pi_p}\right)_3} = \left(\frac{\overline{x}}{\overline{\pi_p}}\right)_3.$$

Thus for an integer n,

$$\left(\frac{n}{\pi_p}\right)_3 = 1 \iff \left(\frac{n}{\overline{\pi_p}}\right)_3 = 1$$

Remark 9.6. *By Lemma 9.3, $x \mapsto \left(\frac{x}{\pi_p}\right)_3$ can be viewed as a character (i.e. group homomorphism) $\mathbf{U}(\mathbb{Z}/p\mathbb{Z}) \cong \mathbf{U}(\mathbb{Z}[\omega]/\pi_p\mathbb{Z}[\omega]) \to \{1, \omega, \omega^2\}$. This character is clearly surjective.*

9.4. **Gauss sums.**

Definition 9.7. *Let q be a prime number satisfying $q \equiv 1 \pmod 3$. For a character $\chi : (\mathbb{Z}/q\mathbb{Z})^\times \to \{1, \omega, \omega^2\}$ (we shall refer such things as q-**cubic characters**), we define the **Gauss sum***

$$g_q(\chi) := \sum_{a \in \mathbb{Z}/q\mathbb{Z}} \chi(a)\zeta_q^a \in \mathbb{Z}[\zeta_{3q}] = \mathbb{Z}[\omega, \zeta_q]$$

where $\chi([0]_q) := 0$ for convenience.

Inspired by the quadratic case, one naturally wonders what $g_q(\chi)^3$ is.

Definition 9.8. *Let q, χ be as in last definition. Let*

$$J_q(\chi) := \sum_{a+b=1,\ a,b \in \mathbb{Z}/q\mathbb{Z}} \chi(a)\chi(b) \in \mathbb{Z}[\omega]$$

*called a **Jacobi sum**.*

Lemma 9.9. *Let q be a prime number satisfying $q \equiv 1 \pmod 3$. Let χ be a nontrivial q-cubic character. Then*

$$g_q(\chi)^2 = g_q(\chi^2) \cdot J_q(\chi)$$

[13] From this point on, we set $\omega := \zeta_3$ to distinguish it from other ζ_p or ζ_q's.

[14] We want to emphasize that even if one only cares whether this quantity is one or not and the related reciprocity law, whose statement does not require this higher arithmetic, it is still essential to distinguish ω or ω^2 to take advantage of the group structure. This will be used in the proof of reciprocity law.

Proof.

$$\begin{aligned} g_q(\chi)^2 &= \sum_{a\in\mathbb{Z}/q\mathbb{Z}} \chi(a)\zeta_q^a \cdot \sum_{b\in\mathbb{Z}/q\mathbb{Z}} \chi(b)\zeta_q^b \\ &= \sum_{a,b\in\mathbb{Z}/q\mathbb{Z}} \chi(ab)\zeta_q^{a+b} \\ &= \sum_{c\in(\mathbb{Z}/q\mathbb{Z})^\times} \zeta_q^c \sum_{b\in(\mathbb{Z}/q\mathbb{Z})^\times} \chi((c-b)b) + \sum_{b\in\mathbb{Z}/q\mathbb{Z}} \chi(-b^2) \\ &= \sum_{c\in(\mathbb{Z}/q\mathbb{Z})^\times} \zeta_q^c \cdot \chi(c)^2 \cdot \sum_{b\in(\mathbb{Z}/q\mathbb{Z})^\times} \chi(b-b^2) \\ &= g_q(\chi^2)\cdot J_q(\chi). \end{aligned}$$

□

Lemma 9.10. *Let q, χ be as in last lemma. Then*

$$g_q(\chi)g_q(\chi^2) = q.$$

Proof. χ being a cubic character implies that $\chi^2 = \chi^{-1}$.

$$\begin{aligned} g_q(\chi)g_q(\chi^2) &= \sum_{a\in\mathbb{Z}/q\mathbb{Z}} \chi(a)\zeta_q^a \cdot \sum_{b\in\mathbb{Z}/q\mathbb{Z}} \chi(b^{-1})\zeta_q^b \\ &= \sum_{a,b\in\mathbb{Z}/q\mathbb{Z}} \chi(ab^{-1})\zeta_q^{a+b} \\ &= \sum_{c\in(\mathbb{Z}/q\mathbb{Z})^\times} \zeta_q^c \sum_{b\in(\mathbb{Z}/q\mathbb{Z})^\times} \chi((c-b)b^{-1}) + \sum_{b\in(\mathbb{Z}/q\mathbb{Z})^\times} \chi(-1) \\ &= \sum_{c\in(\mathbb{Z}/q\mathbb{Z})^\times} \zeta_q^c \sum_{b'\in\mathbb{Z}/q\mathbb{Z}\setminus\{[-1]\}} \chi(b') + (q-1) \\ &= \sum_{c\in(\mathbb{Z}/q\mathbb{Z})^\times} -\zeta_q^c + (q-1) = q \end{aligned}$$

□

Corollary 9.11. *Let q, χ be as above. Then*

$$g_q(\chi)^3 = J_q(\chi)\cdot q.$$

Corollary 9.12. *Let q, χ be as above. Then*

$$g_q(\chi)\cdot\overline{g_q(\chi)} = J_q(\chi)\cdot\overline{J_q(\chi)} = q.$$

Note that $\overline{g_q(\chi)} = g_q(\chi^2)$.

9.5. **Interacting two different primes.** By Corollary 9.11 above $q^{\frac{p-1}{3}} J_q(\chi)^{\frac{p-1}{3}} = g_q(\chi)^{p-1}$. And we are led to compute the p-th power of $g_q(\chi)$ modulo p (or more precisely, modulo $p\mathbb{Z}[\zeta_{3q}]$).

Lemma 9.13. *Let q be a prime number with $q \equiv 1 \pmod 3$ and χ be a q-cubic character. Let $p \neq q$ be another prime number also satisfying $p \equiv 1 \pmod 3$. Then*

$$g_q(\chi)^p \equiv g_q(\chi)\cdot\chi^2([p]_q) \pmod{p\mathbb{Z}[\zeta_{3q}]}$$

Proof. Note that $p \equiv 1 \pmod 3$ implies that $\chi^p = \chi$.

$$\begin{aligned} g_q(\chi)^p &= \Big(\sum_{a\in\mathbb{Z}/q\mathbb{Z}} \chi(a)\zeta_q^a\Big)^p \equiv \sum_{a\in\mathbb{Z}/q\mathbb{Z}} \chi(a)\zeta_q^{ap} \pmod p \\ &\equiv \sum_{b\in\mathbb{Z}/q\mathbb{Z}} \chi(b\cdot[p^{-1}]_q)\zeta_q^b \equiv g_q(\chi)\cdot\chi^2([p]_q) \pmod p \end{aligned}$$

□

Combining results from last subsection, we get

Lemma 9.14. *Let p, q, χ be as in last lemma. Then*

$$J_q(\chi)^{\frac{p-1}{3}} q^{\frac{p-1}{3}} \equiv \chi^2([p]_q) \pmod p.$$

Proof.

$$\begin{aligned} & g_q(\chi)\cdot J_q(\chi)^{\frac{p-1}{3}} q^{\frac{p-1}{3}} = (g_q(\chi))^p \equiv g_q(\chi)\cdot \chi^2([p]_q) \pmod p \\ \Longrightarrow\ & qJ_q(\chi)^{\frac{p-1}{3}} q^{\frac{p-1}{3}} \equiv q\chi^2([p]_q) \pmod p \\ \Longrightarrow\ & J_q(\chi)^{\frac{p-1}{3}} q^{\frac{p-1}{3}} \equiv \chi^2([p]_q) \pmod p. \end{aligned}$$

where we used $g_q(\chi)\cdot\overline{g_q(\chi)} = q$ from Corollary 9.12. □

9.6. **Primes above q as a Jacobi sum.** Take a prime number $q \equiv 1 \pmod 3$ and factorize $q = \pi_q\overline{\pi_q}$. To kill the ambiguity, we require π_q to be primary, that is, $\pi_q \equiv -1 \pmod 3$. With this condition, at least the set $\{\pi_q, \overline{\pi_q}\}$ is uniquely determined from q.

Specialize to the q-cubic character $\chi_{\pi_q}(-) := \left(\frac{-}{\pi_q}\right)_3$. By Corollary 9.12 above,

$$J_q(\chi_{\pi_q})\cdot\overline{J_q(\chi_{\pi_q})} = q.$$

We further have

Lemma 9.15. *Notation as above, $J_q(\chi_{\pi_q}) \equiv -1 \pmod 3$.*

Proof. By Corollary 9.11,

$$\begin{aligned} q\cdot J_q(\chi_{\pi_q}) &= \Big(\sum \chi_{\pi_q}(a)\zeta_q^a\Big)^3 \equiv \sum \chi_{\pi_q}^3(a)\zeta_q^{3a} \pmod 3 \\ &\equiv \sum_{a\neq 0} \zeta_q^{3a} \equiv -1 \pmod 3 \end{aligned}$$

Since $q \equiv 1 \pmod 3$, the above implies

$$J_q(\chi_{\pi_q}) \equiv -1 \pmod 3.$$

□

Remark 9.16. *If one use the original definition of $J_q(\chi_{\pi_q})$, then by taking third power one can show $J_q(\chi_{\pi_q})^3 \equiv -1 \pmod 3$. But this is insufficient to conclude that $J_q(\chi_{\pi_q})$ itself satisfies this congruence condition.*

Therefore $J_q(\chi_{\pi_q}) \in \{\pi_q, \overline{\pi_q}\}$. We claim that

Lemma 9.17. *Notation as above, $J_q(\chi_{\pi_q}) = \pi_q$.*

Proof. By the definition of χ_{π_q}

$$J_q(\chi_{\pi_q}) \equiv \sum_{a\in\mathbb{Z}/q\mathbb{Z}} a^{\frac{q-1}{3}}(1-a)^{\frac{q-1}{3}} \equiv \sum_{a\in\mathbb{Z}/q\mathbb{Z}} \sum_{0\le l\le 2(q-1)/3} \lambda_l a^l \pmod{\pi_q}$$

for some $\lambda_l \in \mathbb{Z}$. We show the latter summation over a vanishes for each l.

For $l < q-1$, there exists $x_0 \in (\mathbb{Z}/q\mathbb{Z})^\times$ such that $x_0^l \neq [1]_q$:

$$\sum_{a\in\mathbb{Z}/q\mathbb{Z}} a^l = \sum_{a\in\mathbb{Z}/q\mathbb{Z}} (x_0 a)^l = x_0^l \sum_{a\in\mathbb{Z}/q\mathbb{Z}} a^l \implies \sum_{a\in\mathbb{Z}/q\mathbb{Z}} a^l = 0.$$

So we are done. □

9.7. **Cubic reciprocity law, I.** It's time to state and prove (a case of) cubic reciprocity.

Theorem 9.18. *Let $p \neq q$ be two distinct prime numbers satisfying $p \equiv q \equiv 1 \pmod 3$. Let π_p (resp. π_q) be a primary prime that lies above p (resp. q). Then*

$$\left(\frac{\pi_p}{\pi_q}\right)_3 = \left(\frac{\pi_q}{\pi_p}\right)_3$$

.

Proof. By Lemma 9.17 first and then 9.14,

$$\begin{aligned} & q^{\frac{p-1}{3}}\pi_q^{\frac{p-1}{3}} \equiv \big(qJ_q(\chi_{\pi_q})\big)^{\frac{p-1}{3}} \equiv \chi_{\pi_q}([p]_q)^2 \pmod{p\mathbb{Z}[\omega]} \\ \Longrightarrow\ & q^{\frac{p-1}{3}}\pi_q^{\frac{p-1}{3}} \equiv \chi_{\pi_q}([p]_q)^2 \pmod{\pi_p\mathbb{Z}[\omega]}. \end{aligned}$$

Therefore,

$$\left(\frac{\pi_q}{\pi_p}\right)_3^2\left(\frac{\overline{\pi_q}}{\pi_p}\right)_3 \equiv \left(\frac{\pi_p}{\pi_q}\right)_3^2\left(\frac{\overline{\pi_p}}{\pi_q}\right)_3^2 \pmod{\pi_p\mathbb{Z}[\omega]} \implies \left(\frac{\pi_q}{\pi_p}\right)_3^2\left(\frac{\overline{\pi_q}}{\pi_p}\right)_3 = \left(\frac{\pi_p}{\pi_q}\right)_3^2\left(\frac{\overline{\pi_p}}{\pi_q}\right)_3^2.$$

Swapping the role of π_q, π_p, one obtains

$$\left(\frac{\pi_q}{\pi_p}\right)_3^2 \left(\frac{\overline{\pi_q}}{\pi_p}\right)_3^2 = \left(\frac{\pi_p}{\pi_q}\right)_3^2 \left(\frac{\overline{\pi_p}}{\pi_q}\right)_3$$

Multiplying them together:

$$\left(\frac{\pi_q}{\pi_p}\right)_3 = \left(\frac{\pi_p}{\pi_q}\right)_3.$$

□

9.8. **Cubic reciprocity law, II.**

Theorem 9.19. *Let p, q be two different primes satisfying $p \equiv 2 \pmod 3$ and $q \equiv 1 \pmod 3$. Let π_q be a primary prime lying over q, then*

$$\left(\frac{p}{\pi_q}\right)_3 = \left(\frac{\pi_q}{p}\right)_3.$$

where $\left(\frac{\pi_q}{p}\right)_3$ is defined to be the unique number in $\{1, \omega, \omega^2\}$ satisfying

$$\pi_q^{\frac{p^2-1}{3}} \equiv \left(\frac{\pi_q}{p}\right)_3 \pmod p.$$

Proof. The proof is similar to Theorem 9.18.

$$g_q(\chi_{\pi_q})^{p^2} \equiv \sum_{a \in \mathbb{Z}/q\mathbb{Z}} \chi_{\pi_q}(a)\zeta_q^{ap^2} \equiv \chi_{\pi_q}([p]_q^{-2}) \cdot g_q(\chi_{\pi_q}) \equiv \chi_{\pi_q}([p]_q) g_q(\chi_{\pi_q}) \pmod{p\mathbb{Z}[\zeta_{3q}]}$$

Since $g_q(\chi_{\pi_q}) \cdot \overline{g_q(\chi_{\pi_q})} = q$, we have $g_q(\chi_{\pi_q})$ is invertible modulo p and hence can be eliminated from both sides:

$$q^{\frac{p^2-1}{3}} \pi_q^{\frac{p^2-1}{3}} \equiv \chi_{\pi_q}([p]_q) \pmod p \implies \left(\frac{\pi_q}{p}\right)_3 \equiv \left(\frac{p}{\pi_q}\right)_3 \pmod p$$

as $\left(\frac{q}{p}\right)_3 = 1$. This completes the proof. □

9.9. **Primes of the form $x^2 + 27y^2$.** We return to the question raised in the beginning in two special cases.

Lemma 9.20. *Let p be a prime number.*

$$p \equiv 1 \pmod 3 \iff 4p = x^2 + 27y^2 \quad \exists\, x, y \in \mathbb{Z}.$$

Proof. By reduction theory, a set of representatives of $\mathrm{Cl}(-4 \cdot 27)$ is

$$x^2 + 27y^2,\ 4x^2 - 2xy + 7y^2,\ 4x^2 + 2xy + 7y^2.$$

Then one applies the theory of composition. □

Notation 9.21. *Whenever p is a prime with $p \equiv 1 \pmod 3$, we will fix a pair $x_p, y_p \in \mathbb{Z}$ satisfying*

$$4p = x_p^2 + 27y_p^2, \quad x_p \equiv 1 \pmod 3.$$

Note that such a pair exists. We also consider

$$\begin{aligned} 4p = x_p^2 + 27y_p^2 &= (x_p + y_p \cdot 3\sqrt{-3})(x_p - y_p \cdot 3\sqrt{-3}) \\ &= ((x_p + 3y_p) + 6y_p \cdot \omega)\,((x_p - 3y_p) - 6y_p \cdot \omega) \end{aligned}$$

and define

$$\pi_p := \frac{x_p + 3y_p}{2} + 3y_p \cdot \omega \in \mathbb{Z}[\omega].$$

Then

$$\overline{\pi_p} = \frac{x_p - 3y_p}{2} - 3y_p \cdot \omega \in \mathbb{Z}[\omega].$$

Thus $\{\pi_p, \overline{\pi_p}\}$ are all the primary primes in $\mathbb{Z}[\omega]$ that lies above p. Note that $x_p \equiv y_p \pmod 2$ so $\frac{x_p+3y_p}{2}$ is indeed an integer.

Theorem 9.22. *Let p be a prime number, we have*

$$p = x^2 + 27y^2 \ \ \exists\, x, y \in \mathbb{Z} \iff p \equiv 1 \pmod 3,\ \ x^3 \equiv 2 \pmod p \ \text{ has a solution.}$$

Proof of $\Longrightarrow$. One finds quickly that $p \equiv 1 \pmod 3$ from $p = x^2 + 27y^2$. Thus one of x, y is odd and the other is even, i.e. $x + y \equiv 1 \pmod 2$. Then $\pi_p := x + 3\sqrt{-3}y = (x + 3y) + 6y \cdot \omega$ is a prime above p. Replacing x, y by $-x, y$ if necessary, assume that π_p is primary.

It remains to show that $\left(\frac{2}{\pi_p}\right)_3 = 1$. By reciprocity law,

$$\left(\frac{2}{\pi_p}\right)_3 = \left(\frac{\pi_p}{2}\right)_3 = \left(\frac{x + 3y + 6\omega}{2}\right)_3 = \left(\frac{x+y}{2}\right)_3 = \left(\frac{1}{2}\right)_3 = 1.$$

□

Proof of $\Longleftarrow$. By assumption $\left(\frac{2}{\pi_p}\right)_3 = 1$. Also, write $4p = x_p^2 + 27y_p^2$ as above. By reciprocity law,

$$1 = \left(\frac{\pi_p}{2}\right)_3 = \left(\frac{\frac{x_p+3y_p}{2} + 3y_p \cdot \omega}{2}\right)_3.$$

The only element in $\mathbb{Z}[\omega]/2\mathbb{Z}[\omega]$ that is a cube is $1 \pmod 2$. So we must have

$$3y_p \equiv 0 \pmod 2,$$

implying $x_p \equiv y_p \equiv 0 \pmod 2$, so $p = \left(\frac{x_p}{2}\right)^2 + 27\left(\frac{y_p}{2}\right)^2$ with $x_p/2, y_p/2 \in \mathbb{Z}$. □

Remark 9.23. *From the proof, one sees another equivalent condition:* $p \equiv 1 \pmod 3$ *and* x_p *(or equivalently* y_p*) is even.*

9.10. **Supplementary laws.** Although we will not prove it[15], we state the supplementary law to the above cubic reciprocity laws.

Theorem 9.24. *Assume* $p \equiv 1 \pmod 3$ *and* π_p *is primary, written as* $(3m-1)+(3n)\cdot\omega$. *Then*

$$\left(\frac{1-\omega}{\pi_p}\right)_3 = \omega^{2m}, \quad \left(\frac{3}{\pi_p}\right)_3 = \omega^{2n}.$$

Likewise, if a prime number $p \equiv 2 \pmod 3$ *is written as* $p = 3m - 1$, *then* $\left(\frac{1-\omega}{p}\right)_3 = \omega^{2m}$.

Using this, let us prove a statement about cubic root of 3 modulo p, also conjectured by Euler.

Theorem 9.25. *Let* $p \equiv 1 \pmod 3$ *and write* $4p^2 = x_p^2 + 27y_p^2$ *for some* $x_p, y_p \in \mathbb{Z}$. *Then*

$$x^3 \equiv 3 \pmod p \text{ has a solution} \iff y_p \equiv 0 \pmod 3.$$

Proof. Indeed

$$x^3 \equiv 3 \pmod p \text{ has a solution} \iff \left(\frac{3}{\pi_p}\right)_3 = 1.$$

Since $\pi_p = \frac{x_p+3y_p}{2} + 3y_p \cdot \omega$, we have, by the supplementary law,

$$\left(\frac{3}{\pi_p}\right)_3 = \omega^{2y_p}$$

which is equal to one iff $y_p \equiv 0 \pmod 3$. This completes the proof. □

In principle, equipped with Theorem 9.18, 9.19 and 9.24, one should be able to calculate any cubic symbol just as we did before in the quadratic case. Here is one example

Example 9.26. $x^3 \equiv 15 \pmod{19}$ *has no solution.*

Proof. We first find by hand that

$$4 \cdot 19 = 76 = 7^2 + 27 \cdot 1^2.$$

Thus π_{19} can be taken to be $5 + 3\omega$ (or its conjugate, does not matter). It remains to calculate $\left(\frac{15}{\pi_{19}}\right)_3$ using Theorem 9.18, 9.19 and 9.24.

[15] See Ireland–Rosen's book, Chapter 9, Exercises 24-26. It is interesting to note that the proof makes use of the above already established cubic laws.

$$\left(\frac{15}{\pi_{19}}\right)_3 = \left(\frac{3}{\pi_{19}}\right)_3 \cdot \left(\frac{5}{\pi_{19}}\right)_3$$
$$= \omega^{2\cdot 1} \cdot \left(\frac{5+3\omega}{5}\right)_3 = \omega^2 \cdot \left(\frac{\omega}{5}\right)_3$$
$$= \omega^2 \cdot \omega^{\frac{5^2-1}{3}} = \omega \neq 1.$$

□

9.11. **Theta function.** Reference for material presented in the next few sections:

- Diamond, Shurman, A First Course In Modular Forms, section 4.11, 5.9, 5.10;
- Hiramatsu, Saito, Introduction to NonAbelian Class Field Theory, section 1.1.

The book by Diamond–Shurman is an accessible yet modern and comprehensive introduction to modular forms. The book by Hiramatsu and Saito is quite advanced, but the first section is worth reading (one must also mention the write-up of Serre, Modular forms of weight 1 and Galois representation. This is also quite advanced.). I also recommend the beautiful introduction to modular forms by Zagier in the book "The 1-2-3 of Modular Forms". The most relevant material is in the section titled "Binary Quadratic Forms of Discriminant -23".

Definition 9.27. *For $\{\tau \in \mathbb{C}, \mathrm{Im}(\tau) > 0\} = \mathbb{H}$ define the Dedekind eta function*

$$\eta(z) := q^{1/24} \prod_{n=1}^{\infty}(1-q^n),$$

where $q = e^{2\pi i \tau}$. Note that $\eta(\tau)$ is indeed a convergent infinite product. Also define

$$\theta(\tau) := \eta(6\tau)\eta(18\tau) = q \prod_{n=1}^{\infty}(1-q^{6n}) \prod_{n=1}^{\infty}(1-q^{18n}),$$

Define (a_k) by its expansion in q:

$$\theta(\tau) = \sum_{k=1}^{\infty} a_k q^k.$$

Here are a few leading terms

$$\begin{aligned} \theta(\tau) &= q(1-q^6-q^{12}-q^{18}+q^{24}+2q^{30}+....) \\ &= q-q^7-q^{13}-q^{19}+q^{25}+2q^{31}+.... \end{aligned} \tag{34}$$

(see Apostol: Introduction To Analytic Number Theory, Section 14.4)

Lemma 9.28 (Pentagonal Number Theorem)**.**

$$\prod_{n=1}^{\infty}(1-q^n) = \sum_{k=-\infty}^{+\infty} (-1)^k q^{\frac{k(3k-1)}{2}}.$$

Remark 9.29. *When expanding $\frac{1}{\prod_{n=1}^{\infty}(1-q^n)}$, the coefficients are exactly the partition function $p(k)$: the number of different ways of writing $k = k_1 + ... + k_l$, a sum of positive integers.*

Corollary 9.30.

$$\theta(\tau) = \sum_{m,n\in\mathbb{Z}} (-1)^{m+n} q^{\frac{1}{4}\left[(6m-1)^2+3(6n-1)^2\right]}.$$

Let, for $k \in \mathbb{Z}^+$,

$$A_k := \#\left\{(m,n) \in \mathbb{Z}^2 \mid 4k = (6m-1)^2 + 3(6n-1)^2\right\}.$$

Lemma 9.31. *If $p \neq 3$ is a prime, then*

$$A_p = \begin{cases} 0 & \text{if } p \not\equiv 1 \pmod 3, \\ 1 & \text{if } p \equiv 1 \pmod 3,\ p \notin \mathrm{Rep}(x^2+27y^2) \\ 2 & \text{if } p \equiv 1 \pmod 3,\ p \in \mathrm{Rep}(x^2+27y^2) \end{cases}.$$

Moreover, if $A_p = 1$ then $m+n$ is odd, if $A_p = 2$ then $m+n$ is even.

$A_p = 0$ also if $p = 2, 3$.

Corollary 9.32. *For a prime number $p \neq 3$,*

$$a_p = \begin{cases} 0 & \text{if } p \not\equiv 1 \pmod 3, \\ -1 & \text{if } p \equiv 1 \pmod 3,\ p \notin \mathrm{Rep}(x^2+27y^2) \\ 2 & \text{if } p \equiv 1 \pmod 3,\ p \in \mathrm{Rep}(x^2+27y^2) \end{cases}.$$

Remark 9.33. *Thanks to the cubic reciprocity law, this can be rewritten as*

$$a_p = \begin{cases} 0 & \text{if } p \not\equiv 1 \pmod 3, \\ -1 & \text{if } p \equiv 1 \pmod 3,\ x^3 \equiv 2 \pmod p \text{ has no solution} \\ 2 & \text{if } p \equiv 1 \pmod 3,\ x^3 \equiv 2 \pmod p \text{ has solution} \end{cases}.$$

Note that in whichever case,

$$a_p + 1 = \#\left\{x \in \mathbb{Z}/p\mathbb{Z} \;\middle|\; x^3 \equiv 2 \pmod p\right\}.$$

The function η satisfies

$$\eta(-\frac{1}{\tau}) = \sqrt{-i\tau}\cdot\eta(\tau).$$

The function θ is enjoys certain symmetric property so that it becomes a modular form.

Theorem 9.34. *$\theta \in \mathcal{M}_1(3\cdot 6^2, \psi)$ where $\psi(d) = \chi(d)\cdot\left(\frac{d}{3}\right)$. Furthermore, it is a normalized eigenform.*

Here ψ is the transformation of θ under the group

$$\Gamma_0(108) := \left\{\begin{bmatrix} a & b \\ c & d\end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \pmod{108}\right\}.$$

So ψ should really be thought of as the composition

$$\begin{bmatrix} a & b \\ c & d\end{bmatrix} \in \Gamma_0(108) \mapsto \begin{bmatrix} [a]_{108} & [b]_{108} \\ 0 & [d]_{108}\end{bmatrix} \mapsto \chi(d)\left(\frac{d}{3}\right).$$

Also, χ is constructed by a cubic character. Actually from the definition we see that θ is a cusp modular form.

The takeaway is that, the solution to $x^3 \equiv 2 \pmod p$ is encoded in the coefficient of some (weight one)[16] modular form!

9.12. **Proof of Lemma 9.31.** The case when $p \equiv 2 \pmod 3$ is left to the reader.

Recall that whenever $p \equiv 1 \pmod 3$, we have fixed $x_p, y_p \in \mathbb{Z}$ such that

$$4p = x_p^2 + 27y_p^2, \quad x_p \equiv 1 \pmod 3.$$

Consequently

$$p = \pi_p\cdot\overline{\pi_p}, \quad \text{where } \pi_p = \frac{x_p+3y_p}{2} + 3y_p\omega,\ \overline{\pi_p} = \frac{x_p-3y_p}{2} - 3y_p\omega.$$

Both π_p and $\overline{\pi_p}$ are primary primes.

Now suppose we are given $(m,n) \in \mathbb{Z}^2$ such that

$$4p = (6m-1)^2 + 3(6n-1)^2.$$

Then

$$p = ((3m+3n-1)+(6n-1)\omega)\cdot\overline{((3m+3n-1)+(6n-1)\omega)}.$$

Multiply by $(-\omega)\cdot\overline{-\omega}$:

$$p = ((6n-1)+(3n-3m)\omega)\cdot\overline{((6n-1)+(3n-3m)\omega)}.$$

Thus by the UFD property and uniqueness of primary element,

$$(6n-1)+(3n-3m)\omega = \begin{cases} \pi_p = \frac{x_p+3y_p}{2} + 3y_p\omega \\ \text{or} \\ \overline{\pi_p} = \frac{x_p-3y_p}{2} - 3y_p\omega \end{cases}.$$

In the former case,

$$\begin{cases} 6n-1 = \frac{x_p+3y_p}{2} & \implies n = \frac{x_p+3y_p+2}{12} \\ n-m = y_p & \implies m = \frac{x_p+3y_p+2}{12} - y_p \end{cases}.$$

[16] weight 2 modular forms would correspond to elliptic curves.

In the latter case,

$$\begin{cases} 6n-1 = \frac{x_p-3y_p}{2} & \implies n = \frac{x_p-3y_p+2}{12} \\ n-m = -y_p & \implies m = \frac{x_p-3y_p+2}{12} + y_p \end{cases}.$$

Note that if n, m are given by such formulas, then naturally $4p = (6m-1)^2 + 3(6n-1)^2$. The only potential issue is that it is not clear m, n are integers or not. In 1st case

$$m, n \in \mathbb{Z} \iff x_p + 3y_p + 2 \equiv 0 \pmod{12} \iff x_p + 3y_p + 2 \equiv 0 \pmod{4}.$$

In the 2nd case,

$$m, n \in \mathbb{Z} \iff x_p - 3y_p + 2 \equiv 0 \pmod{12} \iff x_p - 3y_p + 2 \equiv 0 \pmod{4}.$$

Recall the remark following Theorem 9.22. If $p \notin \mathrm{Rep}(x^2+27y^2)$, then x_p, y_p are odd. Also, $x_p + 3y_p$ is even. Hence exactly one of

$$x_p + 3y_p + 2 \equiv 0 \pmod{4} \text{ or } x_p - 3y_p + 2 \equiv 0 \pmod{4}$$

would happen, implying that the number of m, n is one. Moreover,

$$m + n \equiv y_p \pmod{2}$$

is odd.

On the other hand, if $p \in \mathrm{Rep}(x^2+27y^2)$, then x_p, y_p are even. Hence $\frac{x_p+3y_p}{2}$ must be odd, implying both

$$x_p + 3y_p + 2 \equiv 0 \pmod{4} \text{ and } x_p - 3y_p + 2 \equiv 0 \pmod{4}$$

are true. So the possibilities of m, n are two. In any case

$$m + n \equiv y_p \pmod{2}$$

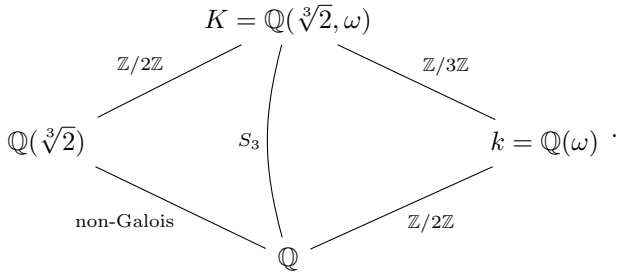
is even.

9.13. **Number fields.** An important goal in algebraic number theory is to study field extensions K of $\mathbb{Q}$ and how primes in p splits in these field extensions. To understand what this means, let us define $\mathcal{O}_K$ to be the algebraic integers contained in K, then it has the following important property (assume $K/\mathbb{Q}$ is Galois)

- Every non-zero ideal of $\mathcal{O}_K$ can be uniquely written as a finite product of prime ideals, which are also maximal ideals. This is a substitute for the UFD property, which does not hold in general. So every prime p, the ideal
$$p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdot ... \mathfrak{P}_r^{e_r}. \tag{35}$$
for some $e_1, ..., e_r$. In the Galois case, actually $e_1 = ... = e_r = e$.
- Each $\mathfrak{P}_i$ is called a prime ideal "above p". It induces a finite field extension: $F_p = \mathbb{Z}/p\mathbb{Z} \to F_{\mathfrak{P}_i} = \mathcal{O}_k/\mathfrak{P}_i$. So there is a corresponding $\mathrm{Frob}_{\mathfrak{P}_i} \in \mathrm{Gal}(F_{\mathfrak{P}_i}/F_p)$. One has a surjection
$$\{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \mid \sigma(\mathfrak{P}_i) = \mathfrak{P}_i\} \to \mathrm{Gal}(F_{\mathfrak{P}_i}/F_p).$$
One often denotes by $\mathrm{Frob}_{\mathfrak{P}_i}$ its lift to $\mathrm{Gal}(K/\mathbb{Q})$, which is well-defined up to conjugation (so if the group is abelian, then it is well-defined).
- There is a number, called "discriminant of $\mathcal{O}_K$". A prime p is unramified (that is, $e_i = 1$ for all i) iff p does not divide this number.
- K is uniquely determined by the set of splitting primes: unramified and r equal to the field extension degree $K/\mathbb{Q}$ (may not be true if $K/\mathbb{Q}$ is not Galois).

Now we consider a specific example $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ and study how prime $p \in \mathbb{Z}^+$ splits in $\mathcal{O}_K$. Let us accept the fact that $p \neq 2, 3 \iff p$ unramified.

Here are the relevant field extensions with Galois group labelled



The splitting pattern then is summarized in the following table ($e := e_1 = ... = e_r$, r is as above and f is the extension degree of the corresponding residue fields: $\mathbb{Z}/p\mathbb{Z} \to \mathcal{O}_K/\mathfrak{P}$):

Condition	**Frob**	**Factor in** K	(e, f, r)
$p \equiv 2 \pmod 3$	(-,-)	$p\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$	$(1, 2, 3)$
$p \equiv 1 \pmod 3$, $\left(\frac{2}{\pi_p}\right)_3 = 1$	id	$p\mathcal{O}_K = \mathfrak{P}_1 \cdots \mathfrak{P}_6$	$(1, 1, 6)$
$p \equiv 1 \pmod 3$, $\left(\frac{2}{\pi_p}\right)_3 \neq 1$	(-,-,-)	$p\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2$	$(1, 3, 2)$

TABLE 2. Splitting of unramified primes $p \neq 2, 3$ in $K = \mathbb{Q}(\omega, \sqrt[3]{2})$

9.14. **Class field theory.** Given a number field k, we have a group $\mathrm{Cl}(\mathcal{O}_k)$ called **ideal class group**, which is trivial iff $\mathcal{O}_k$ is a PID. For certain special k, the ideal class group coincide with our form class group introduced before. This notion has a very important variant. Take an ideal $\mathfrak{m}$ of $\mathcal{O}_k$. Define

$$I_k(\mathfrak{m}) := \{\text{ideals of } \mathcal{O}_k \text{ that is coprime to } \mathfrak{m}\}$$
$$P_{k,1}(\mathfrak{m}) := \{\langle\alpha\rangle \mid \alpha \in \mathcal{O}_k,\ \alpha \equiv 1 \pmod{\mathfrak{m}}\}.$$

Then one can check that $I_k(\mathfrak{m})/P_{k,1}(\mathfrak{m})$ is a group, called the **ray class group** of modulus $\mathfrak{m}$. Class field theory asserts the following:

- There exists a unique Galois extension K/k, called the **ray class field of modulus** $\mathfrak{m}$, such that Lifting Frobenius induces an isomorphism

$$I_k(\mathfrak{m})/P_{k,1}(\mathfrak{m}) \cong \mathrm{Gal}(K/k).$$

  This isomorphism is often referred to as the Artin reciprocity law. It does imply many other reciprocity laws.

Now go back to the special case relevant to us:

- $k = \mathbb{Q}(\omega)$, $K = \mathbb{Q}(\omega, \sqrt[3]{2})$ and $\mathfrak{m} = \langle 6\rangle$.

One can check that indeed, K is the ray class field of modulus $\langle 6\rangle$.

Let us try to understand $I_k(\mathfrak{m})/P_{k,1}(\mathfrak{m})$. If $p \equiv 2 \pmod 3$, then

$$-p \equiv 1 \pmod 3, \quad -p \equiv 1 \pmod 2 \implies -p \equiv 1 \pmod 6.$$

So $\langle p\rangle \in P_{k,1}(\langle 6\rangle)$. Now take $p \equiv 1 \pmod 3$ and $p = \pi_p \cdot \overline{\pi_p}$. Then since already $-\pi_p \equiv 1 \pmod 3$,

$$\begin{aligned}\langle\pi_p\rangle \in P_{k,1}(\langle 6\rangle) &\iff -\pi_p \equiv 1 \pmod 2 \\ &\iff \left(\frac{\pi_p}{2}\right)_3 = \left(\frac{2}{\pi_p}\right)_3 = 1 \\ &\iff x^3 \equiv 2 \pmod p \text{ has a solution.}\end{aligned}$$

By pushing the argument further, one could see that (for $p_1 \equiv p_2 \equiv 1 \pmod 3$)

$$\langle\pi_{p_1}\rangle \equiv \langle\pi_{p_2}\rangle \pmod{P_{k,1}(\langle 6\rangle)} \iff \left(\frac{2}{\pi_{p_1}}\right)_3 = \left(\frac{2}{\pi_{p_2}}\right)_3.$$

For $\langle x\rangle$ coprime to $\langle 6\rangle$, decomposed as $\langle x\rangle = \langle\pi_1\rangle \cdot ...\langle\pi_l\rangle$, define

$$\chi(\langle x\rangle) := \prod_{i=1}^{l} \left(\frac{2}{\pi_{p_i}}\right)_3.$$

So χ induces an isomorphism

$$\overline{\chi} : I_k(\langle 6\rangle)/P_{k,1}(\langle 6\rangle) \cong \{1, \omega, \omega^2\}.$$

On the other hand we can define a homomorphism from $\mathrm{Gal}(K/k) \to \{1, \omega, \omega^2\}$ via

$$\psi : \sigma \mapsto \frac{\sigma(\sqrt[3]{2})}{\sqrt[3]{2}}.$$

Then we have a commutative diagram

$$\begin{array}{ccc} \dfrac{I_k(\langle 6\rangle)}{P_{k,1}(\langle 6\rangle)} & \xrightarrow{\text{Artin map}} & \mathrm{Gal}(K/k) \\ & {\scriptstyle \text{cubic residue } \overline{\chi}} \searrow \quad \swarrow {\scriptstyle \text{cyclotomic char.}\psi} & \\ & \{1,\omega,\omega^2\} & \end{array}.$$

9.15. **L-function.** cf. Diamond–Shurman, section 5.9, page 203.

Define the (Hecke) L-function

$$L(s,\theta)=L(s,\chi):=\sum_{\mathfrak{a}\in I_k(\langle 6\rangle)}\chi(\mathfrak{a})\mathrm{Nm}(\mathfrak{a})^{-s}=\sum_{n=1}^{\infty}a_n n^{-s}.$$

Since the coefficients are multiplicative, we have

$$\begin{aligned} L(s,\chi)&=\prod_{\mathfrak{p}\text{ prime ideal of }\mathcal{O}_k,\,\mathfrak{p}\nmid 6}\frac{1}{1-\chi(\mathfrak{p})\mathrm{Nm}(\mathfrak{p})^{-s}} \\ &=\prod_{p\equiv 2\pmod 3}\frac{1}{1-p^{-2s}}\cdot\prod_{\substack{p\equiv 1\pmod 3\\ \left(\frac{2}{\pi_p}\right)_3=1}}\frac{1}{(1-p^{-s})^2}\cdot\prod_{\substack{p\equiv 1\pmod 3\\ \left(\frac{2}{\pi_p}\right)_3\neq 1}}\frac{1}{1+p^{-s}+p^{-2s}} \end{aligned}$$

where we used $(1-\omega p^{-s})(1-\omega^2 p^{-s})=1+p^{-s}+p^{-2s}$.

Theorem 9.35. *Let $N:=108$. Let $\Lambda(s,\chi):=N^{-s/2}(2\pi)^s\Gamma(s)L(s,\chi)$. Then $L(s,\chi)$ can be meromorphically continued to the whole $\mathbb{C}$. Also, it satisfies the following functional equation*

$$\Lambda(s,\chi)=\pm\Lambda(1-s,\chi).$$

10. Arithmetic of imaginary quadratic fields

10.1. **Notation.** Throughout this lecture, $n\neq 1$ is a positive square-free integer and $K:=\mathbb{Q}(\sqrt{-n})$ is a degree 2 field extension of $\mathbb{Q}$. This extension is sometimes called *imaginary quadratic extension.*

There are two useful maps that shall be used repeatedly. For $\alpha=a+b\sqrt{-n}$, let

$$\mathrm{Nm}(\alpha):=\alpha\cdot\overline{\alpha}=a^2+nb^2,\quad \mathrm{Tr}(\alpha):=\alpha+\overline{\alpha}=2a.$$

For an algebraic number α, its $\mathbb{Q}$-minimal polynomial is the unique smallest degree monic polynomial $f_\alpha\in\mathbb{Q}[X]$ such that $f_\alpha(\alpha)=0$. And α is an algebraic integer iff $f_\alpha\in\mathbb{Z}[X]$. Moreover, if $\alpha\notin\mathbb{Q}$, then

$$f_\alpha(x)=x^2-\mathrm{Tr}(\alpha)\,x+\mathrm{Nm}(x).$$

So $\alpha\in K\setminus\mathbb{Q}$ is an algebraic integer iff $\mathrm{Tr}(\alpha),\mathrm{Nm}(\alpha)\in\mathbb{Z}$.

Also for $x_1,...,x_l\in K$, we let $\langle x_1,...,x_l\rangle$ be the $\mathcal{O}_K$-submodule(definition of $\mathcal{O}_K$?) of K generated by them and $[x_1,...,x_l]$ be the $\mathbb{Z}$-submodule generated by them.

10.2. **Ring of integers.** Algebraic integers of imaginary quadratic extension can be described explicitly

Lemma 10.1. *Let*

$$\mathcal{O}_K:=\begin{cases}\mathbb{Z}[\sqrt{-n}] & n\not\equiv 3\pmod 4\\ \mathbb{Z}\left[\dfrac{1+\sqrt{-n}}{2}\right] & n\equiv 3\pmod 4\end{cases}.$$

Then $\mathcal{O}_K$ is the set of algebraic integers in K.

Proof. Write $\alpha=a+b\sqrt{-n}\in K=\mathbb{Q}[\sqrt{-n}]$. So

$$\alpha\text{ is an algebraic integer }\iff 2a,\ a^2+nb^2\in\mathbb{Z}.$$

This implies that

$$\mathbb{Z}\cdot 1+\mathbb{Z}\cdot\sqrt{-n}\subset\mathcal{O}_K\subset\mathbb{Z}\cdot\frac{1}{2}+\mathbb{Z}\cdot\frac{\sqrt{-n}}{2}.$$

In particular, elements in $\mathcal{O}_K$ are algebraic integers. Since $\mathrm{Tr}\left(\frac{1+\sqrt{-n}}{2}\right)=1$ and $\mathrm{Nm}\left(\frac{1+\sqrt{-n}}{2}\right)=\frac{1+n}{4}$, we find that $\mathcal{O}_K$ belongs to algebraic integers if $n\equiv 3\pmod 4$.

Next we show that if $\alpha\notin\mathbb{Z}[\sqrt{-n}]$ is an algebraic integer, then $n\equiv 3\pmod 4$.

In this case, $a = \frac{1}{2} + m$ for some $m \in \mathbb{Z}$. Thus

$$a^2 + nb^2 = \frac{1}{4} + m + m^2 + nb^2 \in \mathbb{Z}, \text{ which implies } \frac{1}{4} + nb^2 \in \mathbb{Z}.$$

This forces $b \notin \mathbb{Z}$ and $b = \frac{1}{2} + l$ for some $l \in \mathbb{Z}$.

$$\frac{1}{4} + nb^2 = \frac{1+n}{4} + nl + nl^2 \in \mathbb{Z} \implies n \equiv 3 \pmod 4.$$

The proof is now complete. □

There is one reason why we prefer $\mathcal{O}_K$ over $\mathbb{Z}[\sqrt{-n}]$ when $n \equiv 3 \pmod 4$. It will be shown that the ring $\mathcal{O}_K$ has the unique factorization property for ideals whereas $\mathbb{Z}[\sqrt{-n}]$ may not.

10.3. **Ideals associated to quadratic forms.**

Condition 10.1. *From now on till the end of this lecture, $n \not\equiv 3 \pmod 4$.*

should drop this condition!

Notation 10.2. *Let $d_K := -4n$. For a quadratic form $Q = ax^2 + 2bxy + cy^2 \in \mathcal{M}^+_{-4n}$, let $I_Q := \mathbb{Z} \cdot a + \mathbb{Z} \cdot (-b + \sqrt{-n}) = [a, -b + \sqrt{-n}]$.*

Lemma 10.3. *For every $Q \in \mathcal{M}^+_{-4n}$, I_Q is an ideal of $\mathcal{O}_K$.*

Proof. Since I_Q is contained in $\mathcal{O}_K$, it is sufficient to show that I_Q is an $\mathcal{O}_K$-module. As it is already an $\mathbb{Z}$-module, one only needs to check $\sqrt{-n} \cdot I_Q \subset I_Q$:

$$\sqrt{-n} \cdot a = b \cdot a + a \cdot (-b + \sqrt{-n})$$
$$\sqrt{-n} \cdot (-b + \sqrt{-n}) = -b\sqrt{-n} - n = -b\sqrt{-n} + b^2 - ac = -c \cdot a + (-b) \cdot (-b + \sqrt{-n}).$$

So we are done. □

Next we work towards a converse statement.

10.4. **Quadratic forms associated to imaginary quadratic numbers.**

Definition 10.4. *For an algebraic number $\alpha_{\neq 0}$, its $\mathbb{Z}$-minimal polynomial is the unique $f \in \mathbb{Z}[X]$ with positive leading coefficient such that* $\gcd(\text{coeff}(f)) = 1$.

Lemma 10.5. *For $\tau \in K$ with $\text{Im}(\tau) > 0$, let f_τ be its $\mathbb{Z}$-minimal polynomial. Then $f_\tau(x) = ax^2 + 2bx + c$ for some $a, b, c \in \mathbb{Z}$.*

Proof. Write $f_\tau(x) = Ax^2 + Bx + C$ with $A, B, C \in \mathbb{Z}$. We must show B is an even number. If not, $B^2 - 4AC \equiv 1 \pmod 4$.

$$\sqrt{B^2 - 4AC} \in \mathcal{O}_K \implies \sqrt{B^2 - 4AC} = y \cdot \sqrt{-n},\ \exists y \in \mathbb{Z}$$
$$\implies B^2 - 4AC \equiv y^2 \cdot (-n) \equiv 1 \pmod 4.$$

But $y^2 \not\equiv 0 \pmod 4$, so $y^2 \equiv 1 \pmod 4$. Thus $-n \equiv 1 \pmod 4$, a contradiction. □

Notation 10.6. *For every $\tau \in K$ with $\text{Im}(\tau) > 0$, we let $(a_\tau, b_\tau, c_\tau) \in \mathbb{Z}^3$ be the unique set of integers such that $\gcd(a_\tau, 2b_\tau, c_\tau) = 1$, $a_\tau > 0$ and $\tau = \frac{-b_\tau + \sqrt{b_\tau{}^2 - a_\tau c_\tau}}{a_\tau}$. Also let $Q_\tau(x, y) := a_\tau x^2 + 2b_\tau xy + c_\tau y^2$ be the unique (primitive) quadratic form associated to τ.*

Lemma 10.7. *Take $\tau \in K$ with $\text{Im}(\tau) > 0$. Then*

$$[1, \tau] \in \mathcal{O}_K\text{−mod} \iff b_\tau^2 - a_\tau c_\tau = -n.$$

Proof of $\implies$. For simplicity write a, b, c for a_τ, b_τ, c_τ. Also, $\tau = x + y\sqrt{-n}$ for some $x, y \in \mathbb{Q}$.

Find $\lambda_1, ..., \lambda_4 \in \mathbb{Z}$ such that

$$\begin{aligned} \sqrt{-n} \cdot 1 = \lambda_1 + \lambda_2\tau &= (\lambda_1 + \lambda_2 x) + y\lambda_2 \cdot \sqrt{-n} \\ -ny + x \cdot \sqrt{-n} = \sqrt{-n} \cdot \tau &= \lambda_3 + \lambda_4\tau = (\lambda_3 + \lambda_4 x) + y\lambda_4 \cdot \sqrt{-n}. \end{aligned} \tag{36}$$

By comparing coefficients, we get

$$y = \frac{1}{\lambda_2},\ x = -\frac{\lambda_1}{\lambda_2},\ \lambda_4 = \frac{x}{y} = -\lambda_1,\ \lambda_3 = \frac{-n - \lambda_1^2}{\lambda_2}.$$

Thus,

$$\frac{2b}{a} = -\mathrm{Tr}\,(\tau) = -2x = \frac{2\lambda_1}{\lambda_2}$$
$$\frac{c}{a} = \mathrm{Nm}\,(\tau) = x^2 + ny^2 = \frac{\lambda_1^2}{\lambda_2^2} + n\frac{1}{\lambda_2^2} = \frac{n+\lambda_1^2}{\lambda_2}\cdot\frac{1}{\lambda_2} = \frac{-\lambda_3}{\lambda_2}.$$

Since $\lambda_1^2 + \lambda_2\lambda_3 = -n$ and n is square-free, we have $\gcd(\lambda_2, 2\lambda_1, \lambda_3) = 1$, from which it follows that

$$(a, b, c) = \pm(\lambda_2, \lambda_1, \lambda_3).$$

Consequently $b^2 - ac = -n$, as desired. □

Proof of $\Longleftarrow$. It suffices to set $\lambda_1 := b_\tau$, $\lambda_2 := a_\tau$, $\lambda_3 = -c_\tau$ and $\lambda_4 := -b_\tau$ and verify Eq.(36) is true. □

10.5. **Ideals.**

Lemma 10.8. *Every nonzero proper ideal $I \lhd \mathcal{O}_K$ is a rank-2 free $\mathbb{Z}$-module.*

Proof. Take $\alpha_{\neq 0} \in I$, then

$$\mathbb{Z}\cdot\mathrm{Nm}\,(\alpha) + \mathbb{Z}\cdot\mathrm{Nm}\,(\alpha)\sqrt{-n} \subset I \subset \mathbb{Z}\cdot 1 + \mathbb{Z}\cdot\sqrt{-n}$$

is in between two rank 2 free $\mathbb{Z}$-modules. Thus it also has to be so. □

Lemma 10.9. *Every nonzero proper ideal $I \lhd \mathcal{O}_K$ takes the form $I = \dfrac{\alpha}{a_\tau}\cdot I_{Q_\tau}$ for some $\alpha \in I$, $\tau \in K$, $\mathrm{Im}\,(\tau) > 0$. Moreover, $I\cdot\overline{I} = \langle\dfrac{\mathrm{Nm}\,(\alpha)}{a_\tau}\rangle$ with $\mathrm{Nm}\,(\alpha)/a_\tau \in \mathbb{Z}^+$.*

Proof. By last lemma, $I \lhd \mathcal{O}_K$ can be presented as $[\alpha, \beta]$ and we may assume $\mathrm{Im}\,(\beta/\alpha) > 0$. Let $\tau := \alpha/\beta$. Thus

$$[\alpha, \beta] = \alpha\cdot[1, \tau] = \alpha\cdot[1, \frac{b_\tau + \sqrt{-n}}{a_\tau}] = \frac{\alpha}{a_\tau}\cdot I_{Q_\tau}.$$

The rest of the claim follows from

$$\begin{aligned} I_{Q_\tau}\cdot\overline{I_{Q_\tau}} &= [a, -b+\sqrt{-n}]\cdot[a, -b-\sqrt{-n}] \\ &= [a^2, a(b+\sqrt{-n}), a\cdot(2b), b^2+n = ac] = \langle a\rangle. \end{aligned}$$

□

10.6. **Cancellation law and quotients of ideals: Corollary to Lemma 10.9.** We draw a few important corollaries from the fact that each nonzero proper ideal I admits another I' such that $I\cdot I'$ is a principal ideal. The arguments here work word-by-word for general number fields (of course $I\cdot I'$ being principal requires a different proof).

Corollary 10.10. *Let $I, J, \mathfrak{a}$ be nonzero ideals of $\mathcal{O}_K$. Then*

$$I\cdot\mathfrak{a} = J\cdot\mathfrak{a} \implies I = J.$$

Proof. Find $\mathfrak{a}' \lhd \mathcal{O}_K$, $\alpha \in \mathcal{O}_K$ such that $\mathfrak{a}\mathfrak{a}' = \langle\alpha\rangle$. So

$$I\cdot\mathfrak{a} = J\cdot\mathfrak{a} \implies I\cdot\langle\alpha\rangle = J\cdot\langle\alpha\rangle \implies I = J.$$

□

Corollary 10.11. *Let I, J be two nonzero ideals of $\mathcal{O}_K$ with $I \subset J$. Then there exists $\mathfrak{a} \lhd \mathcal{O}_K$ such that $I = J\cdot\mathfrak{a}$.*

Proof. Find $J \lhd \mathcal{O}_K$, $\alpha \in R$ such that $J\cdot J' = \langle\alpha\rangle$. Thus,

$$I\cdot J' \subset J\cdot J' = \langle\alpha\rangle.$$

This shows that $\mathfrak{a} := \dfrac{I\cdot J'}{\alpha}$ is an ideal in $\mathcal{O}_K$. Consequently,

$$I\cdot J' = \langle\alpha\rangle\cdot\mathfrak{a} = J\cdot J'\cdot\mathfrak{a} \implies I = J\cdot\mathfrak{a}$$

by Corollary 10.11.

□

Theorem 10.12. *Every proper nonzero ideal in $\mathcal{O}_K$ can be uniquely written as a product of finitely many prime ideals.*

10.7. **Proof of factorization into prime ideals: Theorem 10.12. First we treat the existence part.**

Assume the conclusion were wrong, find some nonzero proper ideal $I \lhd \mathcal{O}_K$ such that I is maximal among those that can not be written as a product of prime ideals.

Find some maximal (and hence prime) ideal $\mathfrak{p}$ containing I, by Corollary 10.11, $I = \mathfrak{p} \cdot J$ for some $J \lhd \mathcal{O}_K$. Then I is strictly contained in J, implying that J can be written as a product of prime ideals. But then $I = \mathfrak{p} \cdot J$ is also a product of prime ideals. Contradiction.

Next we prove the uniqueness.

Say

$$I = \mathfrak{p}_1 \cdot ... \cdot \mathfrak{p}_n = \mathfrak{q}_1 \cdot ... \cdot \mathfrak{q}_k$$

is a product of prime ideals.

Since $\mathfrak{q}_1 \cdot ... \cdot \mathfrak{q}_k \subset \mathfrak{p}_1$, we have $\mathfrak{p}_1 = \mathfrak{q}_i$ for some i. Up to permutation, $\mathfrak{p}_1 = \mathfrak{q}_1$. By the cancellation law we have

$$\mathfrak{p}_2 \cdot ... \cdot \mathfrak{p}_n = \mathfrak{q}_2 \cdot ... \cdot \mathfrak{q}_k.$$

Repeating the above process we will obtain $k = n$ and $\mathfrak{p}_i = \mathfrak{q}_i$ after some permutation.

10.8. **Splitting pattern of prime numbers in $\mathcal{O}_K$.**

Theorem 10.13. *Let $p \in \mathbb{Z}^+$ be a prime number. Then*

$$p\mathcal{O}_K = \begin{cases} \mathfrak{p}^2 \text{ for some prime } \mathfrak{p} \lhd \mathcal{O}_K,\ \mathfrak{p} = \overline{\mathfrak{p}} & \text{if } p \mid -4n \\ \text{remains prime} & \text{if } p \nmid -4n,\ \left(\frac{-n}{p}\right) \neq 1 \\ \mathfrak{p} \cdot \overline{\mathfrak{p}} \text{ for some prime } \mathfrak{p} \lhd \mathcal{O}_K,\ \mathfrak{p} \neq \overline{\mathfrak{p}} & \text{if } p \nmid -4n,\ \left(\frac{-n}{p}\right) = 1 \end{cases}$$

Conversely, let $\mathfrak{p} \lhd \mathcal{O}_K$ be a nonzero proper prime ideal. Then $\mathfrak{p} \cap \mathbb{Z} = p.\mathbb{Z}$ for some prime number p. Moreover,

$$p\mathcal{O}_K = \begin{cases} \mathfrak{p}^2 & \text{if } p \mid -4n \\ \mathfrak{p} & \text{if } p \nmid -4n,\ \left(\frac{-n}{p}\right) \neq 1 \\ \mathfrak{p} \cdot \overline{\mathfrak{p}} & \text{if } p \nmid -4n,\ \left(\frac{-n}{p}\right) = 1 \end{cases}$$

Only the first part will be provided with a formal proof. Given this, the proof of the second part is not hard and is left to the reader.

Before the proof, let us note that

Lemma 10.14. *Let p be a prime number. Then the prime factorization of $p\mathcal{O}_k$ has only two possibilities*

$$p\mathcal{O}_k = \begin{cases} \mathfrak{p} & \mathfrak{p} \cdot \overline{\mathfrak{p}} = \langle p^2 \rangle \\ \mathfrak{p} \cdot \overline{\mathfrak{p}} & \text{otherwise} \end{cases}$$

It is possible that $\mathfrak{p} = \overline{\mathfrak{p}}$.

Proof. Let $\mathfrak{p}$ be a proper prime ideal containing $p\mathcal{O}_K$. Then $\langle p \rangle = \mathfrak{p} \cdot I$ for some other ideal I. By Lemma 10.9, $\mathfrak{p} \cdot \overline{\mathfrak{p}} = m$ for some integer $m \in \mathbb{Z}^+$. Thus

$$\langle p^2 \rangle = m \cdot (J \cdot \overline{J}) \implies m \mid p^2 \implies m = p \text{ or } p^2.$$

If $m = p$, then we are in the case $p\mathcal{O}_K = \mathfrak{p} \cdot \overline{\mathfrak{p}}$. If $m = p^2$, then $p\mathcal{O}_k = \mathfrak{p}$. □

10.9. **Proof of Theorem 10.13: ramified case.** First we assume $p \mid n$.

Decompose

$$\langle \sqrt{-n} \rangle = \mathfrak{p}_1 \cdot ... \cdot \mathfrak{p}_l$$

Then

$$\langle n \rangle = \mathfrak{p}_1^2 \cdot ... \cdot \mathfrak{p}_l^2 = (\mathfrak{p}_1 \cdot \overline{\mathfrak{p}_1}) \cdot ... \cdot (\mathfrak{p}_l \cdot \overline{\mathfrak{p}_l}).$$

Without loss of generality assume $p \in \mathfrak{p}_1$. By Lemma 10.14, $\mathfrak{p}_1 \cdot \overline{\mathfrak{p}_1} = \langle p \rangle$ or $\langle p^2 \rangle$. But n is squarefree, so the latter case is excluded. So we have $p\mathcal{O}_K = \mathfrak{p}_1 \cdot \overline{\mathfrak{p}_1}$. If $\mathfrak{p}_1 \neq \overline{\mathfrak{p}_1}$, say $\overline{\mathfrak{p}_1} = \mathfrak{p}_2$. Then

$$\langle n \rangle \subset (\mathfrak{p}_1 \cdot \overline{\mathfrak{p}_1})^2$$

a contradiction against the assumption that n is squarefree.

The proof is already complete if n is even. Now assume n is odd, that is $n \equiv 1 \pmod 4$. We need to show $2\mathcal{O}_K = \mathfrak{p}^2$. Let $\mathfrak{p} := [2, 1 + \sqrt{-n}]$. Then

$$\sqrt{-n}(1 + \sqrt{-n}) = (1 + \sqrt{-n}) - (1 + n) \in \mathfrak{p} \implies \mathfrak{p} \in \mathcal{O}_K\text{−mod}.$$

Furthermore,

$$\overline{\mathfrak{p}} = [2, 1 - \sqrt{-n}] = [2, -1 - \sqrt{-n}] = \mathfrak{p}$$
$$\mathfrak{p}^2 = [4, 1 + n, 2(1 - \sqrt{-n}), 2(1 + \sqrt{-n})] = \langle 2 \rangle$$

since $1 + n \equiv 2 \pmod 4$. Note that $\mathfrak{p}$ is certainly a prime.

10.10. **Proof of Theorem 10.13: unramified cases.** So assume $p \nmid -4n$ now.

First we further assume $\left(\frac{-n}{p}\right) = 1$. Then $p \in \mathrm{Rep}(Q)$ for some $Q \in \mathcal{M}^+_{-4n}$. Up to proper equivalence, we assume Q takes the form $px^2 + 2bxy + cy^2$. Therefore I_Q is a prime ideal and

$$I_Q \cdot \overline{I_Q} = [p^2, -bp + p\sqrt{-n}, 2bp, pc] = \langle p \rangle.$$

It remains to show $I_Q \neq \overline{I_Q}$. Otherwise

$$\begin{aligned} &[p, -b + \sqrt{-n}] = [p, -b - \sqrt{-n}] \\ \Longrightarrow\ & b + \sqrt{-n} = A \cdot p + B(-b + \sqrt{-n}) = (Ap - Bb) + B\sqrt{-n}, \ \ \exists\, A, B \in \mathbb{Z} \\ \Longrightarrow\ & B = 1,\ b = Ap - b \implies 2b = Ap \implies p \mid 2b. \end{aligned}$$

But $-4n = (2b)^2 - 4pc$, so $p \mid -4n$. This is a contradiction.

Finally we assume $p\mathcal{O}_K$ is not a prime and show $\left(\frac{-n}{p}\right) = 1$.

By Lemma 10.14, $p\mathcal{O}_K = \mathfrak{p} \cdot \overline{\mathfrak{p}}$ for some prime ideal $\mathfrak{p}$. By Lemma 10.9, $\mathfrak{p} \cdot \overline{\mathfrak{p}} = \langle \frac{\mathrm{Nm}\,(\alpha)}{a} \rangle$ for some $\alpha \in \mathcal{O}_K$ and $a \in \mathbb{Z}^+$. Hence

$$p \mid \mathrm{Nm}\,(\alpha) = x^2 + ny^2 \quad \exists\, x, y \in \mathbb{Z}.$$

This shows $\left(\frac{-n}{p}\right) = 1$.

10.11. **Class groups.**

Definition 10.15. *We define the class group of $\mathcal{O}_K$:*

$$\mathrm{Cl}(\mathcal{O}_K) := \{ \text{ Ideals of } \mathcal{O}_K \} / \{ \text{ principal ideals } \} \text{ equipped with } [I] \cdot [J] := [I \cdot J]$$

That this semigroup is indeed a group follows from Lemma 10.9.

Note that the map

$$ax^2 + 2bxy + cy^2 \mapsto [a, -b + \sqrt{-n}]$$

from $\mathcal{M}^+_{-4n}$ to ideals of $\mathcal{O}_K$ induces a map from $\mathrm{Cl}(-4n)$ to $\mathcal{O}_\mathrm{K}$ (recall $n \not\equiv 3 \pmod 4$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt{-n}]$). We have shown (Lemma 10.9) that this is a surjection.

Lemma 10.16. *This map is an injection.*

Proof. Say the ideals corresponding to $Q = ax^2 + 2bxy + cy^2$ and $Q' = a'x^2 + 2b'xy + c'y^2$ from $\mathcal{M}^+_{-4n}$ are the same modulo principal ideals. That is,

$$[1 : \tau] = \gamma \cdot [1 : \tau'], \quad \exists\, \gamma \in K$$

where $\tau = \frac{-b+\sqrt{-n}}{a}$, $\tau' = \frac{-b'+\sqrt{-n}}{a'}$. Therefore, there exists $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ such that

$$\begin{pmatrix} 1 \\ \tau \end{pmatrix} = \gamma \cdot \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} 1 \\ \tau' \end{pmatrix} \implies \tau = \frac{r + s\tau'}{p + q\tau'}.$$

Since $\mathrm{Im}\,(\tau), \mathrm{Im}\,(\tau') > 0$, we have $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.

The above also implies that

$$\begin{pmatrix} \tau' & 1 \end{pmatrix} \begin{pmatrix} s & p \\ r & q \end{pmatrix} \begin{pmatrix} a & b \\ b & c \end{pmatrix} \begin{pmatrix} s & p \\ r & q \end{pmatrix}^{\mathrm{tr}} \begin{pmatrix} \tau' \\ 1 \end{pmatrix} = \lambda(a\tau^2 + 2b\tau + c) = 0$$

where λ is some constant. As Q' is uniquely determined by τ', we have

$$\begin{pmatrix} s & p \\ r & q \end{pmatrix} \begin{pmatrix} a & b \\ b & c \end{pmatrix} \begin{pmatrix} s & p \\ r & q \end{pmatrix}^{\mathrm{tr}} = \begin{pmatrix} a' & b' \\ b' & c' \end{pmatrix}.$$

In other words Q is properly equivalent to Q'. □

That "Q' is uniquely determined by τ'" can be more precisely stated as

Lemma 10.17. *We have a bijection*

$$\begin{array}{ccc} \{\tau \mid \mathrm{Im}\,(\tau) > 0,\ [\mathbb{Q}(\tau):\mathbb{Q}] = 2\} & \longleftrightarrow & \left\{(a,b,c) \in \mathbb{Z}^3 \mid a, c > 0,\ \gcd(a,b,c) = 1\right\} \\ \tau & \longmapsto & \mathbb{Z}\text{-minimal polynomial} \\ \text{the root with positive imaginary part} & \longleftarrow & ax^2 + bx + c \end{array}$$

Moreover, by restricting to suitable subsets, we get

$$\left\{\tau \mid ...[1,\tau] \text{ is a } \mathbb{Z}[\sqrt{-n}]\text{−mod}\right\} \quad \longleftrightarrow \quad \left\{(a,b,c) \in \mathbb{Z}^3 \mid ...b^2 - 4ac = -4n,\ b \text{ even}\right\}$$

The proof is omitted.
Finally, we show

Theorem 10.18. *The above map* $(a, 2b, c) \mapsto [a, -b + \sqrt{-n}]$ *induces an isomorphism between the groups* $\mathrm{Cl}(-4n) \cong \mathrm{Cl}(\mathbb{Z}[\sqrt{-n}])$ *(*$n \not\equiv 3 \pmod 4$ *as before).*

Proof. It only remains to show that the map respects group structures.

Without loss of generality, we assume (Q, Q' is Lagrange great (i.e., $\gcd(a, a') = 1$ and $b = b'$). Thus

$$[Q] \cdot [Q'] = [aa'x^2 + 2bxy + \frac{c'}{a}y^2]$$

On the other hand,

$$[a, -b + \sqrt{-n}] \cdot [a', -b + \sqrt{-n}] = [aa', a(-b + \sqrt{-n}), a'(-b + \sqrt{-n}), b^2 - n - 2b\sqrt{-n}]$$

Since $\gcd(a, a') = 1$, the above is equal to

$$[aa', -b + \sqrt{-n}],$$

as desired. □

So far we have a good understanding of how primes in $\mathbb{Z}$ "splits" in $\mathcal{O}_K$. However, the understanding of class group of $\mathcal{O}_K$ is less complete. Indeed, a prime $p \nmid -4n$ is represented as $x^2 + ny^2$ iff the prime "above" p is a principal ideal, but we have no criterion to see when this is true. Class field theory relates (subgroups of) class groups to certain field extension of K. This connection will give us a criterion on when p splits into principal prime ideals. Before getting to class field theory, the next lectures will review basic facts about number fields.

11. Field extensions and Galois theory.

This is taken from the appendix of Marcus' book.
We start with a few definitions/facts/notations.

- Given a field extension $K \subset L$, we let $[L : K]$ denote the dimension of L as a K-vector space. It is sometimes referred to as the **degree** of the field extension L/K.
- A subfield $L \subset \mathbb{C}$, which necessarily contains $\mathbb{Q}$, is said to be a **number field** iff $[L : \mathbb{Q}]$ is finite.
- A number $\alpha \in \mathbb{C}$ is said to be an **algebraic number** iff the field generated by α, denoted by $\mathbb{Q}(\alpha)$, is a number field.
- Given an algebraic number α and a number field K, there exist a unique monic irreducible polynomial $f \in K[X]$, called the **minimal polynomial**, such that $f(\alpha) = 0$. Other roots of f are referred to as K-**conjugates** of α. It is not hard to see that $X \mapsto \alpha$ induces

$$\varphi_{K,\alpha} : K[X]/\langle f \rangle \cong K[\alpha] = K(\alpha).$$

- Given a number field K and $f \in K[X]$ irreducible, all roots of f in $\mathbb{C}$ are distinct.
- Given two subfields $K \subset L$ of $\mathbb{C}$, we let $\mathrm{Ebd}(L/K)$ collect all embeddings of L into $\mathbb{C}$ which become identity when restricted to K.

We start by noting that if α is an algebraic number, then $K(\alpha)$ is an extension of K of finite degree. In general, every finitely generated field extension by algebraic numbers has finite degree over $\mathbb{Q}$.

11.1. **Embeddings.** First we show that "there are enough embeddings".

Theorem 11.1. *Given two number fields $K \subset L \subset \mathbb{C}$. $\#\operatorname{Ebd}(L/K) = [L : K]$.*

We start by considering the case $K(\alpha)/K$ for some algebraic number α. Since each $\sigma \in \operatorname{Ebd}(K(\alpha)/K)$ is determined by the image of α, we obtain an injection:

$$\operatorname{Ebd}(K(\alpha)/K) \hookrightarrow \{K\text{-conjugates of } \alpha\}.$$

But this is also surjective. Let β be a K-conjugate of α, we define σ_β by

$$K[\alpha] \xrightarrow{\varphi_{K,\alpha}^{-1}} K[X]/\langle f_\alpha \rangle \xrightarrow{\varphi_{K,\beta}} K[\beta] \xrightarrow{\text{inclusion}} \mathbb{C}$$

Now consider $K(\alpha_1, \alpha_2) = K[\alpha_1, \alpha_2]/K$. Let $K_1 := K(\alpha_1)$ and $K_2 := K_1(\alpha_2) = K(\alpha_1, \alpha_2)$.

Lemma 11.2. *Every $\sigma \in \operatorname{Ebd}(K_1/K)$ admits an extension to some $\sigma' \in \operatorname{Ebd}(K_2/K)$.*

Proof. Let f_2 be the minimal polynomial of α_2 over K_1. Note that $f \mapsto \sigma(f)$, by applying σ to the coefficients, defines an isomorphism between rings (they are fields)

$$\sigma_X : K_1[X]/\langle f_2 \rangle \cong \sigma(K_1)[X]/\langle \sigma(f_2) \rangle$$

Also fix another root β of $\sigma(f_2)$. The desired extension can be defined by

$$K_2 \xrightarrow{\varphi_{K_1,\alpha_2}^{-1}} K_1[X]/\langle f_2 \rangle \xrightarrow{\sigma_X} \sigma(K_1)[X]/\langle \sigma(f_2) \rangle \xrightarrow{\varphi_{K_1(\beta),\beta}} K_1(\beta) \xrightarrow{\text{inclusion}} \mathbb{C}.$$

□

Now fix such an extension σ' for every σ. Sending $\theta \mapsto \theta \circ \sigma'$ defines an injection

$$\operatorname{Ebd}(\sigma'(K_2)/\sigma(K_1)) \hookrightarrow \{\varphi \in \operatorname{Ebd}(K_2/K) \mid \varphi|_{K_1} = \sigma\}.$$

But this is also surjective by counting. LHS has $[K_2 : K_1]$ many elements. Every φ on the RHS is determined by $\varphi(\alpha_2)$, hence has at most $deg(f_2) = [K_2 : K_1]$ many element.

Now let σ vary, RHS forms a disjoint union of $\operatorname{Ebd}(K_2/K)$ showing that $\#\operatorname{Ebd}(K_2/K) = [K_2 : K]$.

The full proof can be completed by an inductive argument.

11.2. **Primitive element.** Given a field extension L/K, an element $\alpha \in L$ is said to be a primitive element iff $L = K(\alpha)$.

Theorem 11.3. *If $K \subset L$ are number fields, then primitive elements exists.*

The proof is based on the last theorem. The essential case is when $L = K(\alpha, \beta)$ for some $\alpha, \beta \in L$. Applying this special case repeatedly yields the general case.

We show that except for finitely many $t \in K$, $L = K(\alpha + t\beta)$. By Theorem 11.1 applied to $L/K(\alpha + t\beta)$,

$$\begin{aligned} L \neq K(\alpha + t\beta) &\implies \sigma(\alpha + t\beta) = \alpha + t\beta \quad \exists\, \sigma_{\neq \mathrm{id}} \in \operatorname{Ebd}(L/K) \\ &\implies \sigma(\alpha) - \alpha = -t \cdot (\sigma(\beta) - \beta) \quad \exists\, \sigma_{\neq \mathrm{id}} \in \operatorname{Ebd}(L/K) \end{aligned}$$

Note that $\sigma \neq \mathrm{id}$ as above implies that $\sigma\beta \neq \beta$ for otherwise $\sigma\alpha = \alpha$ and hence $\sigma = \mathrm{id}$. Therefore $L \neq K(\alpha + t\beta)$ implies that t belongs to the finite list

$$\left\{ -\frac{\sigma(\alpha) - \alpha}{\sigma(\beta) - \beta} \;\middle|\; \sigma_{\neq \mathrm{id}} \in \operatorname{Ebd}(L/K) \right\}.$$

This completes the proof.

11.3. **Normal extension.**

Theorem 11.4. *Let L/K be a finite extension of number fields. We say that this extension is **normal** iff one of the following equivalent conditions is met*

1. *$\sigma(L) \subset L$ for all $\sigma \in \operatorname{Ebd}(L/K)$.*
2. *for every $\alpha \in L$, all K-conjugates of α live in L.*

By Theorem 11.1, for every $\alpha, \alpha' \in L$ that are K-conjugate, there exists $\sigma \in \operatorname{Ebd}(L/K)$ sending α to α'.

So if condition (1) holds, then all K-conjugates of α stays in L. Conversely, $L = K(\alpha_1, ..., \alpha_l)$ for finitely many α_i's. So condition (2) says that σ sends each α_i into L, implying $\sigma(L) \subset L$.

Remark 11.5. *It follows from the definition that for finite field extensions $K \subset F \subset L$. We have L/K normal implies L/F normal.*

11.4. **Normal closure.**

Theorem 11.6. *Given a finite extension L/K of number fields, there exists a finite extension M/L such that M/K is normal.*

The smallest M/L such that M/K is normal is called the **normal closure** of L/K.

Write $L = K(\alpha_1, ..., \alpha_l)$. Let M be the field generated by K and all the K-conjugates of all α_i's. Then M/K is normal be the last theorem.

Notation 11.7. *When L/K is normal, we usually write $\mathrm{Gal}(L/K)$ for the automorphisms of L that fix K pointwise.*

11.5. **Galois correspondence.**

Lemma 11.8. *Assume L/K is normal. Then*

(1) $K = \{x \in L \mid \sigma(x) = x,\ \forall\, \sigma \in \mathrm{Gal}(L/K)\}$;
(2) $K \neq \{x \in L \mid \sigma(x) = x,\ \forall\, \sigma \in H\}$ *for* $H \lneq \mathrm{Gal}(L/K)$.

Proof of (1). The RHS is a field, call it K'. If K' is strictly larger than K, then by Theorem 11.1, there exists nontrivial field embeddings K'/K, which extend to certain $\sigma \in \mathrm{Gal}(L/K)$. Such a σ does not fix K' pointwise. A contradiction. □

Proof of (2). By primitive element theorem, $L = K(\alpha)$. Let f be the K-minimal polynomial of α. So $\deg(f) = [L : K]$.

On the other hand, let

$$f_H(x) := \prod_{\sigma \in H} (x - \sigma(\alpha)).$$

Then f_H, and hence the coefficients of f_H, are fixed by H. But $\deg(f_H) = |H| \lneq [L : K]$, so f_H is not in $K[X]$. Therefore, one of the coefficients of f_H is fixed by H but does not belong to K. □

Theorem 11.9. *Assume L/K is a finite normal extension. For a subgroup H of $\mathrm{Gal}(L/K)$, let $L^H := \{x \in L \mid \sigma(x) = x,\ \forall\, \sigma \in H\}$. Then we have the following bijection*

$$\begin{array}{ccc} \{\textit{Intermediate fields } K \subset F \subset L\} & \cong & \{\textit{Subgroups of } \mathrm{Gal}(L/K)\} \\ F & \longrightarrow & \mathrm{Gal}(L/F) \\ L^H & \longleftarrow & H \end{array}$$

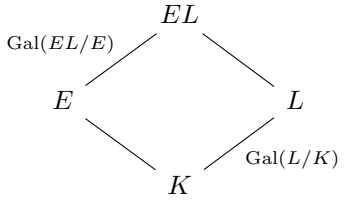
Starting with F, we must show $F = L^{\mathrm{Gal}(L/F)}$, which is just Lemma 11.8.

Starting with $H \leq \mathrm{Gal}(L/F)$, we need to show $H = \mathrm{Gal}(L/L^H)$. That $H \subset \mathrm{Gal}(L/L^H)$ is direct. If this were a strict inclusion, then $L^H \neq L^H$ by part (2) of Lemma 11.8 applied to L/L^H.

11.6. **Composite of field extensions.**

Theorem 11.10. *Take a finite normal extension L/K and a finite extension E/K (not necessarily normal). Let EL be the **composite field** of E and L, namely, the smallest subfield of $\mathbb{C}$ containing E and L. Then*

(1) *the field extension EL/E is normal;*
(2) *the restriction map induces an injective homomorphism $\mathrm{Gal}(EL/E) \to \mathrm{Gal}(L/K)$, which is surjective iff $E \cap L = K$.*



Proof of (1). Take $\sigma \in \mathrm{Ebd}(EL/E)$. Since σ fixes E and hence K, we have

$$\sigma|_L \in \mathrm{Ebd}(L/K) = \mathrm{Gal}(L/K) \implies \sigma(L) \subset L \implies \sigma(EL) \subset EL.$$

□

Proof of (2). Take $\sigma \in \mathrm{Gal}(EL/E)$. Since σ fixes E, σ is trivial iff σ fixes L. This shows the injectivity of the restriction map.

Note that

$$E \cap L = K \iff [EL : E] = [L : K] \iff \#\,\mathrm{Gal}(EL/E) = \#\,\mathrm{Gal}(L/K).$$

Thus the injective homomorphism is surjective iff $E \cap L = K$. □

11.7. **Finite fields.** The morphism $x \mapsto x^{\#\mathcal{O}_K/\mathfrak{p}}$ belongs to and generates $\mathrm{Gal}(F_\mathfrak{q}/F_\mathfrak{p})$.

12. Number fields.

We give in this lecture a quick introduction to algebraic number theory.

Recall that number fields refer to finite field extensions of $\mathbb{Q}$. A number $x \in \mathbb{C}$ is said to be an **algebraic number** iff x is contained in some number field. For such a number x and a number field K, the **K-minimal polynomial** is the unique monic polynomial $f \in K[X]$ of lowest degree such that $f(x) = 0$. The degree of x over K, by definition, is the degree of $f(x)$.

12.1. The ring of algebraic integers.

Lemma 12.1. *An algebraic number $\alpha \in \mathbb{C}$ is said to be an **algebraic integer** iff one of the following equivalent conditions is met:*

1. *the $\mathbb{Q}$-minimal polynomial of α lies in $\mathbb{Z}[X]$;*
2. *there exists a monic polynomial $f \in \mathbb{Z}[X]$ such that $f(\alpha) = 0$.*

Proof. This follows from Gauss' lemma. Details are omitted. □

Notation 12.2. *For a number field K, let $\mathcal{O}_K$ collect all algebraic integers contained in K.*

Proposition 12.3. *$\mathcal{O}_K$ is a ring.*

For the proof, it is useful to note

Lemma 12.4. *Assume K is a number field and $\alpha \in K$. Let $\Lambda \subset K$ be a finitely generated $\mathbb{Z}$-submodule. If α preserves Λ, then $\alpha \in \mathcal{O}_K$.*

Proof. Assume Λ is generated by $x_1, ..., x_k$ for some $x_i \in K$. Then there exists a k-by-k matrix M with $\mathbb{Z}$-coefficients such that

$$\alpha \cdot (x_1, ..., x_k) = (x_1, ..., x_k) \cdot M.$$

Note that this implies

$$(x_1, ..., x_k) \cdot (\alpha I_k - M) = (0, ..., 0).$$

Thus $\alpha I_k - M$ is not invertible (as a square matrix over K), which forces $\det(\alpha I_k - M) = 0$ (otherwise Cramer's rule gives the inverse). But $f(x) := \det(xI_k - M)$ is a monic polynomial in $\mathbb{Z}[X]$. So α is an algebraic integer by Lemma 12.1. □

Proof of Proposition 12.3. Let $\alpha, \beta \in \mathcal{O}_K$ be given. Need to show that $\alpha+\beta$, $\alpha\cdot\beta$ belongs to $\mathcal{O}_K$. In light of Lemma 12.4, it suffices to find a finitely generated $\mathbb{Z}$-submodule Λ of K preserved by them. Assume α has degree l_1 and β has degree l_2 over $\mathbb{Q}$.

Indeed, one may take Λ to be the $\mathbb{Z}$-submodule spanned by $\{\alpha^i\beta^j,\ i = 0, 1, ..., l_1 - 1,\ j = 0, 1, ..., l_2 - 1\}$.

□

12.2. $\mathcal{O}_K$ as a $\mathbb{Z}$-module.

Lemma 12.5. *Let K be a number field of degree l over $\mathbb{Q}$. Then $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank l.*

For the proof, it is useful to make the following definition:

Definition 12.6. *Given a number field $K/\mathbb{Q}$ of degree l and $x_1, ..., x_l \in K$ that forms a basis of K as a $\mathbb{Q}$-vector space. Let $\mathrm{Ebd}(K/\mathbb{Q}) := \{\sigma_1, ..., \sigma_l\}$. We define the discriminant of this l-tuple by*

$$\mathrm{disc}(x_1, ..., x_l) := \det\left(\sigma_i(x_j)\right)^2.$$

Lemma 12.7. *Notation as in last definition.* $\mathrm{disc}(x_1, ..., x_l) \in \mathbb{Q}$.

Proof. If $K/\mathbb{Q}$ is normal, then this follows from Galois theory since it is fixed by every element in $\mathrm{Gal}(K/\mathbb{Q})$.

If not, let $L/\mathbb{Q}$ be its normal closure. Then applying $\sigma\,\mathrm{Gal}(L/\mathbb{Q})$ amounts multiplying by a permutation matrix. Hence $\mathrm{disc}(x_1, ..., x_l)$ is fixed by $\mathrm{Gal}(L/\mathbb{Q})$ and hence lives in $\mathbb{Q}$. □

Proof of Lemma 12.5. Take $x \in \mathcal{O}_K$ of degree $[L; K]$, which exists by primitive theorem. Write $d_x := \mathrm{disc}(1, x, x^2, ..., x^{l-1})$ We are going to show that

$$\mathcal{O}_K \subset \frac{\mathbb{Z} \oplus \mathbb{Z}x \oplus \mathbb{Z}x^2 \oplus ... \oplus \mathbb{Z}x^{l-1}}{d_x}. \tag{37}$$

Since every submodule of a finite generated free $\mathbb{Z}$-module is free, the proof is complete. Take $\alpha \in \mathcal{O}_K$, there exists $\lambda_0, ..., \lambda_{l-1} \in \mathbb{Q}$ such that

$$\alpha = \lambda_0 + \lambda_1 x + ... + \lambda_{l-1} x^{l-1}.$$

Applying $\mathrm{Ebd}(K/\mathbb{Q})$ we get

$$(\sigma_1(\alpha), ..., \sigma_l(\alpha)) = (\lambda_0, ..., \lambda_{l-1}) \cdot \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \sigma_1(x) & \sigma_2(x) & \cdots & \sigma_l(x) \\ \cdots & & & \\ \sigma_1(x^{l-1}) & \sigma_2(x^{l-1}) & \cdots & \sigma_l(x^{l-1}) \end{bmatrix}$$

By Cramer's rule, the inverse of the matrix to the right has coefficients in $\dfrac{\mathcal{O}_K}{d_x}$. This implies that all λ_i's lie in $\dfrac{\mathcal{O}_K}{d_x} \cap \mathbb{Q} = \dfrac{\mathbb{Z}}{d_x}$ and proves Eq.(37). □

12.3. **Finiteness of residue ring.**

Lemma 12.8. *Let K be a number field and $I \triangleleft \mathcal{O}_K$ be a proper nonzero ideal. Then $\mathcal{O}_K/I$ is finite and $I \cong \mathbb{Z}^{\oplus[L:K]}$ as a $\mathbb{Z}$-module.*

Proof. Take $\alpha_{\neq 0} \in I$, then $\mathrm{Nm}\,(\alpha) \in I \cap \mathbb{Z}$ is nonzero. This shows that

$$I \cap \mathbb{Z} = N\mathbb{Z} \quad \exists\, N \in \mathbb{Z}^+.$$

which implies that $N\mathcal{O}_K \subset I \subset \mathcal{O}_K$. But both $N\mathcal{O}_K$ and $\mathcal{O}_K$ are free $\mathbb{Z}$-modules of rank $[L : K]$. Thus so is I. Since $\mathcal{O}_K/N\mathcal{O}_K$ is finite, we have $\mathcal{O}_K/I$ is finite. □

From this lemma we deduce that

Corollary 12.9. *Let K be a number field and $\mathfrak{p} \triangleleft \mathcal{O}_K$ be a nonzero prime ideal. Then $\mathfrak{p}$ is a maximal ideal.*

Proof. Let $x \in \mathcal{O}_K \setminus \mathfrak{p}$, we must show 1 is contained in the ideal generated by x and $\mathfrak{p}$.

Since $\mathcal{O}_K/\mathfrak{p}$ is finite, there exists $m, n \in \mathbb{Z}^+$ such that

$$x^m \equiv x^{m+n} \pmod{\mathfrak{p}}, \text{ which implies } 1 \equiv x^n \pmod{\mathfrak{p}}$$

because $\mathfrak{p}$ is prime. So we are done. □

12.4. **Integrally closed.**

Lemma 12.10. *Let K be a number field. Then $\mathcal{O}_K \subset K$ is **integrally closed**, that is to say, for each monic polynomial $f \in \mathcal{O}_K[X]$ and $\alpha \in K$,*

$$f(\alpha) = 0 \implies \alpha \in \mathcal{O}_K.$$

Proof. Take such a f and x. We need to show $x \in \mathcal{O}_K$, which holds if there exists a finitely generated $\mathbb{Z}$-module Λ in K that is preserved by x.

Write

$$f(x) = x^n + \lambda_1 x^{n-1} + ... + \lambda_n$$

for some λ_i's in $\mathcal{O}_K$. Let $l_i := \deg_{\mathbb{Q}}(\lambda_i)$. Consider the $\mathbb{Z}$-submodule Λ of $\mathcal{O}_K$ generated by

$$\left\{\lambda_1^{i_1} \cdot \lambda_2^{i_2} ... \lambda_n^{i_n} \cdot \alpha^j \mid i_k = 0, ..., l_k - 1,\ j = 0, ..., n-1\right\}$$

It can be directly checked that α preserves Λ and so $\alpha \in \mathcal{O}_K$.

□

12.5. **Dedekind domain.**

Definition 12.11. *Let R be a unital commutative ring. Assume R is an integral domain (i.e., $xy = 0 \implies x = 0$ or $y = 0$). We say R is a **Dedekind domain** if*

(1) *every ideal of R is finitely generated;*
(2) *every proper nonzero prime ideal is maximal;*
(3) *R is integrally closed in its field of fraction $K := Frac(R)$.*

Our efforts so far have shown

Theorem 12.12. *Let K be a number field, then $\mathcal{O}_K$ is a Dedekind domain.*

In the next few subsections we will show

Theorem 12.13. *Let R be a Dedekind domain, then every proper nonzero ideal in R can be uniquely written as products of prime ideals.*

Remark 12.14. *Axiomizing Dedekind domain this way is due to Noether.*

12.6. **Inverse of an ideal modulo principal ideals.**

Theorem 12.15. *Let R be a Dedekind domain and $I \triangleleft R$ be a nonzero proper ideal. Then there exist $J \triangleleft R$ and $\alpha \in R$ such that $I \cdot J = \langle \alpha \rangle$.*

Definition 12.16. *Let K be a number field. Then the set of nonzero ideals of $\mathcal{O}_K$ forms a semigroup under multiplication of ideals. If we say $I \sim J$ iff $I = \alpha J$ for some $\alpha \in K^\times$, and denote by $\mathrm{Cl}(\mathcal{O}_K)$ the set of equivalence classes together with the multiplication $[I] \cdot [J] := [I \cdot J]$. By Theorem 12.15, $\mathrm{Cl}(\mathcal{O}_K)$ is a group, called the **class group**.*

An important theorem, which we shall not prove, is

Theorem 12.17. *$\mathrm{Cl}(\mathcal{O}_K)$ is finite.*

Let us go back to Theorem 12.15. The crucial lemma behind the proof is

Lemma 12.18. *R is a Dedekind domain[17] with fraction field K and I is a nonzero proper ideal of R. Then there exists $x \in K \setminus \mathcal{O}_K$ such that $xI \subset R$.*

Proof of Theorem 12.15 assuming Lemma 12.18. Fix $\alpha_{\neq 0} \in I$ and let $J := \{x \in R \mid xI \subset \langle \alpha \rangle\}$. By definition $I \cdot J \subset \langle \alpha \rangle$ and we wish to show the equality holds.

First we note that

$$I \cdot J \subset \langle \alpha \rangle \iff \frac{I \cdot J}{\alpha} \subset R.$$

And if the first $\subset$ is strict then so is the second. But then, by Lemma 12.18, we can find $\gamma \in K \setminus R$ such that

$$\gamma \cdot J \cdot \frac{I}{\alpha} = \gamma \cdot \frac{I \cdot J}{\alpha} \subset R.$$

Note that $1 \in \frac{I}{\alpha}$ and so $\gamma J \subset R$. But $\gamma J \cdot I \subset \langle \alpha \rangle$ combined with the definition of J implies that $\gamma J \subset J$. Now it is time to invoke Lemma 12.4 to conclude that γ is integral over R and hence lies in R by the Dedekind property. This is a contradiction. □

12.7. **Proof of Lemma 12.18.** If I is principal, this is direct. In general, take $\alpha_{\neq 0} \in I$, we certainly have $\frac{1}{\alpha} \cdot \langle \alpha \rangle \subset R$. We wish to find suitable $\beta \in R \setminus \langle \alpha \rangle$ such that $\frac{\beta}{\alpha} \cdot I \subset R$. This $x := \frac{\beta}{\alpha}$ then satisfies the conclusion.

To construct β, we make use of the following

Lemma 12.19. *Let R be a Dedekind ring[18] and I be a nonzero ideal of R. Then I contains a product of prime ideals.*

Proof. If I is already a prime ideal, there is nothing to prove. In general, let I be a maximal element among those proper ideals that do not contain product of primes and we shall seek for a contradiction.

Since I is not a prime ideal, there exist $x, y \in R \setminus I$ such that $x \cdot y \in I$. As $I + \langle x \rangle$ and $I + \langle y \rangle$ are both strictly larger than I, each of them must contain a product of prime ideals. So their product

$$(I + \langle x \rangle) \cdot (I + \langle y \rangle) = \langle I^2, xI, yI, xy \rangle \subset I$$

also contains a product of prime ideals. A contradiction. □

[17] We do not need the integrally closed assumption.
[18] The integrally closed assumption will not be used.

Now go back to the proof of 12.18. By Lemma 12.19, $\langle\alpha\rangle$ contains a product of primes. We let k be the smallest number such that $\langle\alpha\rangle$ contains a product of k prime ideals:

$$I \supset \langle\alpha\rangle \supset \mathfrak{p}_1 \cdot ... \cdot \mathfrak{p}_k.$$

Let $\mathfrak{p}$ be a prime ideal containing I, then $\mathfrak{p}$ must contain (and hence be equal to) one of $\mathfrak{p}_i$'s. Otherwise, one takes $x_i \in \mathfrak{p}_i \setminus \mathfrak{p}$, then their products $\prod x_i \notin \mathfrak{p}$ but $\prod x_i \in \mathfrak{p}_1 \cdot ... \cdot \mathfrak{p}_k$, a contradiction.

Wlog, assume $\mathfrak{p} = \mathfrak{p}_1$. Take $\beta \in \mathfrak{p}_2 \cdot .... \cdot \mathfrak{p}_k \setminus \langle\alpha\rangle$, which exists by the minimality of k. Then $\beta I \subset \beta\mathfrak{p}_1 \subset \langle\alpha\rangle$, or equivalently, $\dfrac{\beta}{\alpha} \cdot I \subset R$. This completes the proof.

12.8. **Proof of Theorem 12.13.** Just as the case of imaginary quadratic fields, Theorem 12.13 follows from some corollary of Theorem 12.15. We only recall some statements but omit the proof, which is the same.

Lemma 12.20. *Let R be a Dedekind domain and $I, J, \mathfrak{a}$ be nonzero ideals of R. Then*

$$I \cdot \mathfrak{a} = J \cdot \mathfrak{a} \implies I = J.$$

Lemma 12.21. *Let I, J be two nonzero ideals of R with $I \subset J$. Then there exists $\mathfrak{a} \triangleleft R$ such that $I = J \cdot \mathfrak{a}$.*

12.9. **Extension of prime ideals.** Next we study the behaviors of prime ideals under field extensions. We will treat the special case of normal finite extensions.

Definition 12.22. *Let L/K be a normal finite extension of number fields. A prime ideal $\mathfrak{q}$ of $\mathcal{O}_L$ is said to lie over a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ iff $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$. Equivalently, $\mathfrak{q}$ appears in the prime decomposition of $\mathfrak{p} \cdot \mathcal{O}_L$.*

Lemma 12.23. *Given a finite normal extension of number fields L/K. Let $\mathfrak{q}, \mathfrak{q}'$ be two prime ideals of $\mathcal{O}_L$ lying over some prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. Then $\sigma(\mathfrak{q}) = \mathfrak{q}'$ for some $\sigma \in \mathrm{Gal}(L/K)$.*

Proof. Let

$$\mathfrak{a} := \prod_{\sigma \in \mathrm{Gal}(L/K)/\sim} \sigma(\mathfrak{q}), \quad \mathfrak{a}' := \prod_{\sigma \in \mathrm{Gal}(L/K)/\sim} \sigma(\mathfrak{q}')$$

where $\mathrm{Gal}(L/K)/\sim$ is to indicate we modulo the stabilizer of the ideal being acted on.

If the conclusion were wrong, then $\mathfrak{a}$ would be coprime to $\mathfrak{a}'$ (i.e., the ideal generated by them is the full ring). By CRT, we find $x \in \mathcal{O}_L$ satisfying

$$x \equiv 0 \pmod{\mathfrak{a}} \quad x \equiv 1 \pmod{\mathfrak{a}'}.$$

Applying the $\mathrm{Nm}\,()$ map we find

$$\mathrm{Nm}\,(x) \equiv 0 \pmod{\mathfrak{a}} \quad \mathrm{Nm}\,(x) \equiv 1 \pmod{\mathfrak{a}'}.$$

But $\mathrm{Nm}\,(x) \in \mathcal{O}_K$ and $\mathcal{O}_K \cap \mathfrak{a} = \mathcal{O}_K \cap \mathfrak{a}' = \mathfrak{p}$. So

$$\mathrm{Nm}\,(x) \equiv 0 \pmod{\mathfrak{p}} \quad \mathrm{Nm}\,(x) \equiv 1 \pmod{\mathfrak{p}}.$$

A contradiction. □

Notation 12.24. *In light of the above lemma, there exist $e, g \in \mathbb{Z}^+$ and distinct prime ideals $\mathfrak{q}_1, ...\mathfrak{q}_g$ such that*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^e \cdot ... \cdot \mathfrak{q}_g^e.$$

Also, there exists $f \in \mathbb{Z}^+$ such that $f = [\mathcal{O}_L/\mathfrak{q}_i : \mathcal{O}_K/\mathfrak{p}]$ for every i.

Theorem 12.25. *Given a normal extension of number fields $K \subset L$ and $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^e \cdot ... \cdot \mathfrak{q}_g^e$ as above. Then $[L : K] = efg$.*

Proof. By CRT, we have

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \mathcal{O}/\mathfrak{q}_q^e \oplus ... \oplus \mathcal{O}/\mathfrak{q}_g^e.$$

Then we claim that as $\mathcal{O}_L$-module, for any prime ideal $\mathfrak{q}$ of $\mathcal{O}_L$,

$$\mathcal{O}_L/\mathfrak{q} \cong \mathfrak{q}/\mathfrak{q}^2 \cong ... \cong \mathfrak{q}^k/\mathfrak{q}^{k+1}...$$

We only prove the first isomorphism, the rest can be proved similarly. Take $a \in \mathfrak{q} \setminus \mathfrak{q}^2$, define

$$\mathcal{O}_L/\mathfrak{q} \to \mathfrak{q}/\mathfrak{q}^2$$
$$x + \mathfrak{q} \mapsto ax + \mathfrak{q}^2$$

It is quite direct to show that this is an injective morphism. To show surjectivity, note that

$$\langle a\rangle + \mathfrak{q}^2 = \mathfrak{q}.$$

We conclude from above that

$$\#\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = (\#\mathcal{O}_K/\mathfrak{p})^{efg}.$$

On the other hand,

$$\begin{aligned} & \mathcal{O}_L \supset \mathcal{O}_K.v_1 \oplus ... \oplus \mathcal{O}_K.v_k \oplus \text{ finite} \\ \implies & \mathfrak{p}\mathcal{O}_L \supset \mathfrak{p}.v_1 \oplus ... \oplus \mathfrak{p}.v_k \oplus \text{ finite} \\ \implies & \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \sim_{\text{'up to finite part'}} \oplus\mathcal{O}_K.v_i/\mathfrak{p}.v_i \cong \oplus_l \mathcal{O}_K/\mathfrak{p} \end{aligned} \tag{38}$$

where $l = [L;K]$. This shows that

$$\dim_{\mathcal{O}_K/\mathfrak{p}} \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = [L:K] \implies \#\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = (\#\mathcal{O}_K/\mathfrak{p})^{[L:K]}.$$

By comparing with the above computation we finish the proof. □

12.10. **Ramified prime ideals.**

Definition 12.26. *Given a finite normal extension L/K of number fields and a prime ideal $\mathfrak{p} \lhd \mathcal{O}_K$. We say that*

$$\mathfrak{p} \text{ is } \begin{cases} \textbf{ramified} & \text{if } e > 1 \\ \textbf{unramified} & \text{if } e = 1 \\ \textbf{splits completely} & \text{if } e = f = 1 \\ \textbf{intertial} & \text{if } e = g = 1. \end{cases}$$

It is possible to give a criterion on when $\mathfrak{p}$ ramifies.

Theorem 12.27. *Given a finite normal*[19] *extension L/K of number fields, a prime ideal $\mathfrak{p} \lhd \mathcal{O}_K$ and another prime $\mathfrak{q} \lhd \mathcal{O}_L$ above $\mathfrak{p}$.*

$$\mathfrak{p} \text{ ramifies in } \mathcal{O}_L \text{ at } \mathfrak{q} \iff \mathfrak{q} \mid \operatorname{diff}(\mathcal{O}_L/\mathcal{O}_K).$$

where

$$\operatorname{diff}(\mathcal{O}_L/\mathcal{O}_K) := \left\{\alpha \in L \mid \alpha \cdot \{\beta \in L,\ \operatorname{tr}_{L/K}(\beta \cdot \mathcal{O}_L) \subset \mathcal{O}_K\} \subset \mathcal{O}_L\right\}$$

is an ideal of $\mathcal{O}_L$.

There is a case when diff can be calculated more explicitly

Lemma 12.28. *Let L/K be a finite normal extension of number fields. If there exists α such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, then*

$$\operatorname{diff}(\mathcal{O}_L/\mathcal{O}_K) = \langle f'_\alpha(\alpha)\rangle$$

where $f_\alpha \in \mathcal{O}_L[X]$ is the K-minimal polynomial of α.

A key question in algebraic number theory is

Question 12.29. *How to determine the splitting behaviours of unramified prime ideals?*

12.11. **Discriminant.** In this subsection we treat a special case of Theorem 12.27. Let $L/\mathbb{Q}$ be a normal finite extension of degree l. For a $\mathbb{Q}$-basis $(x_1, ..., x_l)$ of L, we have defined what $\operatorname{disc}(x_1, ..., x_l)$ is. And we also fix, in this subsection, a basis $\alpha_1, ..., \alpha_l$ of $\mathcal{O}_L$ as a $\mathbb{Z}$-module.

The discriminant has an geometric analogue. An example is, consider the projection

$$\begin{array}{c} \{(x,y) \in \mathbb{R}^2,\ x = y^2\} \\ \big\downarrow \\ \{x \in \mathbb{R}\} \end{array}$$

In terms of rings, one might think of $\mathbb{R}[x] \to \mathbb{R}[x][\sqrt{x}]$. We think of the projection "ramified" at $x = 0$, which can be detected by $\frac{\mathrm{dx}}{\mathrm{dy}}$ being zero. Here we have something similar:

Lemma 12.30. *If $\mathcal{O}_L = \mathbb{Z}[\alpha]$ and f is the $\mathbb{Q}$-minimal polynomial of α, then* $\operatorname{disc}(\mathcal{O}_L) = (-1)^{\frac{l(l-1)}{2}} \operatorname{Nm}(f'(\alpha))$.

[19] The theorem is stated in a way that the normal assumption can be removed.

Proof. This is a direct calculation. Our assumption $\mathcal{O}_L = \mathbb{Z}[\alpha]$ implies that $\mathcal{O}_L = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\alpha \oplus ... \oplus \mathbb{Z}\cdot\alpha^{l-1}$. Thus (list $\mathrm{Gal}(L/\mathbb{Q}) = \{\sigma_1, ..., \sigma_l\}$)

$$\begin{aligned} \mathrm{disc}(\mathcal{O}_L) =& \mathrm{disc}(1, \alpha, ..., \alpha^{l-1}) \\ (\text{if } l=3) =& \det \begin{pmatrix} 1 & \sigma_1(\alpha) & \sigma_1(\alpha)^2 \\ 1 & \sigma_2(\alpha) & \sigma_1(\alpha)^2 \\ 1 & \sigma_3(\alpha) & \sigma_3(\alpha)^2 \end{pmatrix}^2 \\ =& \prod_{i>j} (\sigma_i(\alpha) - \sigma_j(\alpha))^2 \\ =& (-1)^{l(l-1)/2} \prod_{i\neq j} (\sigma_i(\alpha) - \sigma_j(\alpha)). \end{aligned} \tag{39}$$

On the other hand

$$\begin{aligned} f(x) = \prod (x - \sigma_i(\alpha)) \implies f'(x) &= \sum_i \prod_{j\neq i} (x - \sigma_j(\alpha)) \\ \implies f'(\sigma_k(\alpha)) &= \prod_{j\neq k} (\sigma_k(\alpha) - \sigma_j(\alpha)) = \sigma_k(f'(\alpha)) \end{aligned}$$

Combined with Eq.(39) we have

$$\mathrm{disc}(\mathcal{O}_L) = (-1)^{\frac{l(l-1)}{2}} \cdot \mathrm{Nm}\left(f'(\alpha)\right).$$

□

Let us also point out a relation between diff and disc.

Lemma 12.31. *The absolute norm of* $\mathrm{diff}(\mathcal{O}_L)$ *is equal to* $|\mathrm{disc}(\mathcal{O}_L)|$.

Proof. It can be checked from the definition that

$$\mathrm{diff}(\mathcal{O}_L) \cdot \mathcal{O}_L^* = \mathcal{O}_L$$

where $\mathcal{O}_L^* := \{x \in L \mid \mathrm{Tr}\,(xy) \in \mathbb{Z},\ \forall\ y \in \mathcal{O}_L\}$. Then

$$|\mathcal{O}_L / \mathrm{diff}(\mathcal{O}_L)| = |\mathcal{O}_L^* \mathcal{O}_L / \mathcal{O}_L^* \mathrm{diff}(\mathcal{O}_L)| = |\mathcal{O}_L^* / \mathcal{O}_L|\,.$$

If $(\beta_1, ..., \beta_l)$ is the dual basis to $(\alpha_1, ..., \alpha_l)$ and

$$(\alpha_1, ..., \alpha_l) = (\beta_1, ..., \beta_l) \cdot A$$

for some integral matrix A, then

$$|\mathcal{O}_L^* / \mathcal{O}_L|^2 = |\det A|^2 = \frac{\mathrm{disc}(\alpha_1, ..., \alpha_l)}{\mathrm{disc}(\beta_1, ..., \beta_l)}.$$

But

$$(\sigma_i(\alpha_j)) \cdot (\sigma_j(\beta_i)) = I_l \implies \mathrm{disc}(\alpha_1, ..., \alpha_l) \cdot \mathrm{disc}(\beta_1, ..., \beta_l) = 1$$

So we are done. □

12.12. **Discriminant and ramification.**

Theorem 12.32. *Let $L/\mathbb{Q}$ be a finite normal extension and $p \in \mathbb{Z}^+$ be a prime number. Then*

$$p \text{ ramifies in } \mathcal{O}_L \iff p \mid \mathrm{disc}(\mathcal{O}_L).$$

Idea of $\implies$. The idea is: if $p\mathcal{O}_L$ ramifies, say, as $\mathfrak{p}^2$. This allows us to pick $x_0 \in \mathfrak{p} \setminus p\mathcal{O}_L$. Then x_0 is a primitive vector in $\mathcal{O}_L$, at least at p. Therefore we can complete x_0 to a basis. Then disc of this basis consists of linear combinations of $\sigma(i)(x_0)\sigma_j(x_0)$ which lives in $\mathfrak{p}^2 = p\mathcal{O}_L$. Thus it is divisible by p! □

Proof of $\implies$. Now we start the formal proof. Write $p\mathcal{O}_L = \mathfrak{p} \cdot I$ and assume p ramifies. Then

$$I \text{ is divisible by all prime factors of } p\mathcal{O}_L.$$

Take $\alpha \in I \setminus p\mathcal{O}_L$, written as

$$\alpha = m_1\alpha_1 + ... + m_l\alpha_l, \quad m_i \in \mathbb{Z},\ p \nmid m_1.$$

Thus

$$\mathrm{disc}(\alpha, \alpha_2, ..., \alpha_l) = \mathrm{disc}(m_1\alpha_1, \alpha_2, ..., \alpha_l) = m_1^2\, \mathrm{disc}(\alpha_1, \alpha_2, ..., \alpha_l).$$

Since $p \nmid m_1$, it suffices to show $p \mid \mathrm{disc}(\alpha, \alpha_2, ..., \alpha_l)$. Let me use the case $l = 3$ to illustrate this:

$$\begin{aligned}\mathrm{disc}(\alpha, \alpha_2, ..., \alpha_l) &= \det \begin{pmatrix} \sigma_1(\alpha) & \sigma_1(\alpha_2) & \sigma_1(\alpha_3) \\ \sigma_2(\alpha) & \sigma_2(\alpha_2) & \sigma_1(\alpha_3) \\ \sigma_3(\alpha) & \sigma_3(\alpha_2) & \sigma_3(\alpha_3) \end{pmatrix} \cdot \begin{pmatrix} \sigma_1(\alpha) & \sigma_1(\alpha_2) & \sigma_1(\alpha_3) \\ \sigma_2(\alpha) & \sigma_2(\alpha_2) & \sigma_1(\alpha_3) \\ \sigma_3(\alpha) & \sigma_3(\alpha_2) & \sigma_3(\alpha_3) \end{pmatrix} \\ &= \sum_{i \le j} \sigma_i(\alpha)\sigma_j(\alpha) \cdot \beta_{ij} \quad \exists\, \beta_{ij} \in \mathcal{O}_L\end{aligned}$$

Note that $\sigma_i(\alpha)\sigma_j(\alpha) = \sigma_i(\alpha \cdot \sigma_{j'}(\alpha)) \in p\mathcal{O}_L$: $\alpha \in I$, $\sigma_{j'}(\alpha) \in \sigma_{j'}(I) \subset \mathfrak{p}$ so their product is contained in $I \cdot \mathfrak{p} = p\mathcal{O}_L$.

□

The proof of the other direction uses results in the next subsection.

Proof of $\Longleftarrow$. Now assume

(A) $p \mid \mathrm{disc}(\mathcal{O}_L)$;

(B) $p\mathcal{O}_L = \mathfrak{p}_1 \cdot ... \cdot \mathfrak{p}_g$ factorizes into distinct prime ideals,

from which we will derive a contradiction. Roughly speaking, being unramified implies that the symmetry is faithful when acting on things related to p. But $\mathrm{disc}(\mathcal{O}_L) \equiv 0 \pmod p$ would say the objects that the Galois group could act on is limited. Contradiction arises from this tension.

Let us start the formal proof.

$$\begin{aligned}\text{Condition } A &\implies \mathrm{disc}(\mathcal{O}_L) = \det\left(\mathrm{Tr}\left(\alpha_i\alpha_j\right)\right) \equiv 0 \pmod p \\ &\implies \exists\, m_1 = 1, m_2, ..., m_l \in \mathbb{Z} \text{ s.t.} \\ &\begin{array}{lcccc} m_1\cdot & (\mathrm{Tr}\left(\alpha_1\alpha_1\right), & \mathrm{Tr}\left(\alpha_1\alpha_2\right), & ... & \mathrm{Tr}\left(\alpha_1\alpha_l\right)) \\ & + & & & \\ m_2\cdot & (\mathrm{Tr}\left(\alpha_1\alpha_1\right), & \mathrm{Tr}\left(\alpha_1\alpha_2\right), & ... & \mathrm{Tr}\left(\alpha_1\alpha_l\right)) \\ & + & & & \\ & \vdots & & & \\ & + & & & \\ m_l\cdot & (\mathrm{Tr}\left(\alpha_1\alpha_1\right), & \mathrm{Tr}\left(\alpha_1\alpha_2\right), & ... & \mathrm{Tr}\left(\alpha_1\alpha_l\right)) \\ & \| & & & \\ & \mathbf{0} & & & \end{array} \\ &\pmod p\end{aligned}$$

As a result, if $\alpha := \sum m_i\alpha_i$, then

$$\mathrm{Tr}\left(\alpha \cdot \theta\right) \equiv 0 \pmod p, \quad \forall\, \theta \in \mathcal{O}_L.$$

Note that $\alpha \notin p\mathcal{O}_L \implies \alpha \notin \mathfrak{p}_i$ for some i. Without loss of generality assume this $i = 1$.

On the other hand, we take $\beta \in \mathfrak{p}_2 \cdot ... \cdot \mathfrak{p}_g \setminus \mathfrak{p}_1$ and let

$$D_{\mathfrak{p}_1} := \{\sigma \in \mathrm{Gal}(L/\mathbb{Q}),\ \sigma(\mathfrak{p}_1) = \mathfrak{p}_1\} = \{\varphi_1, ..., \varphi_f\}.$$

be the decomposition group at $\mathfrak{p}_1$. Since $p\mathcal{O}_L$ is unramified, reduction modulo $\mathfrak{p}_1$, $\sigma \mapsto \overline{\sigma}$, induces

$$D_{\mathfrak{p}_1} \cong \mathrm{Gal}(F_{\mathfrak{p}_1}/F_p)$$

An important consequence is that if $\lambda_1, ..., \lambda_f \in \mathbb{Z}$ and

$$\sum_{i=1}^{f} \lambda_i\varphi_i(\theta) \equiv 0 \pmod{\mathfrak{p}_1} \quad \forall\, \theta \in \mathcal{O}_L \implies \lambda_i \equiv 0 \pmod p \quad \forall\, i = 1, ..., f. \tag{40}$$

That is to say, φ_i's are linear independent modulo $\mathfrak{p}$.

Let me illustrate how to get this when $f = 3$. By the existence of primitive element, we find θ_0 such that $F_{\mathfrak{p}_1} = F_p(\theta_0)$. Then $\varphi_i(\theta_0) \neq \varphi_j(\theta_0)$ whenever $i \neq j$. Thus

$$\det \begin{pmatrix} 1 & \varphi_1(\theta_0) & \varphi_1(\theta_0)^2 \\ 1 & \varphi_2(\theta_0) & \varphi_2(\theta_0)^2 \\ 1 & \varphi_3(\theta_0) & \varphi_3(\theta_0)^2 \end{pmatrix} \neq 0.$$

This proves Eq.(40).

Now we combine the condition A and B. For every $\theta \in \mathcal{O}_L$,

$$\mathrm{Tr}\left(\alpha\beta \cdot \theta\right) \equiv 0 \pmod p \implies \mathrm{Tr}\left(\alpha\beta \cdot \theta\right) \equiv 0 \pmod{\mathfrak{p}_1}.$$

But

$$\mathrm{Tr}\,(\alpha\beta\cdot\theta)=\sum_{\sigma\in D_{\mathfrak{p}_1}}\sigma(\alpha\beta\cdot\theta)+\sum_{\sigma\notin D_{\mathfrak{p}_1}}\sigma(\alpha\beta\cdot\theta).$$

We note that $\sigma(\beta)\in\mathfrak{p}_1$ whenever $\sigma\notin D_{\mathfrak{p}_1}$. Thus

$$\sum_{\sigma\in D_{\mathfrak{p}_1}}\sigma(\alpha\beta\cdot\theta)\equiv 0\pmod{\mathfrak{p}_1}\quad\forall\,\theta\in\mathcal{O}_L.$$

Since $\alpha\beta\notin\mathfrak{p}_1$, this implies

$$\sum_{\sigma\in D_{\mathfrak{p}_1}}\sigma(\theta)\equiv 0\pmod{\mathfrak{p}_1}\quad\forall\,\theta\in\mathcal{O}_L.$$

But this contradicts against Eq.(40).

□

12.13. **Decomposition group and Frobenius elements.**

Lemma 12.33. *Let L/K be a finite normal extension of number fields. Let $\mathfrak{p}\lhd\mathcal{O}_K$ be a prime ideal and $\mathfrak{q}\lhd\mathcal{O}_L$ be a prime ideal lying above $\mathfrak{p}$. Then we have an extension of finite fields $F_{\mathfrak{p}}:=\mathcal{O}_K/\mathfrak{p}\to F_{\mathfrak{q}}:=\mathcal{O}_L/\mathfrak{q}$.*

In the unramified case, the Galois group of finite fields is related to the global one.

Definition 12.34. *Given a finite normal extension L/K of number fields, a prime ideal $\mathfrak{p}\lhd\mathcal{O}_K$ and a prime ideal $\mathfrak{q}\lhd\mathcal{O}_L$ lying above $\mathfrak{p}$. The **decomposition group** at $\mathfrak{q}$ is*

$$D_{\mathfrak{q}}:=\{\sigma\in\mathrm{Gal}(L/K)\mid\sigma(\mathfrak{q})=\mathfrak{q}\}.$$

Theorem 12.35. *Notation same as in last lemma. Every $\sigma\in D_{\mathfrak{q}}$ induces some $\overline{\sigma}\in\mathrm{Gal}(F_{\mathfrak{q}}/F_{\mathfrak{p}})$. If $\mathfrak{p}$ is unramified, then $D_{\mathfrak{q}}\cong\mathrm{Gal}(F_{\mathfrak{q}}/F_{\mathfrak{p}})$ via this map.*

In the abelian case, we can lift the distinguished Frobenius in automorphism group of finite fields to $D_{\mathfrak{q}}$.

Lemma 12.36. *Let L/K be a finite abelian extension. For each unramified prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, there exists a unique $\mathrm{Frob}_{\mathfrak{p}}\in\mathrm{Gal}(L/K)$ such that for every prime ideal $\mathfrak{q}$ above $\mathfrak{p}$ one has,*

1. *$\mathrm{Frob}_{\mathfrak{p}}$ preserves $\mathfrak{q}$: $\mathrm{Frob}_{\mathfrak{p}}(\mathfrak{q})=\mathfrak{q}$;*
2. *$\mathrm{Frob}_{\mathfrak{p}}(x)\equiv x^{|\mathcal{O}_K/\mathfrak{p}|}\pmod{\mathfrak{q}}$ for all $x\in\mathcal{O}_L$.*

Corollary 12.37. *Let L/K be a finite abelian extension and $\mathfrak{p}$ be an unramified prime ideal of $\mathcal{O}_K$, the following two are equivalent:*

$$\mathfrak{p}\text{ splits completely in }\mathcal{O}_L\iff\mathrm{Frob}_{\mathfrak{p}}=\mathrm{id}.$$

13. Splitting of primes and reciprocity laws.

13.1. **Cyclotomic fields.** Let q be a prime number and $\zeta_q:=e^{\frac{2\pi i}{q}}$ be a q-th root of unity.

Theorem 13.1. *$f(x):=x^{q-1}+x^{q-2}+\ldots+1$ is the $\mathbb{Q}$-minimal polynomial of ζ_q.*

Since all roots of f are powers of ζ_q, we have $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ is a normal extension of degree $q-1$.

Lemma 13.2. *For $\sigma\in\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$, let $\mathrm{cyc}(\sigma)$ be the element in $(\mathbb{Z}/q\mathbb{Z})^\times$ such that $\sigma(\zeta_q)=\zeta_q^{\mathrm{cyc}(\sigma)}$. Then $\sigma\mapsto\mathrm{cyc}(\sigma)$ gives a canonical isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})=(\mathbb{Z}/q\mathbb{Z})^\times$, called the cyclotomic character.*

Lemma 13.3. *If $K:=\mathbb{Q}[\zeta_q]$, then its ring of integers is $\mathbb{Z}[\zeta_q]$.*

We need to know the whether a prime ramifies in $\mathbb{Z}[\zeta_q]$.

Lemma 13.4. $\mathrm{Nm}\,(\zeta_q-1)=q$.

Proof. Indeed

$$\mathrm{Nm}\,(\zeta_q-1)=\prod_{\sigma\in\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})}(\sigma(\zeta_q)-1)=f(1)=q.$$

□

Lemma 13.5. $\mathrm{disc}(\mathbb{Z}[\zeta_q])=(-1)^{\frac{q-1}{2}}q^{q-2}$.

Proof. By last lecture

$$\operatorname{disc}(\mathbb{Z}[\zeta_q]) = (-1)^{\frac{q-1}{2}} \operatorname{Nm}(f'(\zeta_q))$$

On the other hand,

$$f(x)(x-1) = x^q - 1 \implies f'(x)(x-1) + f(x) = qx^{q-1} \implies f'(\zeta_q) = \frac{q\zeta_q^{q-1}}{\zeta_q - 1}.$$

Hence

$$\operatorname{disc}(\mathbb{Z}[\zeta_q]) = (-1)^{\frac{q-1}{2}} \frac{q^{q-1}\operatorname{Nm}(\zeta_q)^{q-1}}{\operatorname{Nm}(\zeta_q - 1)} = (-1)^{\frac{q-1}{2}} q^{q-2}.$$

□

Corollary 13.6. *If $p \neq q$ is another prime number, then p is unramified in $\mathbb{Z}[\zeta_q]$.*

13.2. **Revisit quadratic reciprocity law.** For simplicity, we only prove the following case of quadratic reciprocity law:

Theorem 13.7. *Let $p \neq q$ be distinct prime numbers. If $p \equiv q \equiv 1 \pmod 4$, then*

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right).$$

Assuming $\left(\frac{q}{p}\right) = 1$, we want to show $\left(\frac{p}{q}\right) = 1$ as well.

Since $q \equiv 1 \pmod 4$, $\left(\frac{-q}{p}\right) = 1$. So $x^2 + q$ splits as a product of two linear functions in $(\mathbb{Z}/p\mathbb{Z})[X]$. Thus we have ring isomorphisms

$$\mathbb{Z}[\sqrt{-q}] \cong \mathbb{Z}[X]/\langle X^2 + q\rangle,$$

which implies that

$$\mathbb{Z}[\sqrt{-q}]/p\mathbb{Z}[\sqrt{-q}] \cong \mathbb{Z}/p\mathbb{Z}[X]/\langle \overline{X^2+q}\rangle \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

is not a field. Since $p \nmid -4q = \operatorname{disc}(\mathbb{Z}[\sqrt{-q}])$, we conclude that

$$p\mathbb{Z}[\sqrt{-q}] = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \text{ with } \mathfrak{p}_1 \neq \mathfrak{p}_2. \tag{41}$$

That is to say, p splits completely in $\mathbb{Q}[\sqrt{-q}]$.

On the other hand $p \nmid \operatorname{disc}(\mathbb{Z}[\zeta_q])$, so p is unramified in $\mathbb{Z}[\zeta_q]$. Say

$$p\mathbb{Z}[\zeta_q] = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_g.$$

Also, we have

$$\operatorname{Frob}_p(\zeta_q) \equiv \zeta_q^p \pmod{\mathfrak{p}_i} \quad \forall\, i = 1, \ldots, g.$$

The order of Frob_p is the extension degree of $F_{\mathfrak{p}_i}/F_p$, which is equal to $\dfrac{q-1}{g}$. If $2 \mid g$, then

$$\operatorname{ord}(\operatorname{Frob}_p) \,\Big|\, \frac{q-1}{2}, \text{ which implies } 1 \equiv \zeta_q^{p^{(q-1)/2}} \equiv \operatorname{Frob}_p^{(q-1)/2}(\zeta_q) \pmod{\mathfrak{p}_i}$$
$$\implies p^{\frac{q-1}{2}} \equiv 1 \pmod q \implies \left(\frac{p}{q}\right) = 1.$$

And the proof would be complete.

It only remains to explain that $2 \mid g$ is indeed true, which would follow from Eq.(41).

Let H be the unique index 2 subgroup of $\operatorname{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$. Then $K := \mathbb{Q}(\zeta_q)^H$ is a quadratic extension of $\mathbb{Q}$ by Galois theory. Since every prime different from q is unramified, a calculation of discriminant shows that K must be $\mathbb{Q}(\sqrt{-q})$ (note that 2 ramifies in $\mathbb{Q}(\sqrt{q})$, which has discriminant $4q$).

Now we can invoke Eq.(41) to conclude that $2 \mid g$.

13.3. **Artin's reciprocity law: unramified case.**

Definition 13.8. *For K a number field, a normal extension L/K is said to be the **Hilbert class field** of K iff*

1. *L/K is unramified: every prime ideals of $\mathcal{O}_K$ is unramified in L;*
2. *L/K is abelian: $\operatorname{Gal}(L/K)$ is abelian;*
3. *$[L : K] = |\operatorname{Cl}(\mathcal{O}_K)|$.*

Theorem 13.9. *Let L/K be the Hilbert class field of a number field K, $\mathfrak{p} \lhd \mathcal{O}_K$ be a prime ideal and $\operatorname{Frob}_\mathfrak{p} \in \operatorname{Gal}(L/K)$ be its Frobenius. Then the map $\mathfrak{p} \mapsto \operatorname{Frob}_\mathfrak{p}$ induces a group isomorphism $\operatorname{Art}_{L/K} : \operatorname{Cl}(\mathcal{O}_K) \cong \operatorname{Gal}(L/K)$, called the **Artin reciprocity map**.*

13.4. **Explicit prime factorizations.**

Lemma 13.10. *Let L/K be a finite normal extension and*

(1) *$\alpha \in \mathcal{O}_L$ with $L = K(\alpha)$, and $\varphi \in \mathcal{O}_K[X]$ is the K-minimal polynomial of α;*
(2) *$\mathfrak{p} \lhd \mathcal{O}_K$ is an unramified prime ideal. Let $f, g \in \mathbb{Z}^+$ be its various indices.*
(3) *g' is a positive number and $\varphi_i \in \mathcal{O}_K[X]$ $(i = 1, ..., g')$ is such that*

$$\varphi \equiv \varphi_1 \cdot ... \cdot \varphi_{g'}$$

is the prime factorization of φ in $\mathcal{O}_K/\mathfrak{p}[X]$.
(4) *Assume that $\overline{\varphi}$ is separable in $\mathcal{O}_K/\mathfrak{p}[X]$, that is, all roots of $\overline{\varphi}$ in the algebraic closure of $\mathcal{O}_K/\mathfrak{p}$ are all distinct.*

The conclusions are

(a) *$\mathfrak{P}'_i := \langle \mathfrak{p}, \varphi_i(\alpha) \rangle$ is a prime ideal in $\mathcal{O}_L$ for each $i = 1, ..., g'$;*
(b) *$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}'_1 \cdot ... \cdot \mathfrak{P}'_{g'}$ is the prime decomposition of $\mathfrak{p}\mathcal{O}_L$.*

Note that $\overline{\varphi}$ being separable is equivalent to $\mathrm{Nm}_K(\varphi'(\alpha)) \notin \mathfrak{p}$.

Corollary 13.11. *Assumption as above, $\mathfrak{p}$ splits completely in L iff $\varphi(x) \equiv 0 \pmod{\mathfrak{p}}$ has a solution.*

Proof. Write $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdot ... \cdot \mathfrak{P}_g$ for the prime decomposition. Since L/K is normal, $\varphi(x) = \prod_{i=1}^{l}(x - \sigma_i(\alpha))$ where $\mathrm{Gal}(L/K) = \{\sigma_1, ..., \sigma_l\}$. Modulo $\mathfrak{P}_1$, we find

$$\begin{aligned} \varphi(x) &\equiv \prod_{i=1}^{l}(x - \sigma_i(\alpha)) \equiv \varphi_1(x) \cdot ... \cdot \varphi_{g'}(x) \pmod{\mathfrak{P}_1} \\ \Longrightarrow \overline{\varphi_i}(x) &= \prod_{k \in I_i}(x - \overline{\sigma_k(\alpha)}) \quad \forall\, i = 1, ..., g' \end{aligned}$$

for certain subsets $\sqcup_i I_i = \{1, ..., l\}$.

Thus for $k \in I_i$, $\varphi_i(\sigma_k(\alpha)) \in \mathfrak{P}_1$. On the other hand, $\sigma_i(\alpha) \not\equiv \sigma_j(\alpha) \pmod{\mathfrak{P}_1}$ by the separability assumption. Therefore, $\varphi_i(\sigma_k(\alpha)) \notin \mathfrak{P}_1$ if $k \notin I_i$. Pulling out the σ_k's,

$$\varphi_i(\alpha) \in \sigma_k^{-1}(\mathfrak{P}_1) \iff k \in I_i.$$

In particular

$$\sigma_k^{-1}(\mathfrak{P}_1) \neq \sigma_{k'}^{-1}(\mathfrak{P}_1) \quad \text{if } k, k' \text{ belongs to different } I'_i s \tag{42}$$

So $g \geq g'$.

On the other hand,

$$\begin{aligned} &\begin{cases} \mathcal{O}_L \supset \mathcal{O}_K[\alpha] \supset \mathrm{disc}(1, \alpha, ..., \alpha^{l-1})\mathcal{O}_L \\ \mathrm{disc}(1, \alpha, ...) = \pm \mathrm{Nm}_K(\varphi'(\alpha)) \text{ is coprime to } \mathfrak{p} \end{cases} \\ \Longrightarrow\ &\mathcal{O}_L/\mathfrak{P}_i = \mathcal{O}_K/\mathfrak{p}[\alpha] \quad \forall\, i = 1, ..., g. \end{aligned}$$

Same argument shows that $\mathcal{O}_L/\mathfrak{P}_1 = \mathcal{O}_K/\mathfrak{p}[\alpha_i]$ for all $i = 1, ..., l$, which implies that $\deg(\varphi_i) = f = [\mathcal{O}_L/\mathfrak{P}_1 : \mathcal{O}_K/\mathfrak{p}]$ for every i. In particular, $g' = g$.

Now Eq.(42) can be promoted to

$$\sigma_k^{-1}(\mathfrak{P}_1) \neq \sigma_{k'}^{-1}(\mathfrak{P}_1) \iff k, k' \text{ belongs to different } I'_i s$$

In other words, for each $i \in \{1, ..., g\}$, $\{\sigma_k^{-1},\ k \in I_i\}$ is a right coset of $D_{\mathfrak{P}_1}$, from which we conclude the existence of unique $\tau_i \in \{1, ..., g\}$ such that

$$\varphi_i(\alpha) \in \mathfrak{P}_{\tau_i} \setminus \bigcup_{j \neq \tau_i} \mathfrak{P}_j.$$

This shows that

$$\langle \mathfrak{p}, \varphi_i(\alpha) \rangle \not\subset \bigcup_{j \neq \tau_i} \mathfrak{P}_j \quad \text{which implies that } \langle \mathfrak{p}, \varphi_i(\alpha) \rangle = \mathfrak{P}_{\tau_i}.$$

□

13.5. **An example of Hilbert class field.** In this subsection we set

- $K := \mathbb{Q}(\sqrt{-14})$ and $L := \mathbb{Q}(\sqrt{-14}, \sqrt{2\sqrt{2}-1})$.

It is easy to see that L/K is a degree 4 extension. Indeed, the K-minimal polynomial of $\alpha := \sqrt{2\sqrt{2}-1}$ is $\varphi(x) = (x^2+1)^2 - 8 = x^4 + 2x^2 - 7$.

Lemma 13.12. *L/K is normal.*

However, $L/\mathbb{Q}$ is not normal.

Proof. Let us list Galois conjugates of $\sqrt{2\sqrt{2}-1}$ over K:

$$\sqrt{2\sqrt{2}-1},\ -\sqrt{2\sqrt{2}-1},\ \sqrt{-2\sqrt{2}-1},\ -\sqrt{-2\sqrt{2}-1}.$$

Only needs to check $\sqrt{-2\sqrt{2}-1} \in L$:

$$\sqrt{2\sqrt{2}-1} \in L \implies \sqrt{2} \in L \implies \sqrt{-7} \in L$$
$$\sqrt{2\sqrt{2}-1} \cdot \sqrt{-2\sqrt{2}-1} = \sqrt{-7} \implies \sqrt{-2\sqrt{2}-1} = \frac{\sqrt{-7}}{\sqrt{2\sqrt{2}-1}} \in L.$$

□

Lemma 13.13. $\mathrm{Gal}(L/K) \cong \mathbb{Z}/4\mathbb{Z}$.

Proof. Elements in $\mathrm{Gal}(L/K)$ are in bijection with Galois conjugates of $\sqrt{2\sqrt{2}-1}$. We consider the unique $\sigma \in \mathrm{Gal}(L/K)$ sending $\sqrt{2\sqrt{2}-1}$ to $\sqrt{-2\sqrt{2}-1}$. Then

$$\sqrt{-7} = \frac{\sqrt{-14}\cdot 2}{(2\sqrt{2}-1)^2+1} \implies \sigma(\sqrt{-7}) = -\sqrt{-7}$$
$$\implies \sqrt{-2\sqrt{2}-1} = \frac{\sqrt{-7}}{\sqrt{2\sqrt{2}-1}} \mapsto \frac{-\sqrt{-7}}{\sqrt{-2\sqrt{2}-1}} = -\sqrt{2\sqrt{2}-1}.$$

This shows that $\sigma^2(\sqrt{2\sqrt{2}-1}) = -\sqrt{-2\sqrt{2}-1}$. So $\sigma^2 \neq \mathrm{id}$ has order 4, implying that $\mathrm{Gal}(L/K) \cong \mathbb{Z}/4\mathbb{Z}$. □

For K, we have shown

- $\mathcal{O}_K = \mathbb{Z}[\sqrt{-14}]$ and $\mathrm{disc}(\mathcal{O}_K) = -56 = -2^3 \cdot 7$;
- $p \neq 2, 7 \iff p$ is unramified in K;
- $p \neq 2, 7$, $\left(\frac{-14}{p}\right) = 1 \iff p$ is unramified and splits in K.

Question 13.14. *Fixing a prime number $p \neq 2, 7$, $\left(\frac{-14}{p}\right) = 1$, hence $p\mathcal{O}_K = \mathfrak{p} \cdot \overline{\mathfrak{p}}$ for some prime ideal $\mathfrak{p} \triangleleft \mathcal{O}_L$. When is $\mathfrak{p}$ principal?*

If L is the Hilbert class field of K, then Artin's reciprocity law implies that $\mathfrak{p}$ principal iff $\mathrm{Frob}_{\mathfrak{p}}$ is trivial, which, by Corollary 13.11, is equivalent to $\varphi(x) \equiv 0 \pmod{\mathfrak{p}}$ has a nontrivial solution.

Lemma 13.15. *L/K is an unramified extension.*

Proof. We will need to decompose L/K into two quadratic extensions:

$$\begin{array}{c} L = K(\sqrt{2\sqrt{2}-1}) \\ | \\ K' = K(\sqrt{2}) = K(\sqrt{-7}) \\ | \\ K = \mathbb{Q}(\sqrt{-14}) \end{array}$$

The desired conclusion would follow from that K'/K and L/K' are both unramified.

Note that for $\beta \in \mathcal{O}_L$ (or $\mathcal{O}_{K'}$) with minimal polynomial ϕ, we have $\mathfrak{p} \nmid \mathrm{Nm}\,(\phi'(\beta)) \implies \mathfrak{p}$ is unramified. We will construct various β to show all primes are unramified.

K'/K is unramified.

Take $\beta := \sqrt{2}$, then

$$\phi(x) = x^2 - 2 \implies \phi'(\sqrt{2}) = 2\sqrt{2} \implies \mathrm{Nm}\left(\phi'(\sqrt{2})\right) = 8.$$

So $\mathfrak{p} \nmid 2 \implies \mathfrak{p}$ unramified.

Take $\beta := \frac{1+\sqrt{-7}}{2}$, we get

$$\phi(x) = x^2 - x + 2 \implies \phi'(\frac{1+\sqrt{-7}}{2}) = 2 \cdot \frac{1+\sqrt{-7}}{2} - 1 = \sqrt{-7}$$
$$\implies \mathrm{Nm}\left(\phi'(\frac{1+\sqrt{-7}}{2}\right) = -7.$$

So $\mathfrak{p} \nmid 7 \implies \mathfrak{p}$ unramified.

L/K' is unramified.

Take $\beta := \dfrac{\sqrt{2\sqrt{2}-1} + \sqrt{-2\sqrt{2}-1}}{2}$. Its trace is 0 and norm is $\frac{1-\sqrt{-7}}{2}$. So its minimal polynomial over K' is $\phi(x) = x^2 - \dfrac{1-\sqrt{-7}}{2}$.

$$\phi'(\beta) = \sqrt{2\sqrt{2}-1} + \sqrt{-2\sqrt{2}-1} \implies \mathrm{Nm}\left(\phi'(\beta)\right) = 2(1-\sqrt{-7})$$
$$\implies \mathrm{Nm}_K(\beta) = 32.$$

So primes not above 2 are unramified.

Take $\beta := \dfrac{\sqrt{2}+1+\sqrt{2\sqrt{2}-1}}{2}$. Its trace is $\sqrt{2}+1$ and norm is $\frac{1}{4}\left((\sqrt{2}+1)^2 - (2\sqrt{2}-1)\right) = 1$. So $\phi(x) = x^2 - (\sqrt{2}+1)x + 1$.

$$\phi'(\beta) = 2 \cdot \frac{\sqrt{2}+1+\sqrt{2\sqrt{2}-1}}{2} - (\sqrt{2}+1) = \sqrt{2\sqrt{2}-1}$$
$$\implies \mathrm{Nm}_{K'}(\phi'(\beta)) = -(2\sqrt{2}-1) \implies \mathrm{Nm}_K(\phi'(\beta)) = -7.$$

So primes not above 7 are unramified.

□

We knew that $\mathrm{Cl}(\mathcal{O}_K) = \mathrm{Cl}(\mathbb{Z}[\sqrt{-14}]) \cong \mathrm{Cl}(-4 \cdot 14)$.

Lemma 13.16. $\#\mathrm{Cl}(-4 \cdot 14) = 4$.

Proof. It suffices to list all positive definite reduced forms of discriminant -56:

$$x^2 + 14y^2,\ 2x^2 + 7y^2,\ 3x^2 \pm 2xy + 5y^2.$$

□

Summarizing efforts made:

Lemma 13.17. *L is the Hilbert class field of K.*

13.6. **Primes of the form $x^2 + 14y^2$.**

Theorem 13.18. *Assume $p \neq 2, 7$ is a prime number.*

$$p = x^2 + 14y^2 \quad \exists\, x, y \in \mathbb{Z} \iff p \equiv 1, 3, 5, 9, 13, 15, 19, 23, 25, 27, 39, 45 \pmod{56};$$
$$x^4 + 2x^2 - 7 \equiv 0 \pmod{p} \quad \textit{has a solution.}$$

Proof.

$$p = x^2 + 14y^2 \iff \text{In } K, p \text{ splits into two different principal ideals } : p\mathcal{O}_K = \mathfrak{p} \cdot \overline{\mathfrak{p}}$$
$$\iff \text{In } K, p \text{ splits as } \mathfrak{p} \cdot \overline{\mathfrak{p}} \text{ and } \mathfrak{p} \text{ splits completely in } L$$
$$\iff \left(\frac{-14}{p}\right) = 1, \quad \mathrm{Frob}_{\mathfrak{p}} = \mathrm{id}$$
$$\iff \left(\frac{-14}{p}\right) = 1, \quad x^4 + 2x^2 - 7 \equiv 0 \pmod{\mathfrak{p}} \text{ has a solution.}$$

It remains to calculate $\left(\dfrac{-14}{p}\right)$ and note that $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z}$. □

13.7. **Existence of Hilbert class field.**

Theorem 13.19. *Let K be a number field. There exists a unique Hilbert class field for K.*