PMATH 641: ALGEBRAIC NUMBER THEORY NOTES

HEESUNG YANG

1. January 05: Modules

One can think of modules as "vector spaces" over some (commutative) ring R. Note that throughout this course we will always assume that R is a commutative ring with unity 1. But of course, this way of looking at modules is true in some way but also not true in other ways. Rather than starting off with definitions we will start with concrete examples such as $\mathbb{Z}$-modules, which are equivalent to abelian groups.

Example 1.1. If $R = \mathbb{Z}$, then a $\mathbb{Z}$-module is an abelian group and vice versa. We also know that $\mathbb{Z}/n\mathbb{Z}$ is a $\mathbb{Z}$-module, one example where a module over an infinite ring need not be infinite. (Compare this to vector spaces.)

Example 1.2. For any ring R, an ideal of R is an R-submodule of R (which can be viewed as an R-module).

Question. What are all the $\mathbb{Z}$-submodules of $\mathbb{Z}[i]$, *the ring of Gaussian integers*? What about $\mathbb{Z}[i]$-submodules?

Solution: For the first part, start with the fact that $\mathbb{Z} \times \mathbb{Z} \cong \mathbb{Z}[i]$ as an abelian group. We are looking for abelian subgroups of $\mathbb{Z}^2 \cong \mathbb{Z}[i]$ as an abelian group. These are $\{0\} \cong \{(0,0)\}, (a+bi)\mathbb{Z}, \{x\mathbb{Z} + y\mathbb{Z} : x, y \in \mathbb{Z}[i]\}$.

For the second part, we are looking for ideals of $\mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is a PID (since $\mathbb{Z}$ is Euclidean), these are exactly the ideals of the form $(a+bi)\mathbb{Z}[i]$ for fixed $a, b \in \mathbb{Z}$.

Definition 1.3. If $S \subset M$ is a subset, then *the R-submodule of M generated by S* is the intersection of all R-submodules of M that contains S. If $S = \{m_1, \ldots, m_r\}$ is finite, then this is $Rm_1 + Rm_2 + \cdots + Rm_r$.

2. January 07: More on modules

Definition 2.1. A *homomorphism of R-modules* $f : M \to N$ is a function such that $f(rm+n) = rf(m) + f(n)$ for all $m, n \in M, r \in R$. The *kernel of f* and *image of f* are defined as follows:

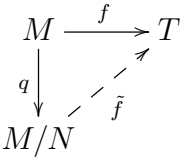
$$\ker f = \{m \in M : f(m) = 0\}$$
$$\operatorname{im} f = \{n \in N : n = f(m) \text{ for some } m \in M\}.$$

Definition 2.2. If $N \subset M$ are R-modules, then the quotient R-module is M/N where the addition comes from the quotient abelian group M/N, and

$$r(m+N) = rm + N.$$

Date: 20 July 2016.

Proposition 2.3 (Universal property of quotients)**.** *Let M, T be R-modules and $N \subset M$ a submodule. Let $f : M \to T$ be a homomorphism and let $q : M \to M/N$ be the quotient homomorphism ($q(m) = m + N$).*



Then there exists a homomorphism $\tilde{f} : M/N \to T$ satisfying $\tilde{f} \circ g = f$ if and only if $\ker f \subset N$. Moreover, if $\tilde{f}$ exists then it is unique.

Question. Let $f : M \to N$ be a homomorphism of modules. Let $M_1 \subset M$ and $N_1 \subset N$ be submodules. Prove that $f(M_1)$ and $f^{-1}(N_1)$ are submodules of N and M, respectively.

Proof. Suffices to verify the scalar multiplication. Straightforward exercise. □

Definition 2.4. Let R be a Noetherian ring. An R-module is *Noetherian* if and only if it is finitely generated.

Remark 2.1. Note that our definition works provided that R is a Noetherian ring. But this does not matter because throughout this course we will always assume that R is Noetherian.

2.1. **Algebraic integers.**

Question. Which algebraic numbers are (algebraic) integers?

Example 2.5 (Example of a non-finitely-generated $\mathbb{Z}$-module). $\mathbb{Z}[\frac{1}{2}] = \{\frac{a}{2^r} : r \in \mathbb{Z}\}$ is not a finitely-generated $\mathbb{Z}$-module (but is a finitely-generated $\mathbb{Z}$-algebra).

Definition 2.6. Let $T \subset D$ be Noetherian domains. An element $d \in D$ is *integral over* T if and only if the ring $T[d]$ is a finitely-generated T-module. Equivalently, d is integral over T if and only if there is a monic polynomial $p(x) \in T[x]$ such that $p(d) = 0$.

Remark 2.2. If T is a PID, then it is enough that the monic minimal polynomial for d have coefficients in T. Thus, algebraic integers are the ones whose minimal polynomials have integer coefficients.

3. January 09

Definition 3.1. Let $T \subset D$ be domains with $\alpha \in D$. Then

(1) α is *integral over* T iff the ring $T[\alpha]$ is a finitely-generated T-module. If T is Noetherian (i.e., every ideal is finitely generated), then this is the same as requiring α to be the root of some monic polynomial $f(x) \in T[x]$.
(2) If T is a PID, then α is integral over T iff the monic minimal polynomial for α over the fraction field $K(T)$ of T has coefficients in T.
(3) We say that D is integral over T iff every element of D is integral over T.

Remark 3.1. Evidently, if α is integral over T, then α is also integral over larger rings containing T. The reverse is not true. $\frac{1}{2}$ is integral over $\mathbb{Q}$ but is not integral over $\mathbb{Z}$. Also, if α is integral over D and D is integral over T, then α is integral over T. This is useful because to check if α is integral over some terrible integral extension of $\mathbb{Z}$, it is the same as checking if α is integral over $\mathbb{Z}$.

Definition 3.2. Let T be a domain with K a ring containing T. Then *the integral closure of T in K* is the set of all elements of K that are integral over T. This set is actually a ring (a subring of K). We say T is *integrally closed* if and only if T is equal to the integral closure in $K(T)$.

Question. Find, *with proof*, the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{-7})$.

Solution: Let $a+b\sqrt{-7}$ be integral over $\mathbb{Z}$,where $a, b \in \mathbb{Q}$. Its minimal polynomial over $\mathbb{Q}$ is $x^2 - 2ax + a^2 + 7b^2 = 0$. It is also known that $2a$ and $a^2 + 7b^2$ are integers. Therefore, a is of the form $\frac{u}{2}$ where $u \in \mathbb{Z}$. Thus $\frac{u^2}{4} + 7b^2 \in \mathbb{Z}$. Thus b can only have 2 or 7 in denominator. But in fact it can only have 2 as a denominator. Otherwise, upon squared, only one 7 can be cancelled. Thus b must be of the form $\frac{v}{2}$ where $v \in \mathbb{Z}$. So $\frac{u^2+7b^2}{4} \in \mathbb{Z}$. This can happen only when u and v are either both odd or even. Thus every integral element is of the form $\frac{u+v\sqrt{-7}}{2}$. Hence the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{-7})$ is $\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$.

Definition 3.3. The integral closure of $\mathbb{Z}$ in a field K is called *the ring of integers of K* (if $[K : \mathbb{Q}]$ is finite), and is written $\mathcal{O}_K$.

4. January 12

Proposition 4.1. *The ring $\mathcal{O}_K$ is always isomorphic as an additive group to $\mathbb{Z}^d$, where $d = [K : \mathbb{Q}]$.*

Proof. Write $K = \mathbb{Q}(\alpha)$. We can multiply α by a sufficiently divisible integer $N \in \mathbb{Z}$ so that $K = \mathbb{Q}(N\alpha)$ and $N\alpha \in \mathcal{O}_K$. Then $\mathbb{Z}[N\alpha] \in \mathcal{O}_K$ and $\mathbb{Z}[N\alpha] \cong \mathbb{Z}[x]/(p(x))$ where $p(x)$ is an irreducible polynomial of degree d. But then $\mathbb{Z}[x]/(p(x)) \cong \mathbb{Z}^d$ as additive groups. Now $\mathcal{O}_K$ is a finitely-generated abelian torsion-free sub group with a subring isomorphic to $\mathbb{Z}^d$. So as an additive group, $\mathcal{O}_K \cong \mathbb{Z}^r$ for some $r \geq d$. So $\mathcal{O}_K$ is a subring of K which is a d-dimensional $\mathbb{Q}$-vector space. Thus $r = d$. □

Proposition 4.2. *Every non-zero ideal of $\mathcal{O}_K$ is also isomorphic to $\mathbb{Z}^d$. Therefore, if $I \subset \mathcal{O}_K$ is a non-zero ideal, then $\mathcal{O}_K/I$ a* finite ring.

Proof. Every ideal can be obtained by multiplying $\mathcal{O}_K$ by an element in $\mathcal{O}_K$, since $\mathcal{O}_K$ is a domain. Note that this is a monomorphism (i.e., injective homomorphism). The result follows. □

Example 4.3. $\mathbb{Z}[\sqrt{2}]/(3+\sqrt{2}) \cong \mathbb{Z}/7\mathbb{Z}$ because the homomorphism $\phi(a+b\sqrt{2}) := a - 3b \pmod 7$ is an isomorphism.

Question. Describe $\mathbb{Z}[\theta]/(\theta^2+4)$ where $\theta \in \mathbb{R}$ has minimal polynomial $x^3 + x + 1$.

Solution: $\mathbb{Z}[\theta]/(\theta^2+4) \cong \mathbb{Z}[x]/(x^2+4, x^3+x+1)$. In this quotient, $x^3 + x + 1 \equiv 0$ and $x^2 + 4 \equiv 0$. Thus $x^3 + 4x - x^3 - x - 1 = 3x - 1 \equiv 0$, and $x(3x-1) - (3x^2+12) = -x - 12 \equiv 0$, so $-3(-x-12) - (3x-1) = 37 \equiv 0$ (Euclidean algorithm!). So the quotient is $\mathbb{Z}/37\mathbb{Z}$ (our guess). Now time to prove that our guess is right! Consider the homomorphism $\mathbb{Z}[x] \to \mathbb{Z}/37\mathbb{Z}$ defined as $f(p(x)) = p(-12) \bmod 37$. By the first isomorphism theorem, it suffices to show that $\ker f = (x^3+x+1, x^2+4)$. Not a hard exercise to show that $(-12)^3 + (-12) + 1$ and $(-12)^2 + 4$ are divisible by 37. As for the reverse inclusion, notice that $(x+12, 37) \subset (x^3+x+1, x^2+4)$ according to our Euclidean algorithm. But $(x+12, 37)$ is a maximal ideal (since if you mod it out by $\mathbb{Z}$, you get $\mathbb{Z}/37\mathbb{Z}$), so (x^2+4, x^3+x+1) contains a maximal ideal. Since $\ker f \neq \mathbb{Z}[x]$, we get the reverse inclusion as desired.

5. January 14: Quadratic integers & Minkowski space of a number field

5.1. Quadratic integers.

Question. What are the algebraic integers of $\mathbb{Q}(\sqrt{d})$?

Note that we many assume that d is a square-free integer (we can pull out squares without changing the field itself). To start, choose any element $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ and assume it is an integer. Then see what conditions a and b should satisfy. The minimal monic polynomial for $a + b\sqrt{d}$ is $x^2 - 2ax + (a^2 - b^2 d)$. Now find when $a^2 - b^2 d$ and $2a \in \mathbb{Z}$. Write $a = u/2$ for some $u \in \mathbb{Z}$, so we have $\frac{u^2}{4} - b^2 d \in \mathbb{Z}$. Let $b := v/w$ for $v, w \in \mathbb{Z}$ and $\gcd(v, w) = 1$. Then

$$\frac{u^2}{4} - \frac{v^2 d}{w^2} = \frac{(uw)^2 - 4v^2 d}{4w^2} \in \mathbb{Z},$$

which implies $4 \mid u^2 w^2$ and $w^2 \mid 4d$. But since d is square-free, $w^2 \mid 4$, so $w \mid 2$. So $b = v/2$ for some v (if $w = 1$, multiply v by 2). Thus $a + b\sqrt{d}$ is of the form $\frac{u+v\sqrt{d}}{2}$ with $u, v \in \mathbb{Z}$. $a^2 - b^2 d \in \mathbb{Z}$, so $\frac{u^2 - dv^2}{4} \in \mathbb{Z}$. If u, v are even, then $\frac{u+v\sqrt{d}}{2}$ is an integer. If $u \not\equiv v \pmod 2$, then it is not an integer. But if u, v both odd, then we need $u^2 - dv^2 \equiv 0 \pmod 4$. But since $u^2, v^2 \equiv 0 \pmod 4$, it follows that $d \equiv 1 \pmod 4$. Hence, if $d \not\equiv 1 \pmod 4$, then every integer in $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}[d]$. But if $d \equiv 1 \pmod 4$, then every integer in $\mathbb{Q}(\sqrt{d})$ is of the form $\frac{u+v\sqrt{d}}{2}$ where $u \equiv v \pmod 2$. So there exists $k \in \mathbb{Z}$ such that

$$\frac{u + v\sqrt{d}}{2} = \frac{v + 2k + v\sqrt{d}}{2} = k + v\left(\frac{1 + \sqrt{d}}{2}\right).$$

Hence every algebraic integer in $\mathbb{Q}(\sqrt{d})$ lies in $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. The monic minimal polynomial for $\frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \pmod 4$ is $x^2 - x + \frac{1-d}{4} \in \mathbb{Z}[x]$, so $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ is integral over $\mathbb{Z}$, and is therefore the ring of integers of $\mathbb{Q}(\sqrt{d})$.

5.2. Introduction to Minkowski spaces of a number field.

Remark 5.1. $\mathbb{Z} \subset \mathbb{Q}$ and $\mathbb{Z}[i] \subset \mathbb{Q}[i]$ are nice lattices. But what about $\mathbb{Z}[\sqrt{2}] \subset \mathbb{Q}[\sqrt{2}]$? That one does not appear to be a nice lattice: for instance, $(-1 + \sqrt{2})^n \to 0$ as $n \to \infty$.

Let $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a number field of degree d. Then $\mathcal{O}_{\mathbb{Q}(\alpha)}$, the ring of integers, is isomorphic to $\mathbb{Z}^d$ as an additive group. We want a nice way to view $\mathbb{Q}(\alpha)$ as a d-dimensional $\mathbb{Q}$-vector space so that $\mathcal{O}_{\mathbb{Q}(\alpha)}$ appears as a nice rank d lattice. This is where the Minkowski space comes into play.

6. January 16 & 19: Minkowski space of a number field

Say $\mathbb{Q}(\alpha)/\mathbb{Q}$ has degree d. We want to find a d-dimensional real vector space that contains $\mathcal{O}_{\mathbb{Q}(\alpha)}$ as a full lattice.

Definition 6.1. Let A be a finitely generated abelian group (or finitely generated $\mathbb{Z}$-module). Then $A \cong \mathbb{Z}^r \times T$ for some non-negative integer r and a finite group T. The integer r is called the *rank of* A.

Question. What are the homomorphisms from $\mathbb{Q}(\alpha)$ to $\mathbb{C}$?

Solution: The homomorphisms are completely determined by the destination of α. $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/((p(x))$, where $p(x)$ is the minimal polynomial for α over $\mathbb{Q}$. Every homomorphism from $\mathbb{Q}(\alpha) \to \mathbb{C}$ is a homomorphism from $\mathbb{Q}[x] \to \mathbb{C}$ such that $p(x) \mapsto 0$. A homomorphism $\mathbb{Q}[x] \to \mathbb{C}$ is determined by the destination of x. By the universal property of quotients (UPQ) we must make sure that x gets mapped to a root of $p(x)$. There are exactly d of those, one for each root of $p(x)$. Thus there are d homomorphisms.

Question. Find the number of homomorphisms from $\mathbb{Q}(\alpha)$ to $\mathbb{R}$ and $\mathbb{C}$, where α is a root of:

(a) $x^5 + 3x + 3$
(b) $x^4 - 5x + 3$

Solution: Just find the number of roots for each polynomial. Calculus comes in handy!

Say $\mathbb{Q}(\alpha)$ has r real embeddings and s complex conjugate embeddings. Then $r + 2s = d$, where d is the degree of a given polynomial.

Definition 6.2. We define the *Minkowski map* $\phi : \mathbb{Q}(\alpha) \to \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^d$ such that $\phi(a) = (f_1(a), \ldots, f_r(a), g_1(a), \ldots, g_s(a))$, where f_i's are the real embeddings and g_j's are the representatives of each complex conjugate pair of complex embeddings.

Example 6.3. Consider $K = \mathbb{Q}(\sqrt{2})$. Then $(r, s) = (2, 0)$. We have $f_1(a + b\sqrt{2}) = a + b\sqrt{2}$ and $f_2(a + b\sqrt{2}) = a - b\sqrt{2}$. Thus $\phi(a + b\sqrt{2}) = (a + b\sqrt{2}, a - b\sqrt{2})$.

Does $\phi(\mathbb{Q}(\alpha))$ span the Minkowski space as a real vector space? Indeed it does. The set $\{\phi(1), \phi(\alpha), \ldots, \phi(\alpha^d)\}$ spans $\mathbb{R}^d$ over $\mathbb{R}$. Since the set has d element, it's enough to show that it is linearly independent over $\mathbb{R}$. Write $\phi(\alpha^r) = (\alpha_1^r, \ldots, \alpha_d^r)$, where $\alpha_1, \ldots, \alpha_d$ are conjugates of α. These vectors are linearly independent (and spanning) if and only if

$$\det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_d \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{d-1} & \alpha_2^{d-1} & \cdots & \alpha_d^{d-1} \end{pmatrix} \neq 0.$$

We see that indeed this is the case. Note that the above matrix is a *Vandermonde determinant*, which vanishes if and only if $\alpha_i = \alpha_j$ for some $i \neq j$. Since the conjugates of α are all different, indeed the determinant does not vanish. Win!

So $\phi(\mathcal{O}_{\mathbb{Q}(\alpha)})$ spans Minkowski space as well, meaning that $\phi(\mathcal{O}_{\mathbb{Q}(\alpha)})$ is the set of $\mathbb{Z}$-linear combinations of a basis of $\mathbb{R}^d$, which is precisely the kind of nice lattice we were looking for.

Question. Write Minkowski map for $K = \mathbb{Q}(\sqrt[3]{2})$. Also compute $\phi(\sqrt[3]{2})$ and $\phi(\sqrt[3]{4})$.

Solution: First question, how many embeddings? Note that $\mathbb{Q}(\sqrt[3]{2})$ has one real embedding and one pairwise complex embedding, so $\phi : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{R} \times \mathbb{C}$ given by $\phi(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = (a + b\sqrt[3]{2} + c\sqrt[3]{4}, a + b\omega\sqrt[3]{2} + c\omega^2\sqrt[3]{4})$, where ω is a cubic root of unity. For the complex embedding, you can just choose one of the two complex conjugates.

Note that the image of ϕ is *not* in $\mathbb{Q}(\sqrt[3]{2})$. This is no surprise, since $K/\mathbb{Q}$ is *not* a Galois extension.

7. January 21

Definition 7.1. Let $\alpha \in \overline{\mathbb{Q}}$ be an algebraic number. The *Galois conjugates* of α over $\mathbb{Q}$ are the roots (in $\overline{\mathbb{Q}}$) of the monic minimal polynomial for α over $\mathbb{Q}$. These are also images of α under homomorphisms $\mathbb{Q}(\alpha) \to \mathbb{C}$.

If $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$, then α has d Galois conjugates including α itself. If α' is a Galois conjugate of α with $\alpha' \in \mathbb{Q}(\alpha)$, then there is an isomorphism $\phi : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$ such that $\phi(\alpha) = \alpha'$. If $\alpha' \in \mathbb{Q}(\alpha)$, then there is an isomorphism $\phi : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha')$ with $\phi(\alpha) = \alpha'$.

Notice that if $K \to \mathbb{R}^r \to \mathbb{C}^s$ is the Minkowski map, then $\phi(\mathbb{Q})$ lies on the grand diagonal $x_1 = x_2 = \cdots = x_r = z_1 = \cdots = z_s$. In general, if $F \subset K$ is a subfield, then the image of F will lie in some subspace of defined by equating some of the coordinates.

Example 7.2. $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then the Minkowski space is $\mathbb{R}^4$, with $\phi(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = (a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}, a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}, a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}, a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6})$. Notice that:

$$\begin{aligned}\phi(\mathbb{Q}) &= \phi(K) \cap \{x_1 = x_2 = x_3 = x_4\} \\ \phi(\mathbb{Q}(\sqrt{2})) &= \phi(K) \cap \{x_1 = x_3, x_2 = x_4\} \\ \phi(\mathbb{Q}(\sqrt{3})) &= \phi(K) \cap \{x_1 = x_2, x_3 = x_4\}.\end{aligned}$$

and so forth.

Definition 7.3. Let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be elements of a number field K of degree n over $\mathbb{Q}$. The *discriminant of* $\{\alpha_1, \ldots, \alpha_n\}$ is:

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \left(\det \begin{bmatrix} \phi_1(\alpha_1) & \cdots & \phi_n(\alpha_1) \\ \vdots & & \vdots \\ \phi_1(\alpha_n) & \cdots & \phi_n(\alpha_n) \end{bmatrix} \right)^2$$

where $\phi_i : K \to \mathbb{C}$ are the K-embeddings.

Example 7.4. $\{1 + \sqrt{2}, \sqrt{2}\} \subset \mathbb{Q}(\sqrt{2})$. Then

$$\operatorname{disc}(1 + \sqrt{2}, \sqrt{2}) = \left(\det \begin{bmatrix} 1 + \sqrt{2} & 1 - \sqrt{2} \\ \sqrt{2} & -\sqrt{2} \end{bmatrix} \right)^2 = 8.$$

Definition 7.5. The *discriminant* $\operatorname{disc}_K(\alpha)$ *of* $\alpha \in \overline{\mathbb{Q}}$ over $\mathbb{Q}$ is $\operatorname{disc}(1, \alpha, \ldots, \alpha^{d-1})$ where $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$.

Notice that if $K \neq \mathbb{Q}(\alpha)$, then $\operatorname{disc}_K(\alpha) = 0$.

8. January 23

Theorem 8.1. *If* $A \in \mathrm{M}_n(\mathbb{Q})$ *with* $a_i \in K$*, then*

$$A \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$$

so $(\det A)^2 \operatorname{disc}(a_1, \ldots, a_n) = \operatorname{disc}(b_1, \ldots, b_n)$.

Proof. Since A is rational,

$$A \begin{bmatrix} \phi_l(a_1) \\ \vdots \\ \phi_l(a_n) \end{bmatrix} = \begin{bmatrix} \phi_l(b_1) \\ \vdots \\ \phi_l(b_n) \end{bmatrix}.$$

So let $C_k := \begin{bmatrix} \phi_k(a_1) \\ \vdots \\ \phi_k(a_n) \end{bmatrix}$. Then

$$\begin{aligned} \operatorname{disc}(b_1, \ldots, b_n) &= \left(\det \begin{bmatrix} \phi_1(\alpha_1) & \cdots & \phi_n(\alpha_1) \\ \vdots & & \vdots \\ \phi_1(\alpha_n) & \cdots & \phi_n(\alpha_n) \end{bmatrix} \right)^2 \\ &= \left(\det \left[\begin{array}{c|c|c|c} AC_1 & AC_2 & \cdots & AC_n \end{array} \right] \right)^2 \\ &= \left(\det A \left[\begin{array}{c|c|c|c} C_1 & C_2 & \cdots & C_n \end{array} \right] \right)^2 \\ &= (\det A)^2 \operatorname{disc}(a_1, \ldots, a_n). \end{aligned}$$

□

Definition 8.2. Let $\mathcal{O} \subseteq K$ be a subring isomorphic to $\mathbb{Z}^n$. Then $\operatorname{disc}(\theta) = \operatorname{disc}(a_1, \ldots, a_n)$ where $\mathcal{O} = \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_n$, i.e. $\{a_1, \ldots, a_n\}$ is an integral basis of $\mathcal{O}$.

Corollary 8.3. *If $\{b_1, \ldots, b_n\}$ is another integral basis of θ, then the change of basis matrix is invertible, and has determinant ± 1.*

Definition 8.4. $\operatorname{disc}(K) = \operatorname{disc}(\text{ring of integers of } K)$.

Question. Compute the discriminant of $\mathbb{Z}[ai]$ and $\mathbb{Z}[a\sqrt{3}, b\sqrt{5}]$.

Solution: For the first one, note that there are two embeddings: $\phi_1 = \mathrm{id}$ and $\phi_2 : 1 \mapsto 1, i \mapsto -i$. So

$$\left(\det \begin{bmatrix} 1 & 1 \\ ai & -ai \end{bmatrix} \right)^2 = -4a^2.$$

As for $\mathbb{Z}[a\sqrt{3}, b\sqrt{5}]$, we have

$$\left(\det \begin{bmatrix} 1 & 1 & 1 & 1 \\ a\sqrt{3} & -a\sqrt{3} & a\sqrt{3} & -a\sqrt{3} \\ b\sqrt{5} & b\sqrt{5} & -b\sqrt{5} & -b\sqrt{5} \\ ab\sqrt{15} & -ab\sqrt{15} & -ab\sqrt{15} & ab\sqrt{15} \end{bmatrix} \right)^2 = 14400a^4b^4.$$

Definition 8.5. Let $p(x) = a \prod_{i=1}^{n} (x - \alpha_i) \in \mathbb{Q}[x]$. Then

$$\operatorname{disc}(p) := \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

S_n acts on $\{\alpha_1, \ldots, \alpha_n\}$ and $\operatorname{disc}(p)$ is invariant under this action.

Each homomorphism ϕ_k "lives in" S_n, i.e., each embedding switches one root to another (i.e., permutation). Therefore $\text{disc}(p) = \phi_k(\text{disc}(p))$. All you are doing is flipping the roots around!

9. January 26

Recall that if $p(x) \in \mathbb{C}[x]$ is no-constant then $\text{disc}(p(x)) = a^{2n-2}\prod_{i<j}(r_i - r_j)^2$, where $n = \deg(p)$ and $p(x) = a\prod_{i=1}^{n}(x - r_i)$. In particular, $\text{disc}(p(x)) = 0 \Leftrightarrow p(x)$ has some repeated root. It's not too hard to see that if $p(x)$ is a minimal polynomial for $\alpha \in \overline{\mathbb{Q}}$ over $\mathbb{Q}$, then $\text{disc}(\alpha)$ equals $\text{disc}(p(x))$.

There is a shortcut for computing $\text{disc}(p(x))$ without needing to know its roots. It comes from the theory of resultants:

$$\text{disc}(p(x)) = (-1)^{\frac{n(n-1)}{2}}\frac{1}{a_n}\text{Res}(p(x), p'(x)),$$

where $p(x) = a_n x^n + \cdots + a_0$ and $\text{Res}(f, g)$ is the following determinant:

$$\det\begin{bmatrix} b_r & b_{r-1} & \cdots & b_0 & 0 & 0 & \cdots & 0 \\ 0 & b_r & b_{r-1} & \cdots & b_0 & 0 & \cdots & 0 \\ & & \ddots & \ddots & \ddots & & & \\ 0 & 0 & \cdots & 0 & b_r & b_{r-1} & \cdots & b_0 \\ c_s & c_{s-1} & \cdots & c_0 & 0 & 0 & \cdots & 0 \\ 0 & c_s & c_{s-1} & \cdots & c_0 & 0 & \cdots & 0 \\ & & \ddots & \ddots & \ddots & & & \\ 0 & 0 & \cdots & 0 & c_s & c_{s-1} & \cdots & c_0 \end{bmatrix},$$

where $f = b_r x^2 r + \cdots + b_0, g = c_s x^s + \cdots + c_0$, and matrix has $r + s$ rows and $r + s$ columns.

Example 9.1. The discriminant of $x^3 + 7x + 3$ is

$$(-1)^{\frac{3(3-1)}{2}}\frac{1}{1}\det\begin{bmatrix} 1 & 0 & 7 & 3 & 0 \\ 0 & 1 & 0 & 7 & 3 \\ 3 & 0 & 7 & 0 & 0 \\ 0 & 3 & 0 & 7 & 0 \\ 0 & 0 & 3 & 0 & 7 \end{bmatrix} = -1615.$$

So if α is a root of $x^3 + 7x + 3$, then the discriminant of α (or of $\mathbb{Z}[\alpha]$) is -1615.

Question. Compute $\text{disc}(ax^2 + bx + c)$ and $\text{disc}(x^3 + ax + b)$.

Solution: $\operatorname{disc}(ax^2+bx+c) = (-1)^{2(2-1)/2}a^{-1}\det\begin{bmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{bmatrix} = b^2-4ac$. On the other hand,

$$\operatorname{disc}(x^3+ax+b) = (-1)^{3(3-1)/2}\frac{1}{1}\det\begin{bmatrix} 1 & 0 & a & b & 0 \\ 0 & 1 & 0 & a & b \\ 3 & 0 & a & 0 & 0 \\ 0 & 3 & 0 & a & 0 \\ 0 & 0 & 3 & 0 & a \end{bmatrix} = -4a^3-27b^2.$$

Let $\mathcal{O}$ be the ring of integers in $\mathbb{Q}(\alpha)$. Then there is a matrix $A \in \mathrm{M}_3(\mathbb{Z})$ such that $A\begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} 1 \\ \alpha \\ \alpha^2 \end{bmatrix}$, where $\mathcal{O} = a\mathbb{Z}+b\mathbb{Z}+c\mathbb{Z}$. This means that $\operatorname{disc}(\mathcal{O})\det A^2 = \operatorname{disc}(\alpha)$, so $(\det A)^2$ is a divisor of $\operatorname{disc}(\alpha) = -1615 = -5\cdot 17\cdot 19$, which is square-free. Therefore $(\det A)^2 = 1$, and by Cramer's rule that $A^{-1} \in \mathrm{M}_3(\mathbb{Z})$ so $\mathcal{O} \subset \mathbb{Z}+\alpha\mathbb{Z}+\alpha^2\mathbb{Z} = \mathbb{Z}[\alpha]$. Thus $\mathcal{O} = \mathbb{Z}[\alpha]$.

If T is a ring integral over $\mathbb{Z}$ with square-free discriminant, then T is the ring of integers of its field of fractions. However, the converse is *not* true. Note that $\operatorname{disc}\mathbb{Z}[i] = 4$.

10. January 28

Let I be an ideal of $\mathcal{O}_K$, the ring of integers of a number field K. Recall that $I \cong \mathbb{Z}^d$ as an additive group, where $d = [K:\mathbb{Q}]$. A basis for I is a basis for I as a $\mathbb{Z}$-module.

Theorem 10.1. *The discriminant of I does* not *depend on the choice of basis. That is, the discriminant of I is the discriminant of a basis of I.*

Example 10.2. $(2+i) \subset \mathbb{Z}[i]$ has basis $\{2+i, -1+2i\}$. The discriminant is -100.

$\mathcal{O}_K$ has dimension one, meaning that every non-zero prime ideal is maximal. In particular, $\mathcal{O}_K/I$ is always finite unless $I = 0$. These facts also apply to any subring of $\mathcal{O}_K$.

The discriminant of K is, by definition, the discriminant of $\mathcal{O}_K$, which is by definition, the discriminant of $(1) \in \mathcal{O}_K$; and this is, by definition, the discriminant of an integral basis of $\mathcal{O}_K$ over $\mathbb{Z}$ – which is, by definition (third time!), a basis for $\mathcal{O}_K$ as a $\mathbb{Z}$-module.

Definition 10.3. The norm of a nonzero ideal $I \subseteq \mathcal{O}_K$ is $\sqrt{\frac{\operatorname{disc}(I)}{\operatorname{disc}(K)}}$. It is written in $N(I)$.

The norm of I is always an integer because $\operatorname{disc}(I) = \det(A)^2\operatorname{disc}(K)$ where A is a matrix with integer entries that expresses a $\mathbb{Z}$-basis in terms of an integral basis of $\mathcal{O}_K$.

Theorem 10.4. *$N(I) = \#(\mathcal{O}_K/I)$, where I is a non-zero ideal.*

Proof. As additive groups, there is an exact sequence:

$$0 \to I \xrightarrow{i} \mathcal{O}_K \xrightarrow{q} \mathcal{O}_K/I \to 0,$$

where i and q are inclusion and quotient maps, respectively. This is just

$$0 \to \mathbb{Z}^d \xrightarrow{A} \mathbb{Z}^d \to T \to 0,$$

where $d = [K:\mathbb{Q}]$, T a finite abelian group. We have chosen a $\mathbb{Z}$-basis of $I, \mathcal{O}_K$.

So A is the $\mathbb{Z}$-linear map that expresses the $\mathbb{Z}$-basis in terms of the $\mathbb{Z}$-basis of $\mathcal{O}_K$. The determinant of this A is exactly $N(I)$, in absolute value.

This means that $\#T = \#(\mathcal{O}_K/I) = |\det A| = N(I)$. □

11. January 30

Theorem 11.1 (Stickelberger's theorem)**.** $\operatorname{disc}(K)$ *is either congruent to* 0 *or* 1 *mod* 4.

Theorem 11.2 (Brill's theorem)**.** $\operatorname{disc}(K)$ *is:*

- *negative if the number of complex conjugate pairs of complex embeddings of* K
- *positive if the number of complex conjugate pairs of complex embeddings of* K*.*

Proof. Suppose that $\omega_1, \dots \omega_d$ are integral basis of $\mathcal{O}_K$ over $\mathbb{Z}$. Then

$$\det \begin{bmatrix} \phi_1(\omega_1) & \cdots & \phi_d(\omega_1) \\ \vdots & & \vdots \\ \phi_1(\omega_d) & \cdots & \phi_d(\omega_d) \end{bmatrix} = A + Bi$$

for some appropriate A and B. Note that $A - Bi$ is the same determinant but with s column switches. Therefore $A + Bi = (-1)^s(A - Bi)$. So if s is event then $B = 0$. Hence the discriminant is positive. If s is odd, then $A = 0$, implying that the discriminant is negative. □

Theorem 11.3. *Let* $v \in \mathbb{Z}^d$ *be a* primitive vector *(the GCD of the coordinates is* 1*). Then there is a basis of* $\mathbb{Z}^d$ *that contains* v*.*

Proof. Time to summon a short exact sequence:

$$0 \to \mathbb{Z}v \to \mathbb{Z}^d \to Q \to 0,$$

where $Q := \mathbb{Z}^d/\mathbb{Z}v$. The rank of Q is $d - 1$. We will show that $Q \cong \mathbb{Z}^{d-1}$ by showing that Q is torsion-free. If $w \in Q$ is torsion, then it is the image of $x \in \mathbb{Z}^d$ such that $nx \in \mathbb{Z}v$ for some $n \in \mathbb{Z} \setminus \{0\}$. Then $x = \lambda v$ for some $\lambda \in \mathbb{Q}$. But since v is primitive, the denominator of λ has to be cancelled by the each of the coordinates of v – thus λ must be 1. $x \in \mathbb{Z}v$ so indeed Q is torsion-free.

Now let $\{w_1, \dots, w_{d-1}\}$ be a basis for Q, and let $\{v_1, \dots, v_{d-1}\}$ be the elements of $\mathbb{Z}^d$ such that $v_i \cong w_i \pmod{\mathbb{Z}v}$. Then $\{v, v_1, \dots, v_{d-1}\}$ is a basis of $\mathbb{Z}^d$. □

Question. Let $K = \mathbb{Q}(\alpha)$, where α is a root of $x^3 + 3x^2 - 2x - 2$, which you can assume to be irreducible. Find $\mathcal{O}_K$. *Hint:* Note that $\operatorname{disc}(x^3 + 3x^2 - 2x - 2)$ is -104.

Solution: Note that the only squares that divide -104 are 1 and 4. But $\operatorname{disc}(K)$ must be -104; otherwise it will contradict Stickelberger's theorem. Therefore $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

12. February 2

Definition 12.1. D is said to be a *Dedekind domain* if it is:

- Noetherian
- Integrally closed (contains all the integral elements)
- One-dimensional (every non-zero prime ideal is maximal)

Example 12.2. For any number field K, the ring of integers $\mathcal{O}_K$ is a Dedekind domain.

Our goal today is to show that any non-zero ideal of a Dedekind domain can be written *uniquely* (up to permutation) as a product of prime ideals.

Definition 12.3. The *product IJ of ideals I and J* is the ideal generated by all products of form xy, where $x \in I, y \in J$. In particular, $(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_m) = (a_i b_j)$ where $1 \leq i \leq n, 1 \leq j \leq m$.

Definition 12.4. Let I, J be non-zero ideals of a domain D. Then we define

$$I \div J := \{\alpha \in \mathrm{Frac}(D) : \alpha J \subset I\}.$$

Remark 12.1. Note that $I \div J$ is *not necessarily* an ideal of D. But it is a D-module.

Definition 12.5. A *fractional ideal* of D is a D-submodule I of $\mathrm{Frac}(D)$ such that there is some $\gamma \in \mathrm{Frac}(D) \setminus \{0\}$ with $\gamma I \subset D$.

Example 12.6. $\frac{1}{2}\mathbb{Z}$ is a fractional ideal of $\mathbb{Z}$.

Example 12.7. For any $\alpha_1, \ldots, \alpha_n \in \mathrm{Frac}(D)$, $I = \alpha_1 D + \cdots + \alpha_n D$ is a fractional ideal of D.

Example 12.8. Any ideal of D is a fractional ideal of D. In fact, a fractional ideal of D is an ideal of D if and only if it's contained in D.

Question. Find generators of $\mathbb{Z}[\sqrt{-10}] \div (2, \sqrt{-10})$ either as a $\mathbb{Z}$-module or a $\mathbb{Z}[\sqrt{-10}]$-module.

Solution. $\mathbb{Z}[\sqrt{-10}] \div (2, \sqrt{-10}) = \{\frac{a}{b} + \frac{c}{d}\sqrt{-10} : 2\frac{a}{b} + 2\frac{c}{d}\sqrt{-10}, \sqrt{-10}\left(\frac{a}{b} + \frac{c}{d}\sqrt{-10}\right) \in \mathbb{Z}[\sqrt{-10}]\}$. In the first case, we need $b, d = 2$. For the second case, we have $b = 1$. Therefore $\frac{a}{b} + \frac{c}{d}\sqrt{-10} = a + c\left(\frac{\sqrt{-10}}{2}\right)$. □

Now let's take a non-zero ideal $I \subset D$ and try to factor into primes. Let P be a prime containing I. Can we write $I = P(I \div P)$? The answer is definitely yes if P is an invertible ideal.

Definition 12.9. A fractional ideal I of D is said to be *invertible* if and only if there is some fractional ideal J of D such that $IJ = D$.

We will see that every nonzero fractional ideal of a Dedekind domain is invertible, and the converse holds.

13. February 4

If I is invertible, then denote I^{-1} to be its inverse ideal. Clearly, if I is an ideal, then I^{-1} is not an ideal but a fractional ideal. If P is invertible, then $I \div P = IP^{-1}$.

If every non-zero ideal of D is invertible, then it is straightforward to deduce that every non-zero ideal is a product of prime ideals in a unique way (up to permutation). But how can we tell if an ideal is invertible?

Definition 13.1. Let R be a domain, and $P \subset R$ a prime ideal. Then *local ring* of R at P is $R_P = \{\frac{a}{b} \in K(R) : b \in R \setminus P\}$. So R_P is the ring of all the elements of $K(R)$ that are well-defined mod P.

Remark 13.1. So how did the name "local ring" come from? Consider the following ring: if $R = \mathbb{C}[x]$ and $p = (x - a)$ for $a \in \mathbb{C}$ then

$$R_P = \{p(x)/q(x) : q(a) \neq 0\}.$$

Remark 13.2. Take $R = \mathbb{Z}$ and $P = (2)$ for instance. Then $\mathbb{Z}_{(2)} = \{\frac{a}{b} : b \equiv 1 \pmod 2\}$. So if a, b odd then a/b is a unit of $\mathbb{Z}_{(2)}$. If $a = 2k$ even, then $\frac{a}{b} = 2\frac{k}{b} \in (2)$. So if $\frac{a}{b} = \frac{2^r \cdot k}{b}$ for k, b odd then $(\frac{a}{b}) = (2^r)$. Therefore, the ideals of $\mathbb{Z}_{(2)}$ are (0) and $\{(2^r) : r \in \mathbb{Z}_{\geq 0}\}$.

Notice that the non-units of R_P form an ideal, namely $PR_P = \{\frac{a}{b}, a \in P, b \notin P\}$. Thus this ideal is the *only* maximal ideal of R_P. Also, R_P is Noetherian and one-dimensional (i.e., every non-zero prime ideal of R_P is maximal). This is a non-obvious fact, but one can show (with not a lot of difficulty) the following: if R is integrally closed, then so is R_P.

So what does this have to do with the invertibility of ideals? The following theorem gives the connection:

Theorem 13.2. *Let I be a nonzero ideal of a domain D. Then I is invertible if and only if I is a finitely-generated D-module and ID_P is* singly *generated (i.e., generated by* one and only one *element) as an D_P-module for all prime ideals $P \subset D$.*

Proofs of these and many other theorems about Dedekind domains and local rings can be found in *Commutative Ring Theory* by Matsumura.

14. February 6

Proposition 14.1. *If P is invertible, then PD_P is a principal ideal, and PD_P is the unique maximal ideal of D_P. Then there exists t such that $PD_P = (t)$.*

Definition 14.2. The t such that $PD_P = (t)$ is called a *uniformizer for D_P.*

If $\alpha \in D_P$ is any element not in (t), then α is a unit of D_P. If $\alpha \in D_P$ is not a unit, then $\alpha = \alpha_1 t$ for some $\alpha_1 \in D_P$. If α_1 is not a unit, then $\alpha_1 = \alpha_2 t$, so $\alpha_2 t^2 = \alpha$ for some $\alpha_2 \in D_P$. Since D_P is Noetherian, this process must eventually stop, since $(\alpha) \subset (\alpha_1) \subset (\alpha_2) \subset \cdots$ is a chain of ideals, which must terminate eventually. Therefore α_i is a unit for some i, hence $\alpha = \alpha_i t^i$ for some unit $\alpha_i \in D_P$. Therefore, we proved the following proposition:

Proposition 14.3. *If P is an invertible prime ideal of a Noetherian domain D, then every non-zero element of D_P can be written* uniquely *as ut^r for $u \in D_P^*$, for t a uniformizer and $r \in \mathbb{Z}_{\geq 0}$.*

Definition 14.4. A *discrete valuation ring (DVR)* is a Noetherian local ring whose maximal ideal is principal.

Every DVR is integrally closed, and if K is the fraction field of a DVR D, then every non-zero element of K can be written uniquely in the form ut^r for $u \in D_P^*, r \in \mathbb{Z}$ and t a uniformizer.

Question. Find a uniformizer for D_P where $D = \mathbb{Z}[\sqrt{-10}]$ and $P = (2, \sqrt{-10})$. Write 6 as a unit times a power of the uniformizer. You may assume that D_P is a DVR.

Solution: Let t be a uniformizer, and write $2 = u_1 t^a$ and $\sqrt{-10} = u_2 t^b$. Since $t \in (2, \sqrt{-10})$, we get either $a = 1$ or $b = 1$. So one of 2 and $\sqrt{-10}$ must be a uniformizer. Thus, at least one

of $\frac{2}{\sqrt{10}}$ and $\frac{\sqrt{-10}}{2}$ must lie in D_P. We say the former lies in D_P, since $\frac{2}{\sqrt{-10}} = \frac{2\sqrt{-10}}{-10} = -\frac{\sqrt{-10}}{5}$. So $2 = \left(\frac{2}{\sqrt{-10}}\right)\sqrt{-10} \in \sqrt{-10}D_P$. Thus $\sqrt{-10}$ is a uniformizer. So P is not a principal ideal as an ideal of D. But P is a principal ideal as an ideal of D_P.

For the second part, note $6 = (\sqrt{-10})^2\left(-\frac{3}{5}\right)$, and $-\frac{3}{5}$ is indeed a unit of D_P.

15. February 9

Theorem 15.1. *The following are equivalent, where D is a domain and P a prime ideal of D:*

(1) D_P is a discrete valuation ring.
(2) D_P is a local PID that is not a field.
(3) D_P has a unique principal maximal ideal and is Noetherian.
(4) D_P is Noetherian, local, one-dimensional, and integrally closed.

Remark 15.1. Let's track back what we have been doing. First, we started with a Dedekind domain D (one-dimensional, Noetherian, integrally closed). Then, for all non-zero primes P, we constructed a DVR D_P (localization). We proved that every non-zero ideal of is invertible. From this, we can deduce that every non-zero ideal can be uniquely factored as a product of prime ideals. In fact, one can "complete the loop" by showing that the unique factorization of ideals implies that D is a Dedekind domain (but this is the hardest direction).

Proposition 15.2. *Suppose D is a Dedekind domain. Then*

$$D = \bigcap_{P \text{ prime}} D_P.$$

Proof. Clearly $D \subset \bigcap D_P$. Now let $a \in \bigcap D_P$. We want to show that $a \in D$. Since D is Dedekind we have $(a) = P_1^{a_1} \cdots P_r^{a_r}$ for $a_i \in \mathbb{Z}$ and prime ideals P_i of D. It suffices to show that $a_i \geq 0$ for all i. But $a \in D_{P_i}$ for all i, so $a = x/y$ where $x, y \in D$ and $y \notin P_i$. Thus $a_i \geq 0$ and $a \in D$. □

Question. Let $D = \mathbb{Z}[2\sqrt{2}]$, and $P = (2, 2\sqrt{2})$. Prove that D_P is *not* a DVR. (*Hint:* Show that PD_P is not a principal ideal domain.)

Solution: We want to show that PD_P is not a principal ideal domain. Suppose it is, i.e., there exists $t \in D_P$ such that $PD_P = (t)$. Note that the candidates for the uniformizer of PD_P are 2 and $2\sqrt{2}$. It suffices to show that neither can be a generator (or a uniformizer if that sounds more pleasant), i.e., show that $PD_P \neq 2D_P$ and $PD_P \neq (2\sqrt{2})D_P$. It further suffices to show that $\frac{2}{2\sqrt{2}}$ and $\frac{2\sqrt{2}}{2}$ are not in D_P – if it were the case, then whatever is in the denominator would be the generator.

To do this, notice that T_Q is a DVR containing D_P, where $T = \mathbb{Z}[\sqrt{2}], Q = (\sqrt{2})$. Furthermore, QT_Q contains PD_P. Obviously, the uniformizer of QT_Q is $\sqrt{2}$, and $2 = 1 \cdot (\sqrt{2})^2, 2\sqrt{2} = 1 \cdot (\sqrt{2})^3$. So $P = 2\mathbb{Z} + 2\sqrt{2}\mathbb{Z}$, so every element of PD_P is divisible in T_Q by $(\sqrt{2})^2$. But $\frac{2}{2\sqrt{2}} = (\sqrt{2})^{-1} \notin D_P$ Similarly, $2\sqrt{2}/2 = \sqrt{2} \notin D_P$, since $\sqrt{2}$ is not divisible by $(\sqrt{2})^2$. Therefore D_P cannot be a DVR.

Remark 15.2. The set of fractional ideals of a Dedekind domain D is a group under multiplication. The group is $\bigoplus_{i \in \mathbb{N}} \mathbb{Z}$ if D is $\mathcal{O}_K$.

16. February 11

Theorem 16.1 (Chinese remainder theorem (CRT))**.** *Let I be a nonzero ideal of a Dedekind domain D, and write $I = P_1^{a_1} \cdots P_r^{a_r}$ as a product of prime ideals. Then*

$$D/I \cong (D/P_1^{a_1}) \times \cdots \times (D/P_r^{a_r}).$$

Proof. Define $\Phi : D \to (D/P_1^{a_1}) \times \cdots \times (D/P_r^{a_r})$ by

$$\Phi(d) = (d \bmod P_1^{a_1}, \cdots, d \bmod P_r^{a_r}).$$

Certainly $I \subset \ker \Phi$, and $\ker \Phi \subset I$ because if $d \in \ker \Phi$, then $d \in P_i^{a_i}$ for all i. So $d \in \bigcap P_i^{a_i}$, and $\bigcap P_i^{a_i} = \prod P_i^{a_i} = I$. So the first isomorphism theorem (or the universal property of quotients) implies that Φ is a well-defined injective mapping from D/I to $(D/P_1^{a_1}) \times \cdots \times (D/P_r^{a_r})$.

To see that Φ is onto, it is enough to show that $e_i = (0, 0, \cdots, 1 \bmod P_i^{a_i}, 0, \cdots, 0) \in \operatorname{im} \Phi$ for all i. Since $P_i^{a_i}$ and $\prod_{j \neq i} P_j^{a_j}$ are coprime, we have $P_i^{a_i} + \prod_{j \neq i} P_j^{a_j} = D$ so there exist $x \in P_i^{a_i}$ and $y \in \prod_{j \neq i} P_j^{a_j}$ such that $x + y = 1$. Then $\Phi(y_i) = e_i$ so Φ in surjective. □

This means that $N(IJ) = N(I)N(J)$ – almost. Say $D = \mathcal{O}_K$ for a number field K. If I and J are relatively prime, then $D/IJ \cong D/I \times D/J$ so we are done.

More generally, write $I = \prod P_i^{a_i}$ and $J = \prod P_i^{b_i}$, where a_i and b_i are non-negative integers. Then $D/I \cong \prod (D/P_i^{a_i}), D/J \cong \prod (D/P_i^{b_i}), D/IJ \cong D/P_i^{a_i+b_i}$. To show that $N(IJ) = N(I)N(J)$, it suffices to show that $\#(D/P^{a+b}) = \#(D/P^a)\#(D/P^b)$. First, we will show that $D/P \cong D_P/PD_P$. Write $\Psi : D \to D_P/PD_P$ by $\Psi(d) = d \bmod PD_P$. Since $P \subset \ker \Psi$, Ψ induces $\Psi : D/P \to D_P/PD_P$. Since $D \cap PD_P = P$, $\ker \Psi = P$, so $D/P \hookrightarrow D_P/PD_P$. Thus we only need to show that Ψ is surjective. Let $a \in D_P$. We will show that there is a $d \in D$ such that $a - d \in PD_P$. So $\Psi(d) = a \bmod PD_P$. Write $a = \frac{\alpha}{\beta}$, where $\alpha, \beta \in D$ and $\beta \notin P$. If $\alpha \in P$, then we are done since $d = 0$ will do the job. If not, write $(\alpha) = \prod P_i^{a_i}$ where $P \neq P_i$ for all i. Define $\Phi : D_P \to D/P$ by $\Phi(a/b) = a/b \bmod P$. This is well-defined because $b \in P$ and D/P is a field. Clearly $PD_P \in \ker \Phi$ so Φ induces a map $\Phi : D_P/PD_P \to D/P$ that is inverse of Ψ. So Φ and Ψ are isomorphisms. Thus $D/P \cong D_P/PD_P$.

17. February 13

Notice that D/P^a is a (D/P)-module. We will show that $\#(D/P^a) = (\#(D/P))^a$. This is enough to show that $N(IJ) = N(I)N(J)$ for all I, J. We have the following short exacts sequence of abelian groups:

$$0 \to P^a/P^{a+1} \to D/P^{a+1} \to D/P^a \to 0.$$

So $\#(D/P^{a+1}) = \#(D/P^a)\#(P^a/P^{a+1})$. Thus, we just need to show that $\#(D^P) = \#(P^a/P^{a+1})$. Note that P^a/P^{a+1} is a vector space over D/P, via $(d + P)(\alpha + P^{a+1}) = (d\alpha + P^{a+1})$. But $(PD_P)^a = P^a D_P$, and $P^a D_P/P^{a+1}D_P = t^a D_P/t^{a+1}D_P$ where t is a uniformizer at P. Thus, t^a generates $P^a D_P/P^{a+1}D_P$ as a D_P-module, and so also as a (D_P/PD_P)-module. So $P^a D_P/P^{a+1}D_P$ is a one-dimensional (D/P)-vector space. But the identity map induces a non-zero injective linear transformation $P^a/P^{a+1} \hookrightarrow P^a D_P/P^{a+1}D_P$, so P^a/P^{a+1} is a one-dimensional (D/P)-vector space.

Question. Factor (10) in $\mathbb{Z}[\sqrt{6}]$.

Solution: The norm of (10) is 100, so the factors of (10) must have norm that has $2, 2^2, 5, 5^2$. Note that $(10) = (2)(5) = (-2+\sqrt{6})(-2-\sqrt{6})(1+\sqrt{6})(1-\sqrt{6})$. Note that the ideals cannot be factored further since each ideal has a prime norm. (End of my solution)

Consider $\mathbb{Z}[\sqrt{6}]/(2) \cong \mathbb{Z}[x]/(x^2-6,2) \cong \mathbb{Z}[x]/(x^2)/2 \cong (\mathbb{Z}/2\mathbb{Z})[x]/(x^2)$. This is not a field since x is a zero divisor. So $(2,\sqrt{6})$ contains the ideal (2) but is *not* a unit ideal. So $(2) = (2,\sqrt{6})^2$. Do the same thing for $\mathbb{Z}[\sqrt{6}]/(5) \cong (\mathbb{Z}/5\mathbb{Z})[x]/(x^2-1) \cong (\mathbb{Z}/5\mathbb{Z})[x]/(x+1) \oplus (\mathbb{Z}/5\mathbb{Z})[x]/(x-1)$. Since $x = \sqrt{6}$, we have $(5) = (1+\sqrt{6})(1-\sqrt{6})$.

18. February 23: More factorizations

More generally, $\mathbb{Z}[\alpha]/(p) \cong \mathbb{Z}[x]/(m(x),p) \cong (\mathbb{Z}/p\mathbb{Z})[x]/(m(x))$, where $m(x)$ is the minimal polynomial of α over $\mathbb{Q}$. In particular, p is prime in $\mathbb{Z}[\alpha]$ if and only if $m(x)$ is irreducible mod p. Even better, prime ideals of $\mathbb{Z}[\alpha]$ that contain p correspond one-to-one with irreducible factors of $m(x)$ mod p.

So we know how ideals factor. But what about factoring elements? As an example:

Question. Factor $10 \in \mathbb{Z}[\sqrt{10}]$ into primes, or prove that it's impossible. Note that not every element can be factored into primes. Recall that primes are defined to be the generators of prime ideals.

Solution: First, take a look at the factorization of (10), which is $(2,\sqrt{10})^2(5,\sqrt{10})^2$. To factor 10 into primes, we need to find generators of $(2,\sqrt{10})$ and $(5,\sqrt{10})$ or prove that none exists. Take the norm of $(2,\sqrt{10})$, which is $\mathrm{N}(2,\sqrt{10}) = 2$. If $(2,\sqrt{10}) = (a+b\sqrt{10})$, then $\mathrm{N}(a+b\sqrt{10}) = 2$. The norm of $(a+b\sqrt{10})$ is a^2-10b^2. If $a^2-10b^2 = 2$, then there is no solution, since $a^2 = 10b^2+2$ and no square integer can have 2 as a unit digit. Thus $(2,\sqrt{10})$ is not principal, hence 10 cannot be factored into primes. Note that when it comes to factoring elements, you only care about *principal prime ideals*. The principal fractional ideals are a subgroup of the group of invertible ideals. This prompts us to introduce a new definition:

Definition 18.1. The quotient defined above is called the *ideal class group* of $\mathcal{O}_K$:

$$\mathrm{Cl}(\mathcal{O}_K) = \mathrm{Cl}(K) = \frac{\text{fractional ideals}}{\text{principal ideals}}$$

Remark 18.1. $\mathrm{Cl}(\mathcal{O}_K) = \{1\}$ iff $\mathcal{O}_K$ is a PID. So the ideal class group "to which extent" $\mathcal{O}_K$ is a PID.

19. February 25

Definition 19.1. We define the *norm of an element* $\alpha \in \mathcal{O}_K$ as follows:

$$\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \prod_i \Phi_i(\alpha),$$

where $\{\Phi_1, \ldots, \Phi_d\}$ are the homomorphisms $\Phi_i : K \hookrightarrow \mathbb{C}$. If $K/\mathbb{Q}$ is Galois and if $G = \mathrm{Gal}(K/\mathbb{Q})$, then

$$\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \left(\prod_{\sigma\in G} \sigma(\alpha)\right)^m,$$

where $m = [K : \mathbb{Q}(\alpha)]$.

Example 19.2. Note that $\mathrm{N}_{\mathbb{Q}}(2) = 2$ and $\mathrm{N}_{\mathbb{Q}(\sqrt{2})}(2) = 2 \cdot 2 = 4$. In general, $\mathrm{N}_K(2) = 2^d$, where $d = [K : \mathbb{Q}]$. Even more generally, if $[L : K] = m$, then $\mathrm{N}_L(\alpha) = \mathrm{N}_K(\alpha)^m$.

Remark 19.1. Note that $|\mathrm{N}_K(\alpha)| = N(\alpha\mathcal{O}_K)$. Also, $\mathrm{N}_K(\alpha) \in \mathbb{Z}$ if $\alpha \in \mathcal{O}_K$. Also, $\mathrm{N}_K(\alpha) = ((-1)^d a_0)^{n/d}$ where a_0 is the constant coefficient in the monic minimal polynomial for α over $\mathbb{Q}$ and $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ and $n = [K : \mathbb{Q}]$.

Proposition 19.3. $\mathrm{N}_K(\alpha) = \pm 1$ *if and only if* $\alpha \in \mathcal{O}_K^*$.

Proof. ($\Rightarrow$) Suppose $\mathrm{N}_K(\alpha) = \pm 1$, and suppose without loss of generality that $\Phi_1 \equiv \mathrm{id}$. Then

$$\alpha \prod_{i=2}^{d} \Phi_i(\alpha) = \pm 1 \in \mathcal{O}_K^*,$$

so $\alpha \in \mathcal{O}_K$, with inverse $\prod \Phi_i(\alpha)$.

($\Leftarrow$) If $\alpha \in \mathcal{O}_K^*$, then $\alpha\beta = 1$ for some $\beta \in \mathcal{O}_K$. Then $1 = \mathrm{N}_K(1) = \mathrm{N}_K(\alpha\beta) = \mathrm{N}_K(\alpha)\,\mathrm{N}_K(\beta)$, so $\mathrm{N}_K(\alpha) \in \mathbb{Z}$ is a unit. Therefore $\mathrm{N}_K(\alpha) = \pm 1$. □

Definition 19.4. We define the *trace of an element* $\alpha \in \mathcal{O}_K$ as follows:

$$\mathrm{tr}_K(\alpha) = \sum_{i=1}^{d} \Phi_i(\alpha).$$

Note that $\mathrm{tr}_K(\alpha) \in \mathbb{Z}$ if $\alpha \in \mathcal{O}_K$ and $\mathrm{tr}(\alpha + \beta) = \mathrm{tr}(\alpha) + \mathrm{tr}(\beta)$. Also, $\mathrm{tr}_L(\alpha) = m\,\mathrm{tr}_K(\alpha)$, where $m = [L : K]$.

Question. Compute the norm and trace of $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. If you want some additional challenge, then compute $\mathrm{N}_K(\zeta_n)$, where $K = \mathbb{Q}(\zeta_n)$ where $\zeta_n = e^{2\pi i/n}$. If you are *still* bored, compute $\mathrm{tr}_K(\zeta_n)$.

Solution: $\mathrm{N}_{\mathbb{Q}(\sqrt{2},\sqrt{3})}(\sqrt{2}+\sqrt{3}) = (\sqrt{2}+\sqrt{3})(\sqrt{2}-\sqrt{3})(-\sqrt{2}+\sqrt{3})(-\sqrt{2}-\sqrt{3}) = 1$. As for trace, $\mathrm{tr}_{\mathbb{Q}(\sqrt{2},\sqrt{3})}(\sqrt{2}+\sqrt{3}) = 0$.

The norm of ζ_n is always 1. Note that

$$\mathrm{N}_K(\zeta_n) = \prod_{\substack{a=1 \\ (a,n)=1}}^{n} \zeta_n^a.$$

This product is a product of factors of the form $\zeta_n^a \zeta_n^{-a} = 1$. Note that ζ_n^a and ζ_n^{-a} are distinct as long as $n \geq 3$. Thus $\mathrm{N}_K(\zeta_n) = 1$. Trace is

$$\mathrm{tr}_K(\zeta_n) = \sum_{\substack{a=1 \\ (a,n)=1}}^{n} \zeta_n^a = \mu(n),$$

where $\mu(n)$ is the Möbius function.

Definition 19.5. If $\mathfrak{p} \subseteq \mathcal{O}_K$ is a prime ideal, then $\mathrm{N}(\mathfrak{p}) = p^F$ for some integer $F \geq 1$ and some prime p. Then the integer F is called the *inertial degree of* $\mathfrak{p}$, written $F_K(\mathfrak{p})$.

Also, suppose $\mathfrak{p}\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$ for prime ideals $\mathfrak{p}_i \in \mathcal{O}_K$. Then $e_i := e_K(\mathfrak{p}_i)$ is called the *ramification index of* $\mathfrak{p}_i$ *in* $\mathcal{O}_K$; and $g = g_k(\mathfrak{p})$ is called the *decomposition number of* $\mathfrak{p}$ *in* K.

20. February 27

Theorem 20.1.

$$\sum_{p\in\mathfrak{p}} e_K(\mathfrak{p})F_K(\mathfrak{p}) = [K:\mathbb{Q}].$$

Proof. Write $p\mathcal{O}_K = (p) = P_1^{e_1}\cdots P_g^{e_g}$. Then

$$p^{[K:\mathbb{Q}]} = \mathrm{N}(p\mathcal{O}_K) = \mathrm{N}(P_1)^{e_1}\cdots\mathrm{N}(P_g)^{e_g} = (p^{f_1})^{e_1}\cdots(p^{f_g})^{e_g}$$

Therefore $[K:\mathbb{Q}] = e_1f_1 + \cdots + e_gf_g$ as needed. □

Definition 20.2. We say that p *ramifies in* K if and only if $e_K(\mathfrak{p}) \geq 2$ for some ideal $\mathfrak{p}$ for some ideal $\mathfrak{p}$ containing p. Otherwise, we say that p is *unramified*.

Remark 20.1. Note that p ramifies in K (say $\mathcal{O}_K = \mathbb{Z}[\alpha]$) if and only if $m(x)$ has a multiple factor mod p, where $m(x)$ is the monic polynomial for α over $\mathbb{Z}$, which happens if and only if $p \in (m(x), m'(x)) \subset \mathbb{Z}[x]$. And this is equivalent to saying that p divides $\mathrm{disc}(m(x)) = \mathrm{disc}(\mathbb{Z}[\alpha])$. In general, p ramifies in K iff $p \,|\, \mathrm{disc}(K)$.

Question. Let $d \neq 1$ be a square-free integer. Which primes ramify in $\mathbb{Q}(\sqrt{d})$?

Solution: If $d \equiv 2, 3 \pmod 4$ then its discriminant is $4d$. Therefore if $p = 2$ or p is a prime dividing d, then p ramifies. If $d \equiv 1 \pmod 4$, then its discriminant is d. Then if $p \,|\, d$, then p ramifies.

20.1. Quick detour to DVRs.

Definition 20.3. A *discrete valuation ring (DVR)* is a Noetherian local domain D with a principal maximal ideal P. If $P = (t)$, then t is called a *uniformizer for* D.

Proposition 20.4. *Every element of D can be written in the form ut^a where $u \in D^*, a \in \mathbb{Z}, a \geq 0$. Every element of $K(D)$ (fraction field of D) can be written in the form ut^a for $u \in D^*, a \in \mathbb{Z}$. The ideals of D are* exactly *(t^a) for $a \in \mathbb{Z}_{\geq 0}$.*

Remark 20.2. In this course, our DVR's are local rings of Dedekind domains at a prime ideal P:

$$D_P = \{ab^{-1} : a, b \in D, b \notin P\}$$
$$D_P^* = \{ab^{-1} : a, b \in D, a, b \notin P\}.$$

Example 20.5. $\mathbb{Z}_{(5)} = \{ab^{-1} : b \in (5)\}$, and $\mathbb{Z}_{(5)}^* = \{ab^{-1} : a, b \notin (5)\}$. Then $P = 5\mathbb{Z}_{(5)} = \{ab^{-1} : a \in (5), b \notin (5)\}$. So 5 is a uniformizer for $\mathbb{Z}_{(5)}$. In fact, 120 works also since $120 = 5 \cdot 24$ and 24 is a unit in $\mathbb{Z}_{(5)}$.

Example 20.6. Let $D = \mathbb{Z}[\sqrt{10}]$ and $P = (5, \sqrt{10})$. Then $\sqrt{10}$ is a uniformizer for D_P because:

$$PD_P = (5, \sqrt{10})D_P = \left(\frac{(\sqrt{10})^2}{2}, \sqrt{10}\right) D_P = \sqrt{10}D_P.$$

Proposition 20.7. *More generally, if $P = (a_1, \ldots, a_n)$ as an ideal of D, then for some i, we have $PD_P = a_iD_P$.*

Proof. Write $a_i = u_i t^{r_i}$ for $u_i \in D_P^*, r_i \in \mathbb{Z}_{\geq 0}$ and t a uniformizer. Then

$$PD_P = (u_1 t^{r_1}, \ldots, u_n t^{r_n}) D_P = (t_1^{r_1}, \ldots, t_n^{r_n}) D_p = (t^r) D_P,$$

where $r = \min(r_i)$. So if without loss of generality $r_1 = r$, then $PD_P = (a_1) D_P$. □

21. March 2

Definition 21.1. Let K be a number field and $\mathcal{O}_K$ its ring of integers. The class group of K is

$$\mathrm{Cl}(K) := \frac{\{\text{non-zero fractional ideals}\}}{\{\text{principal non-zero fractional ideals}\}}.$$

Remark 21.1. Note that $\mathrm{Cl}(K) = \{1\}$ iff $\mathcal{O}_K$ is a PID.

We shall next show that $\mathrm{Cl}(K)$ is *finite*. Roughly speaking, if $\#\,\mathrm{Cl}(K) = n$, then about $\frac{1}{\#\,\mathrm{Cl}(K)}$ of the ideals of $\mathcal{O}_K$ are principal. Meanwhile, it is possible for a Dedekind domain to have an infinite class group. In this case, *almost every* ideal (i.e. all but "0%" of those) is non-principal. Note that this does *not* mean that no ideal is principal.

Definition 21.2. Two fractional ideals I, J of $\mathcal{O}_K$ are equivalent in $\mathrm{Cl}(K)$ iff there is some $\lambda \in K^*$ such that $I = \lambda J$.

We want to show that the number of equivalence classes is finite. We will write down a finite set S of non-zero fractional ideals of $\mathcal{O}_K$ and prove that every non-zero fractional ideal of $\mathcal{O}_K$ is equivalent to an ideal in S. If we fix a real number M, the set of integral ideals $I \subset \mathcal{O}_K$ with $\mathrm{N}(I) \leq M$ is finite. this is because $I = P_1^{e_1} \cdots P_g^{e_g}$, so if $\mathrm{N}(I) \leq M$ then $\mathrm{N}(P_i) \leq M$ as well. Put $N(P_i) = p_i^{f_i}$ so $p_i \leq M$. There are only finitely many such $p_i \in \mathbb{Z}$, and so only finitely many $P \subseteq \mathcal{O}_K$ with $p_i \in P$ and so only finitely many $I \subset \mathcal{O}_K$ that can be built from these P's and still have $\mathrm{N}(I) \leq M$.

Our strategy: we will choose M cleverly and then show that every non-zero fractional ideal of $\mathcal{O}_K$ is equivalent town integral ideal of norm $\leq M$. If $\lambda = a/b \in K^*$ $(a, b \in \mathcal{O}_K)$, we define $\mathrm{N}(\lambda) = \mathrm{N}(a)\,\mathrm{N}(b)$. It is boring and easy to show that this is well-defined. Then $\mathrm{N}(\lambda I) = |\,\mathrm{N}(\lambda)|\,\mathrm{N}(I)$, where $\mathrm{N}(P_1^{e_1} P_2^{e_2} \cdots P_g^{e_g}) = \prod \mathrm{N}(P_i)^{e_i}$ even if $e_i < 0$. For a general I, we need to find $\lambda \in K^*$ such that

- $\lambda I \subset \mathcal{O}_K$; and
- $|\mathrm{N}(\lambda)| \leq M \cdot \mathrm{N}(I)^{-1}$.

The first condition is equivalent to $\lambda \in I^{-1}$. Now we need the following insight by Minkowski: a fractional ideal is a lattice in the Minkowski space, and that a lattice ought to contain a non-zero vector that's not too big compared to its determinant.

Question. Say $L \subset \mathbb{Z}^2$ is a full lattice. Prove that L contains a non-zero vector of length at most $|\det(L)| = |\det(\text{basis of } L)|$.

Proof. Note $\#(\mathbb{Z}^2/L) = |\det(L)|$, so $dv \in L$ for all $v \in \mathbb{Z}^2$. So $(0, d) \in L$. □

22. March 4

Theorem 22.1 (Minkowski's convex body theorem)**.** *Let L be a lattice of rank n in $\mathbb{R}^n$. Let $B \subset \mathbb{R}^n$ be a subset that is convex, centrally symmetric, and such that*

$$\mathrm{vol}(B) > 2^n \det(L) = 2^n \sqrt{|\mathrm{disc}(L)|}.$$

Then B contains a non-zero element of L.

Proof. To use this, we want to relate I to this theorem. So we want to find $x \in K^*$ with small norm. Recall that

$$|\mathrm{N}(\lambda)| = \prod_i |\Phi_i(\lambda)|,$$

where $\Phi_i : K \to \mathbb{C}$ is the i-th embedding.

To bound $|\mathrm{N}(\lambda)|$, we will bound $|\Phi_i(\lambda)|$ for all i. Let B be the set of all points $(a_1, \dots, a_{r+s})$ in the Minkowski space such that $|a_i| < c_i$ for some positive real number c_i that we shall cleverly choose later. Then the volume will become

$$\mathrm{vol}(B) = 2^r \prod_{i=1}^{r} c_i \left(\prod_{j=r+1}^{r+s} \pi c_i^2 \right) = 2^r \pi^s \prod_{i=1}^{r+s} c_i^{m_i}$$

where $m_i = 1$ if Φ_i real and $m_i = 2$ if Φ_i complex.

Recall that we need $\lambda \in K^*$ such that $\lambda \in I^{-1}$ and $|\mathrm{N}(\lambda)| \text{`} M\, \mathrm{N}(I^{-1})$.

To apply Minkowski's theorem, we need

$$\mathrm{vol}(B) > 2^n \sqrt{\mathrm{disc}(I^{-1})} = 2^{r+2s} \sqrt{|\operatorname{disc}(K)|}\, \mathrm{N}(I^{-1}).$$

So we need

$$2^r \pi^s \prod_{i=1}^{r+s} c_i^{m_i} > 2^{r+2s} \sqrt{|d_K|}\, \mathrm{N}(I^{-1}).$$

Choose the c_i so that this is satisfied; this gives us $\lambda \in I^{-1}$ such that

$$|\mathrm{N}(\lambda)| \le \frac{2^{2s} \sqrt{|d_K|}}{\pi^s\, \mathrm{N}(I)} + \varepsilon$$

for any $\varepsilon > 0$. Since I^{-1} is discrete, we can take $\varepsilon = 0$ so we can find $\lambda \in I^{-1}$ such that

$$|\mathrm{N}(\lambda)| \le \left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}\, \mathrm{N}(I^{-1}),$$

so

$$|\mathrm{N}(\lambda I)| \le \left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}.$$

If $M = \left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}$, then every ideal class contains an integral ideal of norms of at most M. □

In fact, with more care in choosing B, one can actually take

$$M = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|d_K|}.$$

This result can be used to compute $\mathrm{Cl}(K)$.

Example 22.2. Compute $\mathrm{Cl}(\mathbb{Z}[\sqrt{6}])$. The minimal polynomial of $\sqrt{6}$ is x^2-6. Now time to plug in some small integers:

n	n^2-6
-2	-2
-1	-5
0	$-6=-2\cdot 3$
1	-5
2	-2

Note that $f(n)=\mathrm{N}(\sqrt{6}-n)$. Since $d_K=4\cdot 6=24$, it follows that we can take

$$M=\left(\frac{4}{\pi}\right)^0\frac{2!}{2^2}\sqrt{24}<\frac{5}{2}<3.$$

Thus every ideal class contains an ideal of norm less than 3. There is only one ideal class of norm less than f and it's $(2,\sqrt{6})=(2+\sqrt{6})$ (norm is 2 by the table above). Hence $\mathrm{Cl}(\mathbb{Z}[\sqrt{6}])=\{1\}$ so $\mathbb{Z}[\sqrt{6}]$ is a PID.

23. March 6

Example 23.1. Let's compute $\mathrm{Cl}(\mathbb{Q}(\sqrt{66}))$. Here is how we will do it:

(1) Compute $\mathrm{disc}(K)$.
Since $66\not\equiv 1 \pmod 4$, the discriminant is $\mathrm{disc}(K)=2^3\cdot 3\cdot 11$.

(2) Estimate $M=\left(\frac{4}{\pi}\right)^s\frac{n!}{n^n}\sqrt{|\mathrm{disc}(K)|}$.
There are no complex embeddings, and $[K:\mathbb{Q}]=n=2$. Therefore it follows $M=\frac{1}{2}\sqrt{2^3\cdot 3\cdot 11}<9$.

(3) Plug in small integers for x to $f(x)$ and factor the results.
In this case, $f(x)=x^2-66$. How many and which integers should I plug in? We want $f(x)$ to be "small", and complete set of residues of residues mod p for all $p<9$.

n	n^2-66
5	-41
6	$-30=-2\cdot 3\cdot 5$
7	-17
8	-2
9	$15=3\cdot 5$
10	$34=2\cdot 17$
11	$55=5\cdot 11$

Since $2\,|\,\mathrm{disc}(K)$, it follows that (2) must ramify. Therefore $(2)=P_2^2$ for some prime ideal P_2. Similarly, $3\,|\,\mathrm{disc}(K)$ so $(3)=P_3^2$ for some prime ideal P_3. But 5 cannot ramify, but since $f(6)$ and $f(9)$ are divisible by 5, this ideal splits. So $(5)=P_5Q_5$, where P_5 is a prime ideal containing (5) that divides $(\sqrt{66}-6)$, and Q_5 a prime ideal containing (5) that divides $(\sqrt{66}-9)$. As for (7), we don't see any value of $f(n)$ that is divisible by 7. So (7) is inert. Hence (7) is prime.

(4) Use the table to find relations in $\mathrm{Cl}(K)$.
Note that $P_2^2\equiv 1\equiv P_3^2\equiv P_5Q_5$ (i.e., trivial in the class group, i.e., they are principal ideals), and again by the table we see that $(\sqrt{66}-6)=P_2P_3P_5\equiv 1$. Note that since $f(8)=-2$ we see that $(\sqrt{66}-8)=P_2\equiv 1$. Also, we see $(\sqrt{66}-9)=P_3Q_5\equiv 1$. So

we see that there are four potential generators, P_2, P_3, P_5, Q_5. $P_2 \equiv 1$, so $P_2P_3P_5 \equiv P_3P_5 \equiv 1$. Therefore $P_3 \equiv P_5^{-1} \equiv P_3$ in $\mathrm{Cl}(K)$. So this means that we don't need P_3 and P_5 either. But also $P_3Q_5 \equiv 1$, or $P_3 \equiv Q_5$. Therefore we don't need Q_5 either, leaving us with P_3 only. Thus $\mathrm{Cl}(K) = \langle P_3 \rangle$. Now the question is: is P_3 principal or not? If so, then $\mathrm{Cl}(K)$ will be trivial; otherwise, $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$.

(5) For ideals that don't look principal, try to prove they're not principal.
$P_3 = (3, \sqrt{66})$. So $\mathrm{N}(P_3) = 3$. If P_3 is principal, then there exist $a, b \in \mathbb{Z}$ such that $\mathrm{N}(a + b\sqrt{66}) = a^2 - 66b^2 = 3$. There is no such (a, b): reduce the relation to mod 9 then we will see that $a^2 \equiv 0 \pmod 9$ and $-3b^2 \equiv 3 \pmod 9$. So $b^2 \equiv -1 \pmod 3$ but this is impossible. Therefore P_3 is not principal.

24. March 9: More ideal class group computation

Example 24.1. Let's compute $\mathrm{Cl}(K)$ for $K = \mathbb{Q}(\alpha)$, where α is a root of $x^3 + 2x - 5$. Let's go through the five steps we mentioned last time:

(1) Compute $\mathrm{disc}(K)$.
Turns out that $\mathrm{disc}(K) = -707 = -7 \cdot 101$. So 7 and 101 are the only two (rational) primes that ramify. Since the discriminant is square-free, it follows that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

(2) Estimate $M = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|\mathrm{disc}(K)|}$.
There is one pair of complex conjugate embeddings, so $M = \frac{4}{\pi} \cdot \frac{3!}{3^3} \sqrt{707} < 8$. So $\mathrm{Cl}(K)$ is generated by prime ideals of norm $2, 3, 4, 5, 7$ (all the prime powers less than 8).

(3) Plug in small integers for x to $f(x)$ and factor the results.
In this case, $f(x) = x^3 + 2x - 5$. How many and which integers should I plug in? We want $f(x)$ to be "small", and complete set of residues of residues mod p for all $p < 7$. So in this case, all the residues mod 7 will do the trick.

n	$f(n)$
-3	$-2 \cdot 19$
-2	-17
-1	-2^3
0	-5
1	-2
2	7
3	$2^2 \cdot 7$

Now it is time to factor some ideals generated by (rational) primes. Note that $x^3 + 2x - 5 = (x + 1)(x^2 + x + 1) \bmod 2$, so there is a prime ideal of norm 2: call this P_2. There can only be one prime ideal of norm 2, and (2) does not ramify and $\mathrm{N}((2)) = 8$ so there exists a prime ideal Q_2 of norm 4 such that $(2) = P_2Q_2$. Note that (3) is inert hence prime since none of the values of $f(n)$'s written in the table above are divisible by 3. As for (5), note that $x^3 + 2x = x(x^2 + 2) \bmod 5$, so there exist a prime ideal of norm 5 (say P_5) such that $P_5 \,|\, (5)$. And this is the only prime ideal of norm 5 (look at the factorization of $f(x)$ mod 5). So $(5) = P_5Q_5$ where Q_5 is a prime ideal of norm 25 (also, recall that (5) does not ramify).

What about (7)? Recall that (7) ramifies since $7 \mid \mathrm{disc}(K)$. Note that $x^3+2x-5 \equiv (x-2)^2(x-3) \bmod 7$, so $(7) = P_7^2 Q_7$, where P_7 and Q_7 are two distinct prime ideals of norm 7.

(4) Use the table to find relations in $\mathrm{Cl}(K)$.
So $P_2Q_2 \equiv P_5Q_5 \equiv P_7^2Q_7 \equiv 1$. Since (α) has norm 5, we have $(\alpha) = P_5 \equiv 1$. Since $(\alpha-1)$ has norm 2, we see that $(\alpha-1) = P_2 \equiv 1$. $(\alpha-2)$ has norm 7, so $(\alpha-2) = P_7 \equiv 1$. By the factorization in mod 7, we see that P_7 a prime ideal containing $(\alpha-2)$ and Q_7 a prime ideal containing $(\alpha-3)$. Thus Q_2 and Q_5 are also principal. Similarly Q_7 is also principal.

(5) For ideals that don't look principal, try to prove they're not principal.
There is nothing to do here, since we see that the generators of $\mathrm{Cl}(K)$ are all principal. Thus $\mathrm{Cl}(K)$ is trivial, thereby proving that $\mathbb{Z}[\alpha]$ is a PID.

25. March 11 & 13

Theorem 25.1 (Lagrange)**.** *Every positive integer is the sum of four squares.*

Proof. Let $m \in \mathbb{Z}, m > 0$. It suffices to assume that m is square-free. Factor $m = p_1 p_2 \cdots p_r$ where each p_i is a prime.

We want to find $(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4$ such that $x_1^2+x_2^2+x_3^2+x_4^2 = m$. Note that $m = \|x\|^2$ where $x = (x_1, x_2, x_3, x_4)$. Now our strategy will be as follows: find $x \in \mathbb{Z}^4 \setminus \{(0,0,0,0)\}$ with $\|x\| < \sqrt{2m}$ and $\|x\|^2 \equiv 0 \pmod{p_i}$ for all i.

Lagrange's trick: write $x_1 \equiv a_i x_3 + b_i x_4 \pmod{p_i}$ and $x_2 \equiv b_i x_3 - a_i x_4 \pmod{p_i}$ for appropriately chosen a_i and b_i. Then we have

$$\begin{aligned}\|x\|^2 &\equiv a_i^2 x_3^2 + 2a_i b_i x_3 x_4 + b_i^2 x_4^2 + b_i^2 x_3^2 - 2a_i b_i x_3 x_4 + a_i^2 x_4^2 + x_3^2 + x_4^2 \\ &\equiv (a_i^2 + b_i^2 + 1)(x_3^2 + x_4^2).\end{aligned}$$

So if we can pick a_i and b_i so that $a_i^2 + b_i^2 \equiv -1 \pmod{p_i}$ for all i, then we are home free. If $p_i = 2$, we see that $a_i = 1$ and $b_i = 0$ do the trick. Otherwise, there are $\frac{p+1}{2}$ possible values of $a_i^2 \pmod{p_i}$, and $\frac{p_i+1}{2}$ possible values of $-b_i^2 - 1 \pmod{p_i}$. More than half of integers mod p_i are of the form a_i^2, and more than half of integers mod p_i are of the form $-b_i^2 - 1$. So at least one integer mod p_i is of both forms, yielding a solution to $a_i^2 + b_i^2 + 1 \equiv 0 \pmod{p_i}$. By the Chinese remainder theorem, this means that there is a non-zero x such that $\|x\|^2 \equiv 0 \pmod{m}$. So we are only left with ensuring that $\|x\|^2 < 2m$. This is we use the geometry of numbers.

Pick $a_i, b_i \in \mathbb{Z}$ such that $a_i^2 + b_i^2 + 1 \equiv 0 \pmod{p_i}$. Define $L = \{x \in \mathbb{Z}^4 : x_1 \equiv a_i x_3 + b_i x_4 \pmod{p_i}, x_2 \equiv b_i x_3 - a_i x_4 \pmod{p_i}\}$. Then L is a lattice of rank four in $\mathbb{R}^4$. To see why, start by observing that L is the kernel of the homomorphism $\phi : \mathbb{Z}^4 \to (\mathbb{Z}/p_i\mathbb{Z})^2 \times \cdots \times (\mathbb{Z}/p_r\mathbb{Z})^2$ defined by $(x_1, x_2, x_3, x_4) \mapsto (x_1 - a_1x_3 - b_1x_4 \bmod p_1, x_2 - b_1x_3 + a_1x_4 \bmod p_1, \ldots, x_1 - a_r x_3 - b_r x_4, x_2 - b_r x_3 + a_r x_4 \bmod p_r)$. So $\operatorname{im}\phi$ is finite, meaning that the $\mathrm{rank}(L) = \mathrm{rank}(\mathbb{Z}^4) = 4$. So the index of L in $\mathbb{Z}^4$ is $\#\operatorname{im}\phi \le m^2$. Thus $\det(L) \le m^2$. Recall that Minkowski's convex body theorem states that if $\mathrm{vol}(B) > 2^4 \cdot \det(L)$, then B will contain a non-zero element in L.

Let B be the sphere of radius $\sqrt{2m}$ in $\mathbb{R}^4$. The volume of the 4-sphere of radius r is $\frac{1}{2}\pi^2 r^4$, so

$$\mathrm{vol}(B) = \frac{\pi^2}{2}(2m)^2 = 2\pi^2 m^2 > 2^4 \det(L),$$

so Minkowski's convex body theorem implies that there is a non-zero vector $x \in L \cap B$. $x \in L$ implies that $x_1^2+x_2^2+x_3^2+x_4^2 \equiv 0 \pmod{m}$. $x \in B$ implies that $x_1^2+x_2^2+x_3^2+x_4^2 < 2m$. That $x \neq 0$ implies that $x_1^2+x_2^2+x_3^2+x_4^2 > 0$. As we wanted, we now have $x_1^2+x_2^2+x_3^2+x_4^2 = m$. This completes the proof. □

Recall that in any fractional ideal I of $\mathcal{O}_K$ (of degree n), we know that there is a non-zero element α with $|\mathrm{N}(\alpha)| \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\mathrm{disc}(K)|}$, where s is the number of pairs of complex conjugate embeddings.

If we choose $I = (1) = K$, then $\sqrt{|\mathrm{disc}(K)|} \geq \left(\frac{\pi}{4}\right)^s \frac{n!}{n^n} \geq \left(\frac{\pi}{4}\right)^{n/2} \frac{n!}{n^n}$. The last quantity is strictly increasing if $n \geq 2$, and if $n = 2$ it equals $\frac{\pi}{4} \cdot 2 > 1$. So if $K \neq \mathbb{Q}$, then $|\mathrm{disc}(K)| > 1$. Therefore, there exists at least one prime dividing $\mathrm{disc}(K)$, so every number field has at least one ramified prime.

Question. Classify all the sublattices of $\mathbb{Z}^2$ with index p, where p is a prime.

Solution: Every sublattice L of index p satisfies $p\mathbb{Z} \times p\mathbb{Z} \subseteq L \subseteq \mathbb{Z}^2$, and $[\mathbb{Z}^2 : L] = [L : p\mathbb{Z} \times p\mathbb{Z}] = p$. Therefore there is a correspondence between L and a subgroup of $(\mathbb{Z}/p\mathbb{Z})^2$ of order p. Thus L is a 1-dimensional subspace of $(\mathbb{Z}/p\mathbb{Z})^2$. There are $p^2 - 1$ non-zero elements, and all non-zero elements have order p. So $(p^2-1)/(p-1) = p+1$ subgroups of order p. Each of $(0,1), (1,1) \ldots, (p-1,1), (1,0)$ generates a distinct subgroup. Now we need to lift it back up to obtain bases. So we get $\{(0,1),(p,0)\}, \{(1,1),(p,0)\}, \cdots, \{(p-1,1),(p,0)\}, \{(1,0),(0,p)\}$.

26. March 16

Theorem 26.1 (Minkowski's convex body theorem)**.** *Let B be a measurable, convex, centrally symmetric subset of $\mathbb{R}^n$. Let $L \subseteq \mathbb{R}^n$ be a lattice. If $\mathrm{vol}(B) > 2^n \det(L)$ then B contains a non-zero vector from L.*

We usually use this to get the following corollary:

Corollary 26.2. *Let K be a number field of degree $n = r+2s$. Let $M = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\mathrm{disc}(K)|}$. Let $\mathcal{O}_K$ be the ring of integers. Then every fractional ideal in $\mathcal{O}_K$ is equivalent to an integral ideal of norm at most M. That is, for any fractional ideal I, there exists $\alpha \neq 0$ such that αI is an integral ideal of norm at most M.*

Proof (general idea). Use the lattice coming from the Minkowski space

$$\phi(x) = (\phi_1(x), \ldots, \phi_r(x), \phi_{r+1}(x), \ldots, \phi_{r+s}(x))$$

and $L = \phi(\mathcal{O}_K)$. □

Theorem 26.3 (Hermite)**.** *Let $N \in \mathbb{R}$. Then there are only finitely many number fields K with $|\mathrm{disc}(K)| < N$.*

Proof. We know that $|\mathrm{disc}(K)| > \left(\frac{\pi}{4}\right)^s \frac{n^n}{n!} > \left(\frac{\pi}{4}\right)^{n/2} \frac{n^n}{n!}$. RHS approaches infinity, so if the degree of K is large enough then $|\mathrm{disc}(K)| > n$. So there are only finitely many n so that $|\mathrm{disc}(K)| < n$.

Hence it suffices to show that there are only finitely many solutions to $|\mathrm{disc}(K)| < N$. Consider $K(\sqrt{-1})$. Either $K = K(\sqrt{-1})$ (i.e., discriminant remains unchanged) or $[K(\sqrt{-1}) : K] = 2$ (discriminant changes by bounded amount). Hence we can restrict our attention to

K of degree n with $\sqrt{-1} \in K$. Further, as there are finitely many $d \in \mathbb{Z}, 0 \leq d \leq N$, we can also fix d. So for fixed d and n, it suffices to prove that there are finitely many $K \ni \sqrt{-1}$ with $|\operatorname{disc}(K)| = d$. In this case, Minkowski space is just $\mathbb{C}^{n/2}$. The lattice is $\phi(\mathcal{O}_K)$. We now need to find a nice, convex, centrally symmetric subset such that for any solution K, there exists a non-zero point in $B \cap L$, where B is some convex body. Then based on that convex body, we will show that there are only finitely many ways of finding the right K, and then show that in $L \cap B$ we have that it is the image of a unique K.

Let $B = \{(z_1, \ldots, z_{n/2}) : |\mathfrak{I}m(z_1)| < c\sqrt{d}, |\mathfrak{R}e(z_1)| < 1, |z_i| < 1, i = 2, \ldots, n/2\}$. Pick L sufficiently large so that $\operatorname{vol}(B) \geq 2^{n/2} \cdot \det(L) \geq 2^{n/2}\sqrt{|d|}$. c depends on n and d but not on K.

Given a solution, eek know good bounds on the roots of its minimal polynomial. This gives us good bounds on the coefficients of an integer polynomial. There are only finitely many such minimal polynomials. Hence only finitely many images of K is mapped to $B \cap L$. Therefore, it remains to prove that one of the $(z_1, \ldots, z_{n/2}) \in B \cap L$ corresponds to a unique K. We know that $\mathbb{Q}(z_1) \subseteq K$. If $\mathbb{Q}(z_1) \neq K$, then there exists $i \neq 1$ such that $\phi_i(z_1) = z_i$. So $z_1 = z_i$ for some i, and we know that $|z_i| < 1$. This means that

$$\mathrm{N}(z_1) = \left| \prod_{i=1}^{n/2} z_j \right| < 1.$$

which is a contradiction. Therefore $\mathbb{Q}(z_1) = K$. Thus there are a finite number of $K = K(\sqrt{-1})$ with $|\operatorname{disc}(K)| = d$ of degree n. Hence there are only finitely many K with $|\operatorname{disc}(K)| < N$, as desired. □

27. March 18 & 20: Structure of the unit group of a number field

Last class using Minkowski's convex body theorem, we proved that there are only finitely many number fields with $|\operatorname{disc}(K)| < N$. We will start by stating a variation of what we proved in last class. We are not going to prove the following theorem, but it's worth noting that with a few additional arguments it is not that hard to prove this.

Theorem 27.1. *Let $P = \{p_1, \ldots, p_n\}$ be a finite set of integers. Then there are only finitely many K with*

$$|\operatorname{disc}(K)| \in \{p_1^{a_1} \cdots p_n^{a_n} : a_i \in \mathbb{N}\}$$

Theorem 27.2 (Dirichlet unit theorem)**.** *Let K be a number field of degree $n = r + 2s$. Then $\mathcal{O}_K^*$, the unit group of the ring of integers of K, is isomorphic to $\mu(K) \times \mathbb{Z}^{r+s-1}$ where $\mu(K)$ are cyclotomic numbers in K (i.e., the roots of unity in K).*

Proof. Consider

$$\psi(z) = (\log|\phi_1(z)|, \log|\phi_2(z)|, \cdots, |\phi_{r+s}(z)|).$$

This map is well-defined on $\mathcal{O}_K^*$ and gives a nice lattice. Notice that

$$|\mathrm{N}(x)| = |\phi_1(x)\phi_2(x)\cdots\phi_r(x)(\phi_{r+1}(x))^2\cdots(\phi_{r+s}(x))^2|.$$

Further, we have

$$\log|\mathrm{N}(x)| = \sum_{i=1}^{r} \log|\phi_i(x)| + 2\sum_{j=r+1}^{r+s} \log|\phi_j(x)|.$$

So the norm relates to the linear map $(y_1, \ldots, y_r, y_{r+1}, \ldots, y_{r+s}) \mapsto y_1 + \cdots + y_r + 2y_{r+1} + \cdots + 2y_{r+s}$. But then since $|\mathrm{N}(x)| = 1$ for all $x \in \mathcal{O}_K^*$, this gives that

$$\psi(\mathcal{O}_K^*) \subseteq H := \{(y_1, \ldots, y_s) : y_1 + \cdots + y_r + 2y_{r+1} + \cdots + 2y_{r+s} = 0\}.$$

Notice that H has dimension $r + s - 1$, which we hope to be helpful in showing that the exponent that appears $\mu(K) \times \mathbb{Z}^{r+s-1}$ is indeed $r + s - 1$. But first, we want to show that

$$1 \to \mu(K) \to \mathcal{O}_K^* \to \psi(\mathcal{O}_K^*) \to 1$$

is a short exact sequence. Notice that $\mathcal{O}_K^* \cong \mu(K) \times \psi(\mathcal{O}_K^*)$ follows as a corollary.

The only non-trivial thing to show is that $\mu(K) = \ker \psi$. Assume that $x \in \mu(K)$. Then $|x| = |\phi_i(x)| = 1$ for all i, so $\psi(x) = (0, 0, \ldots, 0)$ so $x \in \ker \psi$. Now suppose that $x \in \ker \psi$. Then $|\phi_i(x)| = 1$ for all i. There are only finitely many points in the set (actually a group)

$$(\phi_1(x), \ldots, \phi_{r+s}(x)) \cap \{(z_1, \ldots, z_{r+1}) : |z_i| = 1\}.$$

This tells us that $\ker \psi$ is a finite group containing 1 as the identity. So for $x \in \ker \psi$, we have that $x^{|\ker \psi|} = 1$. Therefore x is cyclotomic. This gives that $\ker \psi = \mu(K)$ so indeed the sequence is exact. Therefore $\mathcal{O}_K^* \cong \mu(K) \times \psi(\mathcal{O}_K^*)$. Thus it suffices to show that $\psi(\mathcal{O}_K^*) \cong \mathbb{Z}^{r+s-1}$. As $\psi(\mathcal{O}_K^*)$ is a lattice we have $\psi(\mathcal{O}_K^*) \cong \mathbb{Z}^m$ for some m. Let's show that $m = r + s - 1$.

Step 1: For any bounded C in $\mathbb{R}^{r+s}$ we have that $|\psi(\mathcal{O}_K^*) \cap C|$ is finite. Since C is bounded, then so are $\log |\phi_i(x)|$ for all i. Hence so are $|\phi_i(x)|$ for all i. Therefore all symmetric functions on the $\phi_i(x)$ are bounded. Hence all coefficients in

$$\prod_{i=1}^{r+2s} (z - \phi_i(x)) = z^{r+2s} + a_{r+2s-1} z^{r+2s-1} + \cdots + a_0$$

are bounded, and are integers. This shows that the set is finite. Thus $\psi(\mathcal{O}_K^*) \leq r + s - 1$ as a corollary. Now we must show that $\dim \psi(\mathcal{O}_k^*) \geq r + s - 1$, and we will be done. We shall do this by showing that $\psi(\mathcal{O}_K^*)$ spans H. We will do this by showing that there exists a bounded F such that for all $x, \ldots, x_{r+s} =: x \in H$, we will have $(x) = f + \psi(a)$ where $a \in \mathcal{O}_K^*$. Equivalently, in Minkowski space, we want to show that there exists $E := \psi^{-1}(F)$ so that for all $(y) \in \mathbb{R}^r \times \mathbb{C}^s$ that $(y) = (a) \cdot (e)$, where $(a) = (\phi_1(a), \ldots, \phi_{r+s}(a))$ and $e \in \psi^{-1}(F) = (e_1, \ldots, e_{r+s})$. Consider

$$B(c_1, \ldots, c_{r+s}) := \{(x_1, \ldots, x_{r+s}) : |x_i| < c_i\} \subseteq \mathbb{R}^r \times \mathbb{C}^s.$$

Then the volume is

$$\mathrm{vol}(B) = 2^r \pi^s \prod_{i=1}^{r} c_i \prod_{j=r+1}^{r+s} (c_j)^2 = 2^r \pi^s C',$$

where $C' := (c_1 c_2 \cdots c_r)(c_{r+1} \cdots c_{r+s})^2$. If C' is big enough, then we will have a point $\phi(a) \in B \cap \phi(\mathcal{O}_K)$ for $a \in \phi(\mathcal{O}_K)$. If $(x_1, \ldots, x_{r+s}) \in \psi^{-1}(H)$, then we know that $\log |x_1| + \cdots + \log |x_2| + 2 \log |x_{r+1}| + \cdots + 2 \log |x_{r+s}| = 0$, hence $\log |x_1 x_2 \cdots x_r (x_{r+1} \cdots x_{r+s})^2| = 0$. This gives us that

$$|(x_1 \cdots x_r)(x_{r+1} \cdots x_{r+s})^2| = 1.$$

Note that

$$\begin{aligned}(x)B(c_1,\dots,c_{r+s}) &= \{(z_1x_1,\cdots,z_{r+s}x_{r+s} : |z_i| \le c_i\} \\ &= \left\{(z_1,\dots,z_{r+s}) : |z_i| \le \frac{c_i}{|x_i|}\right\} \\ &= B\left(\frac{c_i}{|x_i|},\dots,\frac{c_{r+s}}{|x_{r+s}|}\right) \\ &= \prod_{i=1}^{r}\left(\frac{c_i}{|x_i|}\right)\prod_{j=r+1}^{r+s}\left(\frac{c_j}{|x_j|}\right)^2 = \frac{C}{1} = C.\end{aligned}$$

So for all $(x) \in \psi^{-1}(H)$, we have a value $a_x \in \mathcal{O}_K$ such that $(a_x) \in (x)\cdot B$. Similarly, we have $(a_{x^{-1}}) \in x^{-1}\cdot B$. So it follows that

$$\begin{aligned}(a_1,\dots,a_{r+s}) &= \left(\frac{z_1}{x_1},\dots,\frac{z_{r+s}}{x_{r+s}}\right) \\ (x_1,\dots,x_{r+s}) &= \left(\frac{z_1}{a_1},\dots,\frac{z_{r+s}}{a_{r+s}}\right),\end{aligned}$$

for all $|z_i| \le c_i$. Hence $(x) \in (a_{1/x}^{-1})\cdot B$.

We want to show that there are only finitely many $(a_{1/x})$. We know that $|\mathrm{N}(a)| \le C$.

Lemma 27.3. *There is a finite eset $T \subseteq \mathcal{O}_K$ such that every $a \in \mathcal{O}_K$ and $|\mathrm{N}(a)| \le C$ then $a = u\cdot t, u \in \mathcal{O}_K^*, t \in T$.*

Proof of the lemma. Ae iuiiet $a \in \mathcal{O}_K$ generates an ideal (a) of norm less than C. There are only finitely many such ideals. If $(a) = (b)$ then $a = bu$ where $u \in \mathcal{O}_K^*$. Let $\{a_1,\dots,a_t\}$ be this finite set so that for all $(x) \in \psi^{-1}(H)$ we have

$$(x) \in \bigcup_{i=1}^{t}(a_i^{-1})B.$$

Let

$$F = \psi^{-1}(H) \cap \left(\bigcup_{i=1}^{t}(a_i^{-1})B\right).$$

Then $E = \psi(F)$ has the desired property. □

Thus the above lemma shows what we want to prove. The proof is therefore complete. □

28. March 23

We proved last time that

Theorem 28.1 (Dirichlet unit theorem)**.** *Let K be a number field with r real embeddings and s complex conjugate pairs of embeddings. Then $\mathcal{O}_K^* \cong \omega \times \mathbb{Z}^{r+s-1}$ where ω is the group of roots of unity in K.*

We will start from an easier case to a harder case. The easiest case? When $\mathcal{O}_K^*$ is finite, that is, when $r+s=1$. If $r=1, s=0$ then $K=\mathbb{Q}$ so $\mathcal{O}_K^* = \langle -1\rangle \cong \mathbb{Z}/2\mathbb{Z}$. If $r=0$ and $s=1$, then $K = \mathbb{Q}(\sqrt{-d})$ for some $d \in \mathbb{Z}$ where d is a positive square-free number. In this

case, if $d = 1$, then $\mathcal{O}_K^* = \langle i \rangle \cong \mathbb{Z}/4\mathbb{Z}$. If $d = 3$, then we have $\mathcal{O}_K^* \cong \mathbb{Z}/6\mathbb{Z}$, and $\mathcal{O}_K^* \cong \mathbb{Z}/2\mathbb{Z}$ otherwise. To see why, note that $\phi(n) = 2$ only when $n = 3, 4, 6$. But when $n = 4$, we already covered this case in $d = 1$. Thus this case matches with $\mathbb{Q}(i)$. As for the remaining two, note that $\mathbb{Q}(\sqrt{-3})$ contain both primitive third roots of unity and the sixth roots of unity. Also, these are the only cases when the units group is finite.

If $r + s = 2$, then there are three cases.

Case I: $(r, s) = (2, 0)$. Then $\omega = \{\pm 1\}$ since K is isomorphic to a subfield of $\mathbb{R}$.

Definition 28.2. A *fundamental unit of* K is a generator for the unit group of K up to multiplication by ± 1.

So how do we find a fundamental unit? Say $K = \mathbb{Q}(\sqrt{d})$ for positive $d \in \mathbb{Z}$. Then $a + b\sqrt{d}$ is a unit iff $a + b\sqrt{d} \in \mathcal{O}_K$ and $\mathrm{N}(a + b\sqrt{d}) = \pm 1$. So we need $a^2 - db^2 = \pm 1$ and $a, b \in \mathbb{Z}$ if $d \not\equiv 1 \pmod 4$, or $a, b \in \frac{1}{2}\mathbb{Z}$ with $a + b \in \mathbb{Z}$ if $d \equiv 1 \pmod 4$. We need to solve either $a^2 - db^2 = \pm 1$ ($d \not\equiv 1 \pmod 4$) or $a^2 - db^2 = \pm 4$ and $a \equiv b \pmod 2$ ($d \equiv 1 \pmod p$). In all cases, we need

$$\left| \frac{a^2}{b^2} - d \right| \leq \frac{4}{b^2}.$$

We are looking for rational numbers close to $\sqrt{d}$.

Example 28.3. Suppose that $K = \mathbb{Q}(\sqrt{2})$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$. Then $\mathrm{N}(1 + \sqrt{2}) = -1$. But how do we know this is a fundamental unit? If not, then there is a fundamental unit β such that $\beta^n = 1 + \sqrt{2}$. If this is true, then $(\log|1 + \sqrt{2}|, \log|1 - \sqrt{2}|) = n(\log|\beta|, \log|\bar{\beta}|)$. Therefore $\log|\beta| < \log|1 + \sqrt{2}|$ and $\log|\bar{\beta}| < \log|1 - \sqrt{2}|$. There are only finitely many elements of $\mathcal{O}_K$ in that box:

$$|\beta| < |1 + \sqrt{2}| < \frac{5}{2}, |\bar{\beta}| < |1 - \sqrt{2}| < \frac{1}{2}.$$

Write $\beta = a + b\sqrt{2}$. Then $|a + b\sqrt{2}| < \frac{5}{2}$ and $|a - b\sqrt{2}| < \frac{1}{2}$. By the triangle inequality, $|a + b\sqrt{2}| + |a - b\sqrt{2}| < 3$, so $-\frac{3}{2} < a < \frac{3}{2}$ and $-3 < 2\sqrt{2}b < 3$. Since a and b are integers, $\{a, b\} \subset \{-1, 0, 1\}$. Therefore $1 + \sqrt{2}$ is indeed a fundamental unit.

Question. Do the same for $\mathbb{Z}[\sqrt{3}]$.

Solution: $\mathrm{N}(2 + \sqrt{3}) = 1$, so $2 + \sqrt{3}$ is a unit. Suppose there is β that's "more fundamental" than $2 + \sqrt{3}$. Then there exists n such that $(\log|2 + \sqrt{3}|, \log|2 - \sqrt{3}|) = n(\log|\beta|, \log|\bar{\beta}|)$. So we have

$$|\beta| < |2 + \sqrt{3}| < 4, |\bar{\beta}| < |2 - \sqrt{3}| < \frac{1}{2}.$$

Let $\beta = a + b\sqrt{3}$. So $-\frac{9}{4} < a < \frac{9}{4}$ and $-\frac{9}{4} < \sqrt{3}b < \frac{9}{4}$.

29. March 25

Question. Do the same for $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

Solution: The same method, but be mindful of the half-integers... The end for today due to evaluation. Really? Yes really!

30. March 27

How can we find all the roots of unity in K? We can't because we don't have enough tools. Let ζ be a root of unity. Then $\zeta \in K$ if and only if $\mathbb{Q}(\zeta) \subset K$. So $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ must divide $[K : \mathbb{Q}]$. If ζ is a primitive n-th root of unity, then $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$, where n is the Euler totient function. This reduces the search to a finite collection of values of n.

Question. For $n = 1, 2, 3, 4, 5$, find the group of roots of unity in every field K with $[K : \mathbb{Q}] = n$.

Solution. If $n = 1$, then $K = \mathbb{Q}$ so $\{\pm 1\}$ is the group we are looking for. As for $n = 3, 5$, note that $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ must be 1, since $\phi(n)$ is always even unless $n = 2$. Thus $\{\pm 1\}$ is the group. Alternatively, one can recognize that every odd-degree extension must have at least one real embedding, from which the same claim follows. We already did the $n = 2$ case in class. So the only non-trivial case that we are left with is $n = 4$. Note that if $\phi(n) = 4$, then $n = 5, 8, 10, 12$. So $\mathbb{Q}(\zeta_{10}) = \mathbb{Q}(\zeta_5), \mathbb{Q}(\zeta_8), \mathbb{Q}(\zeta_{12})$ are the only cyclotomic fields of degree 4. But this is not enough since it may contain a quadratic subextension. We already did this in class: any quadratic extension of $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$ also has non-trivial roots of unity. Those are the only cases where a quartic extension has a non-trivial group of roots of unity. □

Can we do better than this? Yes, we can. Suppose that p ramifies in $\mathbb{Z}[\zeta_n]$, and that $\zeta_n \in K$. Then p must ramify in $\mathcal{O}_K$ also. Better yet, if K is a subfield of L, then $\operatorname{disc}(K) \,|\, \operatorname{disc}(L)$.

Proof. Clearly $\mathcal{O}_K \subset \mathcal{O}_L$. Recall also that $\operatorname{disc}(K)$ is the square of the determinant of an integral basis of $\mathcal{O}_K$. If $\{v_1, \ldots, v_n\}$ is an integral basis of $\mathcal{O}_K$, then we can extend it to an integral basis of $\mathcal{O}_L$ $\{v_1, \ldots, v_n, w_{n+1}, \ldots, w_m\}$. We are relying on the fact that $\mathcal{O}_L \cong \mathcal{O}_K \times \mathbb{Z}^d$ (as additive groups) for some non-negative integer d. Unlike with vector spaces, we cannot always extend a basis as we did here. The proof is done once you compute the determinant directly. □

31. March 30: Diophantine equations

Consider the equation $y^2 = x^3 - 19$. What are all the integer solutions?

Claim. There is none!

Proof. Say we found integers x, y such that $y^2 = x^3 - 19$. Then $x^3 = y^2 + 19 = (y + \sqrt{-19})(y - \sqrt{-19})$. It's not hard to see that $y + \sqrt{-19}$ and $y - \sqrt{-19}$ are relatively prime. Since $(y+\sqrt{-19})(y-\sqrt{-19})$ is a perfect cube, so are $y+\sqrt{-19}$ and $y-\sqrt{-19}$ individually. So we have $y+\sqrt{-19} = (a+b\sqrt{-19})^3$. Note that $(a+b\sqrt{-19})^3 = a^3-57ab^2+(3a^2b-19b^3)\sqrt{-19}$. Thus $3a^2b - 19b^3 = -1$ and $a^3 - 57ab^2 = y$. $b = \pm 1$ because $b \,|\, 1$. Hence $3a^2 - 19 = \pm 1$. This has no integer solutions. □

Except that this is actually *wrong*! This one does have at least one solution: $(x, y) = (7, 18)$.

Question. Find the errors, and try correcting the "solution" above.

Solution: First, $\mathbb{Z}[\sqrt{-19}]$ is not the ring of integers of $\mathbb{Q}(\sqrt{-19})$ – notice that $-19 \equiv 1 \pmod 4$. So $\mathbb{Z}[\sqrt{-19}]$ is not a PID since it is not even a Dedekind domain. Thus we *cannot* conclude that $(y + \sqrt{-19})(y - \sqrt{-19})$ being a cube does not mean that $y + \sqrt{-19}$ and

$y - \sqrt{-19}$ are cubes individually. Thus we made a mistake when we set up the equation $y + \sqrt{-19} = (a + b\sqrt{-19})^3$ with $a, b \in \mathbb{Z}$.

Now let's try to solve the correct equation, which is

$$y + \sqrt{-19} = \frac{(a + b\sqrt{-19})^3}{8},$$

with $a, b \in \mathbb{Z}$ and $a \equiv b \pmod 2$. So we have $3a^2b - 19b^3 = b(3a^2 - 19b^2) = 8$. meaning that $b = \pm 1, \pm 2, \pm 4, \pm 8$. If $b = \pm 8$, then $3a^2 - 19 \cdot 64 = \pm 1$, which has no integral solution. Similarly, if $b = \pm 4, \pm 2$, then there is no integral solution. (Alternatively, notice that if b is even then so should a meaning that $(a + b\sqrt{-19})/2 \in \mathbb{Z}[\sqrt{-19}]$ – and we know that there is no solution in $\mathbb{Z}[\sqrt{-19}]$. Thus we can jump straight to the $b = \pm 1$ case.) If $b = \pm 1$, then $3a^2 - 19 = \pm 8$. Thus $3a^2 = 27$, hence $a = \pm 3$. Thus $y = (a^3 - 57a)/8 = ((\pm 3)^3 - 57(\pm 3))/8 = (\pm 27 \mp 171)/8 = \mp 18$. So $x = 7$ as expected.

32. April 1

Every cyclotomic field $\mathbb{Q}(\zeta_n)$ contains at least one quadratic subfield $\mathbb{Q}(\sqrt{d})$. So our natural question is: which one? But this involves some Galois theory, which is not a prerequisite to this course. So we won't necessarily prove this claim. But we *can* still prove the following with the tools we have:

Proposition 32.1. *If $p \in \mathbb{Z}$ is a prime, then $p \mid \operatorname{disc}(\mathbb{Q}(\zeta_n))$ if and only if $p \mid n$.*

Proof. We employ the following characterization of discriminants:

$$\operatorname{disc}(\mathbb{Q}(\zeta_n)) = \prod_{a,b} (\zeta_n^a - \zeta_n^b)^2,$$

where a, b range over distinct pairs of distinct elements of $(\mathbb{Z}/n\mathbb{Z})^*$. The elements ζ_n^a for $a \in (\mathbb{Z}/n\mathbb{Z})^*$ are exactly the roots of $\Phi_n(x)$, the n-th cyclotomic polynomial (i.e., the minimal polynomial for ζ_n over $\mathbb{Q}$). Therefore $p \mid \operatorname{disc}(\mathbb{Q}(\zeta_n))$ if and only if $\Phi_n(x)$ has multiple factors mod p. Now, $\Phi_n(x) \mid x^n - 1$ (clearly!). If $p \nmid n$, then $\gcd(x^n - 1, nx^{n-1}) = 1$ so $\Phi_n(x) \mid x^n - 1$ has no multiple factors. Therefore $p \nmid \operatorname{disc}(\mathbb{Q}(\zeta_n))$.

If $p \mid n$, then $\mathbb{Q}(\zeta_p) \subseteq \mathbb{Q}(\zeta_n)$. It therefore suffices to show that $p \mid \operatorname{disc}(\mathbb{Q}(\zeta_p))$. But $\Phi_p(x) \mid x^p - 1 \equiv (x-1)^p \pmod p$, so $\Phi_p(x)$ has only one root mod p. Therefore $p \mid \operatorname{disc}(\mathbb{Q}(\zeta_p))$, and hence also $p \mid \operatorname{disc}(\mathbb{Q}(\zeta_n))$. □

Now let's find some quadratic subfields of $\mathbb{Q}(\zeta_n)$ for some n:

n	Quadratic subfield(s)
3	$\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$
4	$\mathbb{Q}(i) = \mathbb{Q}(\zeta_4)$
5	$\mathbb{Q}(\sqrt{5})$
6	$\mathbb{Q}(\zeta_6) = \mathbb{Q}(\zeta_3)$
7	$\mathbb{Q}(\sqrt{-7})$

In fact, if $n = p$ for some p prime, then $\mathbb{Q}(\zeta_p)$ contains $\mathbb{Q}(\sqrt{p})$ if $p \equiv 1 \pmod 4$ and $\mathbb{Q}(\sqrt{-p})$ if $p \equiv -1 \pmod 4$. More generally, by Kronecker and Weber proved that

Theorem 32.2 (Kronecker-Weber)**.** *every quadratic extension of $\mathbb{Q}$ is contained in $\mathbb{Q}(\zeta_n)$ for some n.*

So by Kronecker-Weber, there must exist some n such that $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\zeta_n)$, which we haven't found any. But since $\zeta_8 = (1+i)/\sqrt{2}$, so $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\zeta_8)$, and we can also find that $\mathbb{Q}(\sqrt{-2}) \subset \mathbb{Q}(\zeta_8)$. What about $\mathbb{Q}(\sqrt{3})$? We see that $\mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\zeta_{12})$. In general, we see that $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_{4p})$.

33. Splitting of prime ideals

Question: Given an extension L/K of number fields and a prime ideal P of $\mathcal{O}_K$, how does $P\mathcal{O}_L$ factor into prime ideals of $\mathcal{O}_L$?

Proposition 33.1. *If Q is a prime ideal of $\mathcal{O}_L$, then $Q \cap \mathcal{O}_K$ is prime also.*

Let L/K be an extension of number fields, so $\mathcal{O}_K \subseteq \mathcal{O}_L$. Let P be a prime ideal of $\mathcal{O}_L$. Then $Q = P \cap \mathcal{O}_K$ is also a prime ideal of $\mathcal{O}_K$. In this case, we say that P *lies over* Q. Thus $Q\mathcal{O}_L$ is an ideal of $\mathcal{O}_L$ and $Q\mathcal{O}_L \subseteq P$, so

$$Q\mathcal{O}_L = P^a \prod_{i=1}^{r} P_i^{a_i}$$

where $P_i \neq P$ for any i.

Definition 33.2. We define $e(P/Q) = a$ and $f(P/Q) = [\mathcal{O}_L/P : \mathcal{O}_K/Q]$. We also call $e(P/Q)$ the *ramification index* of P over Q, and $f(P/Q)$ the *inertia degree* of P over Q.

Example 33.3. Let $K = \mathbb{Q}, L = \mathbb{Q}(i), Q = (2), P = (1+i)$. Note that $Q\mathcal{O}_L = P^2$, so $e(P/Q) = 2$. On the other hand, $\mathcal{O}_L/P = \mathbb{Z}[i]/(1+i) \cong \mathbb{F}_2$. Clearly, $\mathcal{O}_K/Q = \mathbb{Z}/2\mathbb{Z} \cong \mathbb{F}_2$. Thus $f(P/Q) = 1$.

Example 33.4. Let K and L be the same fields. Let $Q = 3\mathbb{Z}$ and $P = 3\mathbb{Z}[i]$. Then $e(P/Q) = 1$ and $f(P/Q) = [\mathbb{Z}[i]/P : \mathbb{Z}/3\mathbb{Z}] = 2$.

Example 33.5. Same K and L, and this time let $Q = (5)$ and $P = (2+i)$. Then $e(P/Q) = 1$ and $f(P/Q) = 1$, since $\#(\mathbb{Z}[i]/(2+i)) = 5$.

Say $K \subseteq L \subseteq M$ are number fields. Suppose that $P \subset \mathcal{O}_M$ is prime, and let $Q = P \cap \mathcal{O}_L, R = P \cap \mathcal{O}_K = Q \cap \mathcal{O}_K$. Then we have $e(P/R) = e(P/Q)e(Q/R)$ and $f(P/R) = f(P/Q)f(Q/R)$ because $[\mathcal{O}_M/P : \mathcal{O}_K/R] = [\mathcal{O}_M/P : \mathcal{O}_L/Q][\mathcal{O}_L/Q : \mathcal{O}_K/R]$.

Theorem 33.6. *Let L/K be number fields, $Q \subset \mathcal{O}_K$ a non-zero prime ideal. Factor $Q\mathcal{O}_L = P_1^{e_1} \dots P_r^{e_r}$. Then*

$$\sum_{i=1}^{r} e(P_i/Q) f(P_i/Q) = [L : K].$$

Proof. We will prove the case when $K = \mathbb{Q}$. take the norm of $Q\mathcal{O}_L$:

$$\mathrm{N}(Q\mathcal{O}_L) = \prod_{i=1}^{r} \mathrm{N}(P_i)^{e_i}.$$

Then $\mathrm{N}(Q\mathcal{O}_L) = \#(\mathcal{O}_L/Q\mathcal{O}_L)$. Also, per the Chinese remainder theorem, we have

$$\mathcal{O}_L/Q\mathcal{O}_L \cong \mathcal{O}_L/P_1^{e_1} \times \cdots \times \mathcal{O}_L/P_r^{e_r}$$

where $e_i = e(P_i/Q)$. Further,

$$\#(\mathcal{O}_L/Q\mathcal{O}_L) = \#(\mathcal{O}_K/Q)^{[L:K]} = q^{[L:K]}$$
$$\#(\mathcal{O}_L/P_i^{e_i}) = \mathrm{N}(P_i)^{e_i} = (q^{f(P_i/Q)})^{e(P_i/Q)}.$$

Thus, $q^{[L:K]} = q^{\sum e(P_i/Q)f(P_i/Q)}$. The conclusion follows. □

Definition 33.7. Let L/K be number fields, and $a \in L$. Consider a K-linear transformation $T_a : L \to L$ which we define $T(x) = ax$. The *trace* of L over K is $\mathrm{tr}_{L/K}(a) = \mathrm{trace}(T_a) = \sum f_i(a)$. The *norm* of L over K is $\mathrm{N}_{L/K}(a) = \det(T_a) = \prod f_i(a)$, where $f_1, \ldots, f_r : L \to \overline{K}$ are the embedding of L into $\overline{K}$, the algebraic closure of K.

That is, fix an embedding $K \overset{\phi}{\hookrightarrow} \mathbb{C}$ and let $f_1, \ldots, f_r$ be the embeddings of $L \hookrightarrow \mathbb{C}$ such that $f_i|_K = \phi$.

Example 33.8. Let $K = \mathbb{Q}(\sqrt{2}), L = \mathbb{Q}(\sqrt{2}, \sqrt{5})$, and $a = \sqrt{2} + \sqrt{5}$. Then $\mathrm{tr}_{L/K}(a) = (\sqrt{2}+\sqrt{5}) + (\sqrt{2}-\sqrt{5}) = 2\sqrt{2}$ and $\mathrm{N}_{L/K}(a) = (\sqrt{2}+\sqrt{5})(\sqrt{2}-\sqrt{5}) = -3$. Or, choose basis of L/K: $\{1, \sqrt{5}\}$. Then

$$T_a(1) = \sqrt{2} + \sqrt{5} \longleftrightarrow (\sqrt{2}, 1)$$
$$T_a(\sqrt{5}) = \sqrt{2} \cdot \sqrt{5} + 5 \longleftrightarrow (5, \sqrt{2}).$$

Thus

$$[T_a] = \begin{pmatrix} \sqrt{2} & 5 \\ 1 & \sqrt{2} \end{pmatrix}.$$

Thus, the determinant is -3 and trace is $2\sqrt{2}$ as expected.

Proposition 33.9. *Let $K \subset L \subset M$ be tower of fields. Then*

$$\mathrm{N}_{L/K}(\mathrm{N}_{M/L}(a)) = \mathrm{N}_{M/K}(a)$$
$$\mathrm{tr}_{L/K}(\mathrm{tr}_{M/L}(a)) = \mathrm{tr}_{M/K}(a).$$

Also, $\mathrm{N}_{L/K}(a)$ and $\mathrm{tr}_{L/K}(a)$ lie in K. Furthermore, if $a \in \mathcal{O}_L$, then $\mathrm{N}_{L/K}(a)$ and $\mathrm{tr}_{L/K}(a)$ lie in $\mathcal{O}_K$.

Remark 33.1. The converse is *false*. Also, note that $\mathrm{N}_{L/K}(a)$ and $\mathrm{tr}_{L/K}(a)$ are, up to sign, coefficients in the monic minimal polynomial of a over K, raised to the power $[L : K(a)]$.

We also want to define $\mathrm{N}_{L/K}(I)$ for an ideal $I \subset \mathcal{O}_L$. If $I = P_1^{a_1} \cdots P_r^{a_r}$ for prime ideals $P_i \subset \mathcal{O}_L$ and if $K = \mathbb{Q}$, then $\mathrm{N}_{L/K}(I) = (p_1)^{a_i f(P_1/(p_1))} \cdots (p_r)^{a_r f(P_r/(p_r))}$. So we define

$$\mathrm{N}_{L/K}(I) = Q_i^{a_1 f(P_1/Q_1)} \cdots Q_r^{a_r f(P_r/Q_r)},$$

where $Q_i = P_i \cap \mathcal{O}_K$.

Example 33.10. Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $K = \mathbb{Q}(\sqrt{2})$. Then we have $\mathcal{O}_L = \mathbb{Z}\left[\sqrt{2}, \frac{\sqrt{2}+\sqrt{6}}{2}\right]$, and $\mathrm{disc}(L) = 2^8 \cdot 3^2$. Factor $(2), (3), (5)$ in $\mathcal{O}_L$, and compute all the relevant ramification indices and inertia degrees that arise. Compute the norm and trace of $\frac{\sqrt{6}+\sqrt{2}}{2}$.

Solution: Note that $(2) = (\sqrt{(2)})^2$. Write $\alpha := \frac{\sqrt{2}+\sqrt{6}}{2}$. Also, we have

$$\mathcal{O}_L/(\sqrt{2}) \cong \mathbb{Z}[\sqrt{2}][x]/(x^2 - \sqrt{2}x - 1, \sqrt{2}) \cong (\mathbb{Z}/2\mathbb{Z})[x]/(x-1)^2.$$

Therefore, $(\sqrt{2}) = (\alpha - 1, \sqrt{2})^2 = P^2$, so $(2) = (\alpha - 1, \sqrt{2})^4$. Therefore $e(P/(2)) = 4$ and $f(P/(2)) = 1$. Similarly, we see that (3) is prime in $\mathcal{O}_K$. Thus

$$\begin{aligned}\mathcal{O}_L/(3) &\cong \mathbb{Z}[\sqrt{2}][x]/(x^2 - \sqrt{2}x - 1, 3) \cong [\mathbb{Z}[\sqrt{2}]/(3)][x]/(x^2 - \sqrt{2}x - 1) \\ &\cong [\mathbb{Z}[\sqrt{2}]/(3)][x]/(x - \sqrt{2}/2)^2 \cong [\mathbb{Z}[\sqrt{2}]/(3)][x]/(x + \sqrt{2})^2.\end{aligned}$$

Hence, $3\mathcal{O}_L = (\alpha + \sqrt{2}, 3)^2$ and $e(P/(3)) = f(P/(3)) = 2$. (5) is also prime in $\mathcal{O}_K$, and

$$\begin{aligned}\mathcal{O}_L/(5) &\cong \mathbb{Z}[\sqrt{2}][x]/(x^2 - \sqrt{2}x - 1, 5) \cong [\mathbb{Z}[\sqrt{2}]/(5)][x]/(x^2 - \sqrt{2}x - 1) \\ &\cong [\mathbb{Z}[\sqrt{2}]/(5)][x]/(x - 3\sqrt{2} - 3)(x - 3\sqrt{2} + 3)).\end{aligned}$$

So $(5) = (\alpha - 3\sqrt{2} + 3, 5) \cdot (\alpha - 3\sqrt{2} + 3, 5)$. The ramification index of the both ideal arising from the factorization is 1. Since the extension is Galois, we see that the inertia degree of both ideals must be the same, which we shall prove in the next section. Thus, the inertia degrees of the two ideals must be 2.

34. Different and codifferent

Theorem 34.1. *Let L/K be* Galois*, and let $\mathcal{O}_K, \mathcal{O}_L$ be rings of integers. Say $P \subset \mathcal{O}_K$ is prime, and that $P\mathcal{O}_L = Q_1^{e_1} \cdots Q_g^{e_g}$. Then $e_i = e_j$ for all i, j.*

Remark 34.1. As noted in the emphasis on the word "Galois", the theorem is *not necessarily true* if L/K is not Galois. As an example, consider $L = \mathbb{Q}(\sqrt[3]{2}), K = \mathbb{Q}, P = (5)$. Then $\mathcal{O}_L$ contains $\mathbb{Z}[\sqrt[3]{2}]$ as a subring of finite index, and $5 \nmid \operatorname{disc}(\mathbb{Z}[\sqrt[3]{2}])$. Thus, we have $(\mathbb{Z}[\sqrt[3]{2}])_{(Q \cap \mathbb{Z}[\sqrt[3]{2}])} = (\mathcal{O}_L)_Q$ and $\mathbb{Z}[\sqrt[3]{2}]/(Q \cap \mathbb{Z}[\sqrt[3]{2}]) \cong \mathcal{O}_L/Q$ for any Q containing 5. Then we have

$$\mathbb{Z}[\sqrt[3]{2}]/(5) \cong \mathbb{Z}[x]/(x^3 - 2, 5) \cong (\mathbb{Z}/5\mathbb{Z})[x]/(x^3 - 2) \cong (\mathbb{Z}/5\mathbb{Z})[x]/(x+2)(x^2 - 2x - 1).$$

Therefore, $(5) = (\sqrt[3]{2} + 2, 5)(\sqrt[3]{4} - 2\sqrt[3]{2} - 1, 5)$. So $(\sqrt[3]{2} + 2, 5)$ has inertia degree 1 while $(\sqrt[3]{4} - 2\sqrt[3]{2} - 1, 5)$ has inertia degree 2.

Proof. The claim follows from the fact that if $Q_i \cap \mathcal{O}_K = Q_j \cap \mathcal{O}_K$ for prime ideals $Q_i, Q_j \in \mathcal{O}_L, i \neq j$, then there is some element $\sigma \in \operatorname{Gal}(L/K)$ satisfying $\sigma(Q_i) = Q_j$. For any i, choose $\alpha \in Q$ such that $\alpha \equiv 1 \pmod{Q_j}$ for all $j \neq i$. Then $\mathrm{N}_{L/K}(\alpha) \in P \subset \mathcal{O}_K$ but $\mathrm{N}_{L/K}(\alpha) = \prod_{\sigma \in \operatorname{Gal}(L/K)} \sigma(\alpha) \in Q_j$ for all j because $P \subset Q - j$ for all j. So for each j, there is some $\sigma_j \in \operatorname{Gal}(L/K)$ with $\sigma_j(\alpha) \in Q_j$. But $\sigma_j(\alpha) \equiv 1 \pmod{Q_k}$ for all other k. Therefore $\sigma_j(\alpha) \notin Q_k$ for $k \neq j$. Therefore $\sigma_j(Q_i) = Q_j$, as required. □

Given $\sigma \in \operatorname{Gal}(L/K)$, can we "reduce σ mod P" for some prime ideal $P \subset \mathcal{O}_L$? The answer is *no*. To see this, let $L = \mathbb{Q}(\sqrt{2}$ and $K = \mathbb{Q}$. Let $P = (7, \sqrt{2} - 3)$. Then

$$\begin{aligned}\mathcal{O}_L/P &\cong \mathbb{Z}[\sqrt{2}]/(7, \sqrt{2} - 3) \cong \mathbb{Z}[x]/(x^2 - 2, x - 3, 7) \\ &\cong (\mathbb{Z}/7\mathbb{Z})[x]/(x^2 - 2, x - 3) = (\mathbb{Z}/7\mathbb{Z})[x]/(x - 3) \cong \mathbb{Z}/7\mathbb{Z},\end{aligned}$$

since $x^2 - 2 = (x-3)(x+3)$.

$$\begin{array}{ccc} \mathcal{O}_L & \xrightarrow{\sigma} & \mathcal{O}_L \\ \downarrow q & \searrow^{q\circ\sigma} & \downarrow q \\ \mathcal{O}_L/P & \xrightarrow{\bar{\sigma}} & \mathcal{O}_L/P \end{array}$$

Thus if $P \not\subset \ker(q\circ\sigma)$, then $\bar{\sigma}$ does not exist. However, $\ker(q\circ\sigma) = \sigma^{-1}(P)$ so $\bar{\sigma}$ exists if and only if $P = \sigma(P)$. So $\bar{\sigma} \in \mathrm{Gal}((\mathcal{O}_L/P)/(\mathcal{O}_K/(P\cap K)))$ exists if and only if $\sigma(P) = P$.

Definition 34.2. For fixed P, the set

$$D_P = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(P) = P\}$$

is a subgroup, called the *decomposition group* of P.

So there is a homomorphism

$$\phi_P : D_P \to \mathrm{Gal}((\mathcal{O}_L/P)/(\mathcal{O}_K/(P\cap K))).$$

This homomorphism need not be injective, and this prompts us to introduce a new group.

Definition 34.3. Let $I_P = \ker(\phi_P) = \{\sigma \in D_P : \sigma = 1 \text{ in } \mathrm{Gal}((\mathcal{O}_L/P)/(\mathcal{O}_K/(P\cap K)))\}$. Then I_P is called the *inertia group* of P.

Question. Write $\alpha = \frac{\sqrt{6}+\sqrt{2}}{2}$. Let $L = \mathbb{Q}(\sqrt{2},\sqrt{3}), \mathcal{O}_L = \mathbb{Z}\left[\sqrt{2},\alpha\right], K = \mathbb{Q}, \mathcal{O}_K = \mathbb{Z}$. Let $P_2 = (\alpha+1,\sqrt{2}), P_3 = (\alpha+\sqrt{2},3), P_5 = (\alpha - 3\sqrt{2}+3,5)$. Find D_P and I_P for all three ideals.

Solution: Note $(2) = P_2^4$, so $D_{P_2} = \mathrm{Gal}(L/\mathbb{Q})$; similarly, $(3) = P_3^2$ so $D_{P_3} = \mathrm{Gal}(L/\mathbb{Q})$. On the other hand, recall that (5) splits, i.e., $(5) = P_5\bar{P}_5$, where $P_5 = (\alpha - 3\sqrt{2} - 3, 5)$ and $\bar{P}_5 = (\alpha - 3\sqrt{2}+3,5)$. Consider the four conjugates: $(\alpha - 3\sqrt{2}-3,5), (-\alpha+3\sqrt{2}-3,5), ((-\sqrt{6}+\sqrt{2})/2 - 3\sqrt{2}-3,5), ((\sqrt{6}-\sqrt{2})/2+3\sqrt{2}-3,5)$. Note that the first two are P_5 and $\bar{P}_5$, respectively. The third conjugate is also $\bar{P}_5$. Thus the fourth one is P_5. Hence $D_{P_5} = \{1,\sigma\}$ where $\sigma(\sqrt{6}) = \sqrt{6}$ and $\sigma(\sqrt{2}) = -\sqrt{2}$. On the other hand, $\sigma \not\equiv 1 \pmod{P_5}$ since $\sqrt{2} \mapsto -\sqrt{2}$; thus $I_{P_5} = \{1\}$. As for P_3, note that $I_{P_3} = \{1,\tau\}$ where τ maps $\sqrt{2}$ to $\sqrt{2}$ and $\sqrt{3}$ to $-\sqrt{3}$. (Clearly, I_{P_3} must have two elements since $\mathcal{O}_L/P_3$ is a degree-two extension over $\mathbb{Z}/3\mathbb{Z}$. Finally, note that $\mathcal{O}_L/P_2$ is a degree-one extension over $\mathbb{Z}/2\mathbb{Z}$. Hence $I_{P_2} = D_{P_2}$.

Definition 34.4. Let L/K be an extension of number fields, $I \subset \mathcal{O}_L$ an ideal. Then the *codifferent* of I over K is

$$I^* := \{x \in L : \mathrm{tr}_{L/K}(xI) \subset \mathcal{O}_K\}.$$

This turns out to be a fractional ideal of L. The *codifferent* of L/K is the codifferent of $\mathcal{O}_L$ over K. The *different* is the inverse (in the class group sense) of a codifferent, i.e., $(I^*)^{-1}$.

Example 34.5. Codifferent of (1) in $\mathbb{Z}[\sqrt{2}]$ over $\mathbb{Q}$ is the codifferent of $\mathbb{Q}(\sqrt{2})$. So we need $\mathrm{tr}(a+b\sqrt{2}) \in \mathbb{Z}$, i.e., $2a \in \mathbb{Z}$. We also need that $\mathrm{tr}((a+b\sqrt{2})\sqrt{2}) \in \mathbb{Z} \Leftrightarrow \mathrm{tr}(2b+a\sqrt{2}) \in \mathbb{Z} \Leftrightarrow 4b \in \mathbb{Z}$. Hence

$$(1)^* = \left\{\frac{k}{2} + \frac{l\sqrt{2}}{4} : k,l \in \mathbb{Z}\right\} = \left(\frac{\sqrt{2}}{4}\right).$$

Proposition 34.6. $II^* = \mathcal{O}_L^*$.

Proposition 34.7. *If $I \subset \mathcal{O}_L$, then $(I^*)^{-1} \subset \mathcal{O}_L$.*

Proposition 34.8. *If $I \subset J$, then $J^* \subset I^*$.*

Definition 34.9. The different of $\mathcal{O}_L$ over K is written $\mathcal{D}_{L/K}$.

Proposition 34.10. *$\mathcal{D}_{M/K} = \mathcal{D}_{M/L}\mathcal{D}_{L/K}$. If L/K is Galois, then for all $\sigma \in \mathrm{Gal}(L/K)$ we have $\sigma(\mathcal{D}_{L/K}) = \mathcal{D}_{L/K}$.*

Definition 34.11. The *discriminant* of L/K is $\Delta_{L/K} = \mathrm{N}_{L/K}(\mathcal{D}_{L/K})$.

Theorem 34.12. $\mathrm{disc}(\mathcal{O}_K) = \Delta_{K/\mathbb{Q}}$.

Proof. We will show that $(\mathrm{disc}\,\mathcal{O}_K)^2$ generates $\Delta_{K/\mathbb{Q}}^2$ for any ideal $I \subset \mathcal{O}_K$ we have $I = a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$ for some $a_1, \ldots, a_n \in \mathcal{O}_K$. The ideal I^* is $I^* = a_1^*\mathbb{Z} + \cdots + a_n^*\mathbb{Z}$ where $a_i^* \in K$ satisfies $\mathrm{tr}(a_i a_j^*) = \delta_{ij}$ (δ_{ij} is the Kronecker delta). So $\mathcal{O}_K^* = a_1^*\mathbb{Z} + \cdots + a_n^*\mathbb{Z}$ where $\mathcal{O}_K = a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$. There is some non-zero $m \in \mathbb{Z}$ with $m\mathcal{O}_K^* \subset \mathcal{O}_K$. Define $I := m\mathcal{O}_K^*$. So $\mathrm{N}_{K/\mathbb{Q}}(\mathcal{D}_{K/\mathbb{Q}})^2$ is the generator of this ideal. Since $(\mathcal{O}_K^*)^{-1} = \mathcal{D}_{K/\mathbb{Q}}$, it follows that

$$\begin{aligned}\mathrm{N}_{K/\mathbb{Q}}(\mathcal{D}_{K/\mathbb{Q}})^2 &= \frac{1}{\mathrm{N}_{K/\mathbb{Q}}(\mathcal{O}_K^*)^2} = \frac{m^{2n}}{\mathrm{N}_{K/\mathbb{Q}}(I)^2} \\ &= \frac{m^{2n}\,\mathrm{disc}(a_1, \ldots, a_n)}{\mathrm{disc}(ma_1^*, \ldots, ma_n^*)} = \frac{\mathrm{disc}(a_1, \ldots, a_n)}{\mathrm{disc}(a_1^*, \ldots, a_n^*)}.\end{aligned}$$

Now we shall prove that $\mathrm{disc}(a_1^*, \ldots, a_n^*) = \mathrm{disc}(a_1, \ldots, a_n)^{-1}$. Indeed, we have that the (ij)-th entry of the product of the two matrices

$$\begin{pmatrix} f_1(a_1) & \cdots & f_n(a_1) \\ \vdots & \ddots & \vdots \\ f_n(a_1) & \cdots & f_n(a_n) \end{pmatrix} \text{ and } \begin{pmatrix} f_1(a_1^*) & \cdots & f_n(a_1^*) \\ \vdots & \ddots & \vdots \\ f_n(a_1^*) & \cdots & f_n(a_n^*) \end{pmatrix}$$

is equal to $f_1(a_i)f_1(a_j^*) + \cdots + f_n(a_i)f_n(a_j^*) = \mathrm{tr}_{K/\mathbb{Q}}(a_i a_j^*) = \delta_{ij}$. Hence, the claim follows. □

Proposition 34.13. $\Delta_{M/K} = \Delta_{L/K}^{[M:L]} \cdot \mathrm{N}_{L/K}(\Delta_{M/L})$.

Theorem 34.14. *Say $P \subset \mathcal{O}_L$ is a prime ideal and $Q = P \cap \mathcal{O}_K$ and $e = e(P/Q)$. Then $P^{e-1} \,|\, \mathcal{D}_{L/K}$ and if $\gcd(e, \mathrm{N}_{L/\mathbb{Q}}(P)) = 1$, then $P^{e-1} \,\|\, \mathcal{D}_{L/K}$.*

Theorem 34.15. *Let $n \in \mathbb{Z}$ and $\mathcal{S}$ a finite set of prime ideals of $\mathcal{O}_K$. The set of extensions L/K with $[L : K] \leq n$ and L ramified only over prime ideals in $\mathcal{S}$ is finite.*

Theorem 34.16 (Hermite)**.** *Let $n \in \mathbb{Z}$. There are finitely many number fields with discriminant at most n.*

Question. $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}), K = \mathbb{Q}(\sqrt{2})$. Compute $\Delta_{L/K}$.

Solution: First, we compute $\mathcal{O}_L^*$ over K. Write $x = a + b\alpha$ where $\alpha := (\sqrt{6} + \sqrt{2})/2$.

$$\mathrm{tr}(x1) = \mathrm{tr}(a + b\alpha) = 2a + \sqrt{2}b$$

$$\mathrm{tr}(x\alpha) = \mathrm{tr}(a\alpha + b\alpha^2) = \mathrm{tr}(a\alpha + \sqrt{2}\alpha b + b) = 2b + 2b + \sqrt{2}a = 4b + \sqrt{2}a.$$

Therefore,

$$\mathcal{O}_L^* = \left(-\frac{\sqrt{2}}{6} + \frac{\alpha}{3}\right)\mathcal{O}_K + \left(\frac{2}{3} - \frac{\sqrt{2}\alpha}{6}\right)\mathcal{O}_K = \frac{1}{\sqrt{6}}\mathcal{O}_L.$$

Note that this works since we are working with PID's. To see why $\mathcal{O}_L^* = \frac{1}{\sqrt{6}}\mathcal{O}_L$ (which is not an obvious claim), note first that

35. Galois theory of finite fields

Recall that $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$. If $[K : \mathbb{F}_p] = d$, then K is the finite field of p^d elements. Then K^* has $p^d - 1$ elements and is a group; hence, K is the splitting field of $x^{p^d} - x$. This means that *every* extension of finite fields is Galois. Up to isomorphism, there is exactly one field with p^d elements if p is prime and $d \geq 1$. Also, note that $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^c}$ if and only if $d \,|\, c$.

Let $K \subset L \subset M$ be a field extension of finite degree, and suppose that M/K is Galois. Then M/L is Galois. In fact, $\mathrm{Gal}(M/L) = \{\sigma \in \mathrm{Gal}(M/K) : \sigma(\alpha) = \alpha \text{ for all } \alpha \in L\}$. So what is $\mathrm{Gal}(\mathbb{F}_{p^k}/\mathbb{F}_p)$? There is a natural automorphism (Frobenius automorphism) of $\mathbb{F}_{p^k}$ given by $\mathrm{Frob}_p = \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$ given by $\mathrm{Frob}_p(\alpha) = \alpha^p$. Fermat's little theorem implies that Frob_p fixes $\mathbb{F}_p$ pointwise. Is it true that $\mathrm{Gal}(\mathbb{F}_{p^k}/\mathbb{F}_p) = \langle \mathrm{Frob}_p \rangle$? Yes indeed. Note that $\#(\mathrm{Gal}(\mathbb{F}_{p^k}/\mathbb{F}_p)) = k$ while $\#\langle \mathrm{Frob}_p \rangle$ is equal to the order of Frob_p. Note that $(\mathrm{Frob}_p)^2(\alpha) = (\alpha^p)^p = \alpha^{p^2}$; via induction we have $(\mathrm{Frob}_p)^n(\alpha) = \alpha^{p^n}$. This is trivial on $\mathbb{F}_{p^k}$ if and only if $\alpha = \alpha^{p^n}$ for all $\alpha \in \mathbb{F}_{p^k}$. Therefore, the order of Frob_p divides k. the fixed field of $(\mathrm{Frob}_p)^n$ is the splitting field of $x^{p^n} - x$, namely $\mathbb{F}_{p^n}$. So Frob_p has order k as an automorphism of $\mathbb{F}_{p^k}$, as required. Hence, $\mathrm{Gal}(\mathbb{F}_{p^k}/\mathbb{F}_p)$ is cyclic, making any finite extension over finite fields a cyclic extension. Clearly, any subgroup of a cyclic group is also cyclic, which implies that $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})$ is cyclic also. Particularly, $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})$ is generated by $(\mathrm{Frob}_p)^m$.

Question. Let $a \in \mathbb{F}_{5^3} = \mathbb{F}_5(a)$ be a root of $x^3 + 3x + 7$. Find the other two roots in the form of $x + ya + za^2$ for $x, y, z \in \mathbb{F}_5 = \{0, 1, 2, 3, 4\}$.

Solution: Note $(\mathrm{Frob}_5)^3$ is the identity map, so the roots are $a, \mathrm{Frob}_5(a) = a^5, (\mathrm{Frob}_5)^2(a) = a^{25}$. Now we express these as a linear combination of $1, a, a^2$. Note that $a^5 = a^2(a^3) = a^2(-3a - 7) = (2a - 2)a^2 = 2a^3 - 2a^2 = 2(-3a - 7) - 2a^2 = -6a - 14 - 2a^2 = 1 + 4a + 3a^2$. As for a^{25}, we have

$$\begin{aligned}
a^{25} &= (3a^2 + 4a + 1)^5 = 3^5a^{10} + 4^5a^5 + 1 = 3a^{10} + 4a^5 + 1 \\
&= 3(a^5)^2 + 4a^5 + 1 = 3(3a^2 + 4a + 1)^2 + 4a^5 + 1 \\
&= 3(4a^4 + 4a^3 + 2a^2 + 3a + 1) + 4(1 + 4a + 3a^2) + 1 \\
&= 12a^4 + 12a^3 + 8a^2 + 8 = 2a^4 + 2a^3 + 3a^2 + 3 \\
&= 2a^3(a + 1) + 3a^2 + 3 = 2(-3a - 7)(a + 1) + 3a^2 + 3 \\
&= 2(2a + 3)(a + 1) + 3a^2 + 3 = 2(2a^2 + 3) + 3a^2 + 3 = 2a^2 + 4.
\end{aligned}$$

Thus the two other roots are $1 + 4a + 3a^2$ and $4 + 2a^2$.

36. Return to decomposition groups and inertia groups

Let L/K be Galois, and $P \subset \mathcal{O}_K$ and $Q \subset \mathcal{O}_L$ prime ideals. Recall that $D_P = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(P) = P\}$ and $I_P = \{\sigma \in D_p : \sigma \equiv \mathrm{id} \bmod P\}$.

Definition 36.1. Let L/K be a Galois extension of number fields and $P \subset \mathcal{O}_L$ a prime ideal lying over $Q \subset \mathcal{O}_K$. The *decomposition field* of P over K is Z_P, the fixed field of D_P. The *inertia field* of P over K is F_P, the fixed field of I_P.

If P_1 and P_2 both lie over Q, then D_{P_1} and D_{P_2} are conjugate, so Z_{P_1} and Z_{P_2} are isomorphic.

Theorem 36.2. *Let L/K be a Galois extension of number fields, $P \subset \mathcal{O}_L$ prime and $Q = P \cap \mathcal{O}_K$. Let Z_P be the decomposition field of P. Write $P_Z = P \cap \mathcal{O}_Z$. Then:*

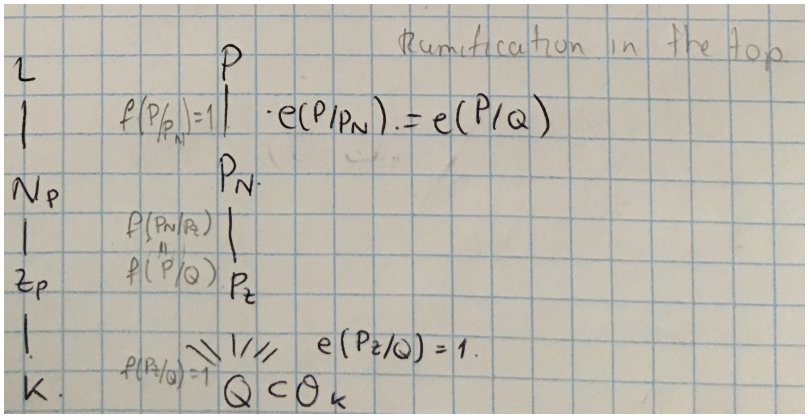
(1) P is the only *prime ideal of $\mathcal{O}_L$ lying over P_Z.*
(2) $[L : Z] = \#D_P = e(P/Q)f(P/Q)$.
(3) $e(P_Z/Q) = f(P_Z/Q) = 1$.

Proof. For the first claim, note that $\mathrm{Gal}(L/Z) = D_P$. So $\mathrm{Gal}(L/Z)$ fixes P, and acts transitively on the primes lying over P_Z, as desired. The second claim is slightly trickier to prove than the first one, but this is still not too bad. Since L/K is Galois, we have that $[L : K] = e(P/Q)f(P/Q)n$, where n is the index of D_P in $\mathrm{Gal}(L/K)$. Therefore $[L : K] = e(P/Q)f(P/Q)[L : K]/\#D_P$, from which it follows $\#D_P = e(P/Q)f(P/Q)$. The third claim is immediate from the second one and the fact that L/K is Galois. Since $[L : Z] = e(P/P_Z)f(P/P_Z)$, we have $[L : K] = e(P/P_Z)f(P/P_Z)[Z : K]$. But then $[L : K] = e(P/Q)f(P/Q)[Z : K]$, so $e(P/P_Z)f(P/P_Z) = e(P/Q)f(P/Q)$. $e(P/P_Z)$ is a multiple of $e(P/Q)$ but they are the same, so the claim follows. □

Definition 36.3. The *inertia field* N_P of $P \subset \mathcal{O}_L$ over K is the fixed field of the inertia group I_P.

Recall that I_P is a normal subgroup of D_P, so N_P is a Galois extension of the decomposition field Z_P.

Proposition 36.4. $\mathrm{Gal}(N_P/Z_P) \cong \mathrm{Gal}(l/k)$ *where $l = \mathcal{O}_L/P$ and $k = \mathcal{O}_K/Q$ where $Q := P \cap \mathcal{O}_K$. Furthermore, we have $\mathrm{Gal}(L/N_P) = I_P$. If $P_N := P \cap \mathcal{O}_{N_P}$ and $P_Z := P \cap \mathcal{O}_{Z_P}$. Therefore, $e(P/P_N) = e(P/Q), f(P/P_N) = 1, e(P_N/P_Z) = 1$, and $f(P_N/P_Z) = f(P/Q)$.*



Department of Pure Mathematics, University of Waterloo, 200 University Avenue West, Waterloo, ON, Canada N2L 3G1
E-mail address: hsyang@uwaterloo.ca