PMATH 441 Notes

Spring 2024

Based on Professor David McKinnon's Lectures

Contents

Lecture 1, 2024/05/06

1 Algebraic Integers

1.1 Introduction

Definition. A **number field** is a finite extension of $\mathbb{Q}$.

What are integers in a number field? That is, which algebraic numbers are like 'integers' in $\mathbb{Q}$? The only thing we know about an algebraic number is its minimal polynomial.

Let $a/b \in \mathbb{Q}$ be a rational number, its monic minimal polynomial is $x - a/b \in \mathbb{Q}[x]$. Note that $a/b \in \mathbb{Q}$ is an integer if and only if $x - a/b$ has integer coefficients. So, this might be the answer.

Definition. An **algebraic integer** α is an algebraic number over $\mathbb{Q}$ whose monic minimal polynomial over $\mathbb{Q}$ has its coefficients in $\mathbb{Z}$.

Notation. In this notes, every ring is a commutative ring with 1.

Definition. Let R be a ring and T be a ring such that $R \subseteq T$. Then $\alpha \in T$ is **integral** over R if $p(\alpha) = 0$ for some monic $p(x) \in R[x]$.

Theorem 1.1. Let α is an algebraic number over $\mathbb{Q}$ satisfying $p(\alpha) = 0$ for some monic $p(x) \in \mathbb{Z}[x]$, then α is an algebraic integer.

Proof: Let $p(x) \in \mathbb{Z}[x]$ be monic with $p(\alpha) = 0$, and let $m(x)$ be the monic minimal polynomial of α over $\mathbb{Q}$. Then $p(x) = q(x)m(x)$ for some $q(x) \in \mathbb{Q}[x]$. Write:

$$M(x) = bm(x) \quad \text{and} \quad Q(x) = aq(x)$$

where $a \in \mathbb{Z}$ is the lcm of all denominators of coefficients in $q(x)$, same for b. By this clearing of denominators, we have $M(x) \in \mathbb{Z}[x]$ and $Q(x) \in \mathbb{Z}[x]$. And in fact, $M(x)$ and $Q(x)$ are primitive. Then we have:

$$dp(x) = Q(x)M(x)$$

where $d := ab$. By Gauss' Lemma, $dp(x)$ is a primitive polynomial, this means $d = 1$. Therefore both QM is monic, so M is monic. Hence the monic polynomial of α over $\mathbb{Q}$ is M. □

Example. The ring of integers of $\mathbb{Q}$ are $\mathbb{Z}$.

Example. $\sqrt{2}$ is an algebraic integer by $m(x) = x^2 - 2$.

Example. The cube root of unity $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$ is an algebraic integer as it is a root of $x^2 + x + 1$.

Example. What are the algebraic integers of $\mathbb{Q}(\sqrt{2})$? Say $\alpha = a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$ is an algebraic integer, then its minimal polynomial is:

$$(x - a - b\sqrt{2})(x - a + b\sqrt{2}) = x^2 - 2ax + (a^2 - 2b^2) \in \mathbb{Z}[x]$$

It means $-2a \in \mathbb{Z}$ and $a^2 - 2b^2 \in \mathbb{Z}$. It turns out that $a, b \in \mathbb{Z}$. So the algebraic integer of $\mathbb{Q}(\sqrt{2})$ are exactly $\mathbb{Z}[\sqrt{2}]$, which is a ring.

1.2 Modules

Definition. Let R be a ring. An R-**module** is a set M with two operations $+ : M \times M \to M$ (addition) and $\cdot : R \times M \to M$ (scalar multiplication) satisfying:

(1) M is an abelian group under $+$.

(2) For all $m \in M$, we have $1 \cdot m = m$.

(3) For all $m_1, m_2 \in M$ and $r \in R$ we have $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$.

(4) For all $m \in M$ and $r_1, r_2 \in R$ we have $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$

(5) For all $m \in M$ and $r_1, r_2 \in R$ we have $(r_1 r_2) \cdot m = r_1(r_2 \cdot m)$.

Example. If R is a field, then M is a R-vector space.

Example. A $\mathbb{Z}$-module is exactly an abelian group.

Example. Let $I \subseteq R$ be an ideal, then I is an R-module. In fact, an ideal of R is exactly an R-submodule of R.

Example. If $R \subseteq T$ are rings, then T is an R-module.

Example. If $\phi : R \to T$ is a ring homomorphism, then T is an R-module by:

$$r \cdot \alpha := \phi(r) \cdot \alpha$$

for $r \in R$ and $\alpha \in T$.

Lecture 2, 2024/05/08

Definition. Let M, N be R-modules. An R-**module homomorphism** is a function $f : M \to N$ such that:

(1) For all $m_1, m_2 \in M$, we have $f(m_1 + m_2) = f(m_1) + f(m_2)$.

(2) For all $r \in R$ and $m \in M$ we have $f(rm) = rf(m)$.

Example. If R is a field, then an R-module homomorphism is a linear transformation.

Example. Let $M = \mathbb{Z}[i]$ and $N = \mathbb{Z}[i]$. Define $f : M \to N$ by:

$$f(a+bi) = a - bi$$

then f is a $\mathbb{Z}$-module homomorphism. But it is not a homomorphism as a $\mathbb{Z}[i]$-module, because:

$$f(i \cdot 1) = -i \neq i = i \cdot f(1)$$

This is also a ring homomorphism.

Example. Let $M = N = \mathbb{Z}$ by $f(n) = 2n$. This is a $\mathbb{Z}$-module homomorphism by not a ring homomorphism as $f(1) = 2 \neq 1$.

Proposition 1.2. Let M, N be R-modules. Let $A \subseteq M$ and $B \subseteq N$ be R-submodules. Then $f(A)$ is an R-submodule of N and $f^{-1}(B)$ is an R-submodule of M. In particular, $\operatorname{Ker} f$ and $\operatorname{im} f$ are R-submodules.

Proposition 1.3. Compositions of R-module homomorphisms is an R-module homomorphism, and if f, g are R-module homomorphisms and $a, b \in \mathbb{R}$, then $af + bg$ is also an R-module homomorphism.

Definition. Let M be an R-module and $S \subseteq M$ be any subset. Then the **R-submodule of M generated by** S, denoted by $\langle S \rangle$, is the intersection of all R-submodules of M that contain S.

Theorem 1.4. Let M be an R-module with $S = \{s_1, \cdots, s_n\} \subseteq M$, then:

$$\langle S \rangle = \{r_1 s_1 + \cdots + r_n s_n : r_i \in R\}$$

Proof: Define the set:

$$RS = \{r_1 s_1 + \cdots + r_n s_n : r_i \in R\}$$

Clearly $RS \subseteq S$ because $s_1, \cdots, s_n \in N$ for all N in the intersection, thus $\sum r_i s_i$ is also contained in N as N is a module. Also, RS is an R-submodule of M that contains S, so RS is in that big intersection and thus $S \subseteq RS$. □

Remark. If S is infinite, we can let RS be the set of all finite linear combinations of elements in S, then $RS = \langle S \rangle$.

Definition. Let M be an R-module and $N \subseteq M$ an R-submodule. The **quotient R-module** M/N is the abelian group M/N with the R-multiplication by:

$$r \cdot (m + N) := (rm) + N$$

Easy to check that this is always well-defined.

Remark. If $\{s_1, \cdots, s_n\}$ generates M, then the set:

$$\{s_1 + N, \cdots, s_n + N\}$$

generates M/N. So if M/N is finitely generated, then so is M/N.

Theorem 1.5 (Universal Property of Quotients). Let $f : M \to N$ be an R-module homomorphism. Let $H \subseteq M$ be an R-submodule, and $q : M \to M/H$ the quotient map.

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "q"'] & N \\ M/H \arrow[ur, dashed, "\exists! \tilde{f}"'] & \end{tikzcd}$$

Then there is an R-module homomorphism $\tilde{f} : M/H \to N$ satisfying $f = \tilde{f} \circ q$ if and only if $H \subseteq \operatorname{Ker} f$. In this case:

$$\operatorname{Ker} \tilde{f} = q(\operatorname{Ker} f) \quad \text{and} \quad \operatorname{im} \tilde{f} = \operatorname{im} f$$

Definition. An R**-module isomorphism** is an R-module homomorphism whose inverse is also an R-module homomorphism. We can show that f is an R-module isomorphism if and only if f is a homomorphism and is bijective.

Corollary 1.6 (First Isomorphism Theorem). Let $f : M \to N$ be an R-module homomorphism, then $M/\operatorname{Ker} f \cong \operatorname{im} f$.

Proof: If we restrict the codomain to $\operatorname{im} f$, then f is surjective. To show the injectivity, note that $\operatorname{Ker} f \subseteq \operatorname{Ker} f$, so as in the UPQ, we have an homomorphism $\tilde{f} : M/\operatorname{Ker} f \to \operatorname{im} f$. Also, $\operatorname{Ker} \tilde{f} = q(\operatorname{Ker} f) = 0$. Therefore $\tilde{f}$ is an isomorphism. □

Lecture 3, 2024/05/10

Proof of UPQ: ($\Rightarrow$). If $\tilde{f}$ exists with $f = \tilde{f} \circ q$, then it follows immediately that $H \subseteq \operatorname{Ker} f$. Then we are done.

($\Leftarrow$). Assume $H \subseteq \operatorname{Ker} f$, we define $\tilde{f} : M/H \to N$ by:

$$\tilde{f}(m + H) = f(m)$$

To show this is well-defined, let $m + H = m' + H$ so that $m' - m = h \in H$, then:

$$\begin{aligned} \tilde{f}(m' + H) = f(m') = f(m + h) = f(m) + \underbrace{f(h)}_{=0} \\ = f(m) = \tilde{f}(m + H) \end{aligned}$$

The rest of the proof is trivial. □

1.3 The Ring of Integers

Definition. A ring R is **Noetherian** if every ideal of R is finitely generated.

Theorem 1.7. Let R be Noetherian and M a finitely generated R-module, then every submodule of M is finitely generated.

Proof: Google. □

Theorem 1.8. Let A be a Noetherian domain. Let T be a ring containing A, and $\alpha \in T$ an element. Then α is integral over A if and only if the ring $A[\alpha]$ is a finitely generated A-module.

Proof: ($\Rightarrow$). Let α be integral over A, so there are $a_0, \cdots, a_{n-1} \in A$ such that:

$$\alpha^n = a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 \tag{1}$$

Also, by definition we have:

$$A[\alpha] = A + \alpha A + \alpha^2 A + \cdots$$

By (1), we have that:

$$\alpha^n \in A + \alpha A + \cdots + \alpha^{n-1} A \tag{2}$$

By (2), we can see that:

$$\begin{aligned} \alpha^{n+1} &\in \alpha A + \cdots + \alpha^2 A + \cdots \alpha^n A \\ &\in A + \alpha A + \cdots + \alpha^{n-1} A \end{aligned}$$

Continue doing this, we see that this is true for all powers of α, hence:

$$A[\alpha] = A + \alpha A + \cdots + \alpha^{n-1} A$$

is a finitely generated A-module.

($\Leftarrow$). Suppose $A[\alpha]$ is a finitely generated A-module. Say it is generated by $p_1(\alpha), \cdots, p_r(\alpha)$ where $p_i(x) \in A[x]$ are polynomials. For all $n \in \mathbb{N}$ we have:

$$\alpha^n = a_1 p_1(\alpha) + \cdots + a_r p_r(\alpha)$$

for some $a_i \in A$. For $n \in \mathbb{N}$ large enough (larger than any degree of $p_i(x)$), we have:

$$\begin{aligned} \alpha^n &= a_1 p_1(\alpha) + \cdots + a_r p_r(\alpha) \\ &= b_0 + b_1\alpha + \cdots + b_m \alpha^m \end{aligned}$$

So that $m < n$. It follows that $f(x) = x^n - b_1 x - \cdots - b_m x^m \in A[x]$ vanishes at α and is monic. □

Theorem 1.9. Let A be a Noetherian domain. Let T be a ring containing A. The set of elements of T that are integral over A is a ring, called the **integral closure** of A in T.

Proof: Clearly 1 is integral over A. Suppose $\alpha, \beta \in T$ are integral over A. Then $A[\alpha]$ and $A[\beta]$ are finitely generated A-modules. Write:

$$A[\alpha] = a_1 A + \cdots + a_r A \qquad (a_1 = 1)$$
$$A[\beta] = b_1 A + \cdots + b_m A \qquad (b_1 = 1)$$

Then $A[\alpha, \beta]$ is contained in the A-module:

$$R = \sum_{i,j} a_i b_j A$$

which is the A-module generated by $\{a_i b_j\}$ with $1 \leq i \leq r$ nad $1 \leq j \leq m$. Clearly R is finitely generated, and since A is Noetherian and $A[\alpha, \beta] \subseteq R$, we see that $A[\alpha, \beta]$ is finitely generated by Theorem 1.7. Now, clearly:

$$A[\alpha \pm \beta],\ A[\alpha\beta] \subseteq A[\alpha, \beta]$$

It follows that $A[\alpha \pm \beta]$ and $A[\alpha\beta]$ are both finitely generated A-modules, which implies $\alpha \pm \beta$ and $\alpha\beta$ are integral over A. □

Definition. Let K be a number field, the set of algebraic integers in K is the set of elements of K that are integral over $\mathbb{Z}$, called the **ring of integers** of K, we denote it by $\mathcal{O}_K$.

Lecture 4, 2024/05/13

1.4 Trace and Norm

Definition. Let K be a field, a K**-algebra** is a set A that is a ring and also a vector space over K using the same operations.

Example. Any ring that contains K is a K-algebra.

Definition. Let K be a field and L a K-algebra that is also a finite dimensional vector space over K. Let $\alpha \in L$ be an element. Define $T_\alpha : L \to L$ by $T_\alpha(x) = \alpha x$. This is a linear transformation. We define the **trace** of α over K to be:

$$\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}(T_\alpha)$$

The **norm** of α over K is:

$$N_{L/K}(\alpha) = \det(T_\alpha)$$

Example. Pick $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$. Let $\alpha = 3 + 4i$. Choose a basis $\{1, i\}$ for L/K, then:

$$[T_\alpha] = \begin{pmatrix} 3 & -4 \\ 4 & 3 \end{pmatrix}$$

It follows that $\mathrm{Tr}_{L/K}(\alpha) = 6$ and $N_{L/K}(\alpha) = 25$.

Theorem 1.10. If L/K is a field extension, let $f(x)$ be the characteristic polynomial of T_α over K and $m(x)$ the minimal polynomial of α over K, then:

$$f(x) = m(x)^r$$

with $r = \deg(f)/\deg(m) = [L : K(\alpha)]$.

Proof: Let $M(x) \in K[x]$ be the minimal polynomial of the linear map T_α, that is, $M(T_\alpha)$ is the zero map from L to L. We claim that $M(\alpha) = 0$, indeed, if:

$$M(x) = a_n x^n + \cdots + a_1 x + a_0$$

then we have:

$$M(T_\alpha) = a_n T_\alpha^n + \cdots + a_1 T_\alpha + a_0$$

Plug in $x = 1$ to this function $M(T_\alpha)$ we get 0, thus:

$$0 = a_n T_\alpha^n(1) + \cdots + a_1 T_\alpha(1) + a_0 = a_n \alpha^n + \cdots + a_1 \alpha + a_0 = M(\alpha)$$

Since $m(x)$ is the minimal polynomial for α over K, we have $m(x) \mid M(x)$. Since $M(x)$ is irreducible, we have $m(x) = M(x)$. Since $M(x)$ and $f(x)$ have the same roots, we know $m(x)$ and $f(x)$ have the same roots. Now, note that if $p(x)$ is irreducible and $p(x) \mid f(x)$, then $M(x) \mid p(x)$, thus $M(x) = p(x)$. It means the only irreducible factor of $f(x)$ is $M(x) = m(x)$. Therefore $f(x) = m(x)^r$ where:

$$r = \deg(f)/\deg(m) = \frac{[L : K]}{[K(\alpha) : K]} = [L : K(\alpha)]$$

As desired. □

Thus $\mathrm{Tr}_{L/K}(\alpha)$ is the sum of Galois conjugates of α with multiplicity. If L/K is separable, then no multiplicity and:

$$\mathrm{Tr}_{L/K}(\alpha) = r(\alpha_1 + \cdots + \alpha_d)$$
$$N_{L/K}(\alpha) = (\alpha_1 \cdots \alpha_d)^r$$

where $\alpha_1, \cdots, \alpha_d$ are the conjugates of α, that is, they are all roots of the minimal polynomial $m(x)$ of α over K.

Example. The trace and norm of α is dependent on the L and K, for example:

$$\mathrm{Tr}_{\mathbb{Q}/\mathbb{Q}}(3) = 3 \text{ and } \mathrm{Tr}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(3) = 6$$

Definition. A **symmetric bilinear pairing** on a ring L is a map:

$$\langle \cdot, \cdot \rangle : L \times L \to L$$

by $\langle x, y \rangle = \mathrm{Tr}(xy)$. It is easy to check this is symmetric and bilinear.

It is also non-degenerate: If $x \in L$ and $x \neq 0$, then $\langle x, \frac{1}{x} \rangle = [L : K] \neq 0$.

Theorem 1.11. Let $L/\mathbb{Q}$ be a field extension of degree d. Then the ring of integers $\mathcal{O}_L \subseteq L$ is isomorphic to $\mathbb{Z}^d$ as an additive group.

Lemma 1.12. The fraction field of $\mathcal{O}_L$ is L.

Proof: Let $\alpha \in L$. It is enough to show that $N\alpha \in \mathcal{O}_L$ for some $N \in \mathbb{Z}$ and $N \neq 0$. Let $m(x) \in \mathbb{Q}[x]$ be the monic minimal polynomial of α over $\mathbb{Q}$. We can choose $N \in \mathbb{Z}$ to be the lcm of all denominators of coefficients of $m(x)$. Then $Nm(x) \in \mathbb{Z}[x]$. The monic minimal polynomial of $N\alpha$ over $\mathbb{Q}$ is $N^d m(x/N)$, which is in $\mathbb{Z}[x]$ and monic. Hence $N\alpha \in \mathcal{O}_L$. □

Proof of Theorem 1.8: Note that if α is an algebraic integer, then so are $\mathrm{Tr}_{L/K}(\alpha)$ and $N_{L/K}(\alpha)$, as $\alpha_1, \cdots, \alpha_d$ have the same minimal polynomial. Then α is an algebraic integer $\iff$ α_i is an algebraic integer. Let $\{x_1, \cdots, x_d\}$ be a $\mathbb{Q}$-basis of L. By the lemma, we can multiply each x_i by some N to make them lie in $\mathcal{O}_L$. Thus WLOG suppose all x_i lie in $\mathcal{O}_L$. Define $\phi : L \to \mathbb{Q}^d$ by:

$$\phi(\alpha) = (\langle \alpha, x_1 \rangle, \cdots, \langle \alpha, x_d \rangle) = (\mathrm{Tr}_{L/K}(\alpha x_1), \cdots, \mathrm{Tr}_{L/K}(\alpha x_d))$$

This is a K-linear map. It is injective by the non-degeneracy of the pairing. The image of $\mathcal{O}_L$ under ϕ is a subset of $\mathbb{Z}^d$. And ϕ is a $\mathbb{Z}$-module homomorphism, so $\phi(\mathcal{O}_L)$ is a $\mathbb{Z}$-submodule of $\mathbb{Z}^d$. Hence $\Phi(\mathcal{O}_L) \cong \mathbb{Z}^d$ for some r. But $\mathcal{O}_L$ contains a basis of $\mathbb{Q}^d$, so $r = d$. Therefore $\mathcal{O}_L \cong \mathbb{Z}^d$. □

Therefore $\mathcal{O}_K = \alpha\mathbb{Z} + \cdots + \alpha_d\mathbb{Z}$ for some $\alpha_i \in \mathcal{O}_K$.

Lecture 5, 2024/05/15

Theorem 1.13. Let $I \subseteq \mathcal{O}_K$ be a nonzero ideal, then $I \cong \mathbb{Z}^d$ as additive groups.

Proof: Let $\alpha \in I$ with $\alpha \neq 0$. Then clearly $\alpha\mathcal{O}_K \subseteq I$. But $\mathcal{O}_K \cong \alpha\mathcal{O}_K$ as additive groups via $x \mapsto \alpha x$. So $\alpha\mathcal{O}_K \cong \mathbb{Z}^d$ as additive groups and:

$$\alpha\mathcal{O}_K \subseteq I \subseteq \mathcal{O}_K$$

Since we have $\alpha\mathcal{O}_K \cong \mathcal{O}_K \cong \mathbb{Z}^d$, this means $I \cong \mathbb{Z}^d$ because I is a torsion free, finitely generated abelian group of rank between d and d. □

Theorem 1.14. Let $I \subseteq \mathcal{O}_K$ be a nonzero ideal, then $\mathcal{O}_K/I$ is a finite ring.

Proof: Since $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module, so is $\mathcal{O}_K/I$. It suffices to show every element of $\mathcal{O}_K/I$ has finite order, because of this: Let $y_1, \cdots, y_n$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K/I$, then:

$$\mathcal{O}_K/I = \{a_1y_1 + \cdots + a_ny_n : a_i \in \mathbb{Z}\}$$

If a_iy_i can only represent finitely many elements in $\mathcal{O}_K/I$ for each i, then $\mathcal{O}_K/I$ must be finite. Let $\overline{x} \in \mathcal{O}_K/I$ be an element and let $x \in \mathcal{O}_K$ be a preimage of $\overline{x}$. We want to show that $nx \in I$ for some nonzero $n \in \mathbb{Z}$. Let $\{x_1, \cdots, x_d\}$ be a $\mathbb{Z}$-basis for I. They are also a $\mathbb{Q}$-basis for K, so there exist $a_1, \cdots, a_d \in \mathbb{Q}$ with:

$$x = a_1x_1 + \cdots + a_dx_d$$

Clearing denominators gives $Ax = A_1x_1 + \cdots A_dx_d$ for some $A_1, \cdots, A_d \in \mathbb{Z}$ and $0 \neq A \in \mathbb{Z}$. Therefore $A\overline{x} = 0$ in $\mathcal{O}_K/I$, done. □

Theorem 1.15. Let $\alpha \in \mathcal{O}_K$ be nonzero, then $\mathcal{O}_K/(\alpha)$ has $|N_{K/\mathbb{Q}}(\alpha)|$ elements.

Proof: Recall that $\alpha\mathcal{O}_K$ has a basis $\{\alpha x_1, \cdots, \alpha x_d\}$, where $\{x_1, \cdots, x_d\}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$. That is, $\alpha\mathcal{O}_K$ is $T_\alpha(\mathcal{O}_K)$. And $|N(\alpha)| = |\det T_\alpha|$. By some Geometry fact from Appendix, we have:

$$|\mathcal{O}_K/T_\alpha(\mathcal{O}_K)| = |\det T_\alpha|$$

The result follows. □

Theorem 1.16. Every finite domain is a field.

Proof: Let R be a finite domain. It is enough to show R is a division ring. Let $a \in R$, define a map $T : R \to R$ by $T(x) = ax$. Then T is injective since R is a domain, therefore it must be onto, in particular $T(x) = ax = 1$ for some $x \in R$. □

Corollary 1.17. Every nonzero prime ideal of $\mathcal{O}_K$ is maximal.

Proof: Let P be a prime ideal, then $\mathcal{O}_K/P$ is a finite domain, thus a field. □

1.5 Dedekind Domains

Definition. Let R be a ring, the **Krull dimension** of R is the length of a maximal chain of prime ideals by inclusion. More explicity, if the longest chain in R is:

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_d$$

then R has Krull dimension d. If R has chains of arbitrary length, then we say it has dimension ∞.

In particular, if R has Krull dimension 1, then every prime ideal of R is maximal and vice versa.

Definition. Let $A \subseteq T$ be rings, the set of elements in T that are integral over A is called the **integral closure** of A in T. We say A is **integrally closed in** T if $A =$ its integral closure in T.

Definition. A domain R is **integrally closed** if it is integrally closed in its field of fraction.

Theorem 1.18. Let A, T be Noetherian. If α is integral over T and T is integral over A, then α is integral over A.

Proof: Since T is Noetherian and integral over A, it is finitely generated as an A-algebra:

$$T = A[a_1, \cdots, a_r]$$

In particular, all we need is that α is integral over $A[a_1, \cdots, a_r]$, where a_i are the coefficients of the monic minimal polynomial of α over T. We want to show $A[\alpha]$ is a finitely generated A-module, but:

$$A[\alpha] \subseteq \bigoplus_{i,j} A[a_i b_j]$$

which is a finitely generated A-algebra. Then:

$$A[a_1, \cdots, a_r, \alpha] = \bigoplus_{j} A[a_1, \cdots, a_r] b_j$$

so $A[\alpha]$ is contained in a finitely generated A-module and it therefore finitely generated since A is Noetherian. □

Definition. A **Dedekind Domain** is a domain that is integrally closed and is Noetherian of Krull dimension 1.

Lecture 6, 2024/05/17

1.6 Geometry of Numbers

Definition. A **lattice** in $\mathbb{R}^n$ is an additive subgroup $\Lambda \subseteq \mathbb{R}^n$ that spans $\mathbb{R}^n$ and is isomorphic to $\mathbb{Z}^n$ as additive groups.

So a lattice is just the set of $\mathbb{Z}$-linear combinations of some basis of $\mathbb{R}^n$. We are going to build a $\mathbb{R}$-vector space in which $\mathcal{O}_K$ is a lattice.

As $\mathcal{O}_K \cong \mathbb{Z}^d$, we need a d-dimensional vector space. By Galois Theory, there are d embeddings $K \to \mathbb{C}$, so we can define $\phi : K \to \mathbb{C}^d$ by:

$$\phi(\alpha) = (\phi_1(\alpha), \cdots, \phi_d(\alpha))$$

where $\phi_1, \cdots, \phi_d$ are the d embeddings. This map ϕ is called the **Minkowski map**. It is a homomorphism and a $\mathbb{Q}$-linear map.

Example. If $K = \mathbb{Q}(\sqrt{2})$, then:

$$\phi(a + b\sqrt{2}) = (a + b\sqrt{2}, a - b\sqrt{2})$$

Then $\phi(\mathcal{O}_K) \cong \mathbb{Z}^d$ in $\mathbb{C}^d$, However, we want to embed $\mathcal{O}_K$ in $\mathbb{R}^d$, not $\mathbb{C}^d$.

Let $\phi_1, \cdots, \phi_r$ be the real embeddings. Pair up the complex embeddings with their complex conjugates so that:

$$\phi_{r+1} = \overline{\phi_{r+2}}, \ \cdots, \phi_{d-1} = \overline{\phi_d}$$

Define the **Minkowski Space** V_K of K to be the subspace of $\mathbb{C}^d$ defined by:

$$\begin{aligned} \operatorname{Im}(x_1) = \cdots = \operatorname{Im}(x_r) &= 0 \\ \operatorname{Im}(x_{i+1}) &= -\operatorname{Im}(x_{i+2}) \ \ \forall r \le i \le d-1 \\ \operatorname{Re}(x_{i+1}) &= \operatorname{Re}(x_{i+2}) \ \ \forall r \le i \le d-1 \end{aligned}$$

The Minkowski space is a subset of $\mathbb{C}^d$ such that if we view it as a vector space over $\mathbb{R}$, it has dimension r. That is $\dim_{\mathbb{R}} V_K = r$. Also $\phi(K) \subseteq V_K$. So:

$$\phi(\mathcal{O}_K) \cong \mathcal{O}_K \cong \mathbb{Z}^d$$

as additive groups. And $\phi(\mathcal{O}_K)$ sits inside a $\mathbb{R}$-vector space of dimension d, so it is a lattice: To show this, need to show $\phi(\mathcal{O}_K)$ spans the Minkowski space a $\mathbb{R}$-vector space (See Appendix).

Example. Let $K = \mathbb{Q}(\sqrt{2})$, then $\phi(a + b\sqrt{2}) = (a + b\sqrt{2}, a - b\sqrt{2})$.

Example. Let $K = \mathbb{Q}(i)$, then $\phi(a + bi) = (a + bi, a - bi)$. We have:

$$\phi(1) = (1, 1) \text{ and } \phi(i) = (i, -i)$$

Here both $\phi(1)$ and $\phi(i)$ have length $\sqrt{2}$. So $\phi(\mathbb{Z}[i])$ is a square lattice with side length $\sqrt{2}$.

Lecture 7, 2024/05/21

Example. Let $K = \mathbb{Q}(\alpha)$, where α is a root of $f(x) = x^3 + 3x + 3$. Then $f'(x) = 3x^2 + 3$ has no real roots. So f has exactly one real root and two complex roots. So $\mathbb{Q}(\alpha)$ is different depending on which α we pick. If $\alpha \in \mathbb{Q}$ then $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, while the complex roots give $\mathbb{Q}(\alpha) \not\subseteq \mathbb{R}$. But $\mathbb{Q}(\alpha)$ is well-defined up to isomorphism.

More importantly, no matter which α we pick, we get the same Minkowski space out of it, with the same image of K in it.

$$\phi(a) = (\phi_1(a), \phi_2(a), \phi_3(a))$$

where ϕ_1, ϕ_2, ϕ_3 are the embeddings of $\mathbb{Q}(\alpha)$ in $\mathbb{C}$. These 3 embeddings have the same image regardless of which root we pick, so the images of K and $\mathcal{O}_K$ are the same, too.

In this case, it can be shown that $\mathcal{O}_K = \mathbb{Z}[\alpha]$, it has basis $\{1, \alpha, \alpha^2\}$ as a $\mathbb{Z}$-module. What are their images under ϕ_1, ϕ_2, ϕ_3? Say the roots of $f(x)$ are $\alpha_1, \alpha_2, \alpha_3$ where $\alpha_1 \in \mathbb{R}$ and $\alpha_2 = \overline{\alpha_3}$.

$$\begin{aligned}\phi(1) &= (1, 1, 1)\\ \phi(\alpha) &= (\alpha_1, \alpha_2, \alpha_3)\\ \phi(\alpha^2) &= (\alpha_1^2, \alpha_2^2, \alpha_3^2)\end{aligned}$$

To see what they look like, we can compute the angles between them. We know:

$$\|u\|\|v\| \cos\theta = u \cdot v$$

(i). For $\phi(1)$ and $\phi(\alpha)$, we have:

$$\phi(1) \cdot \phi(\alpha) = \overline{\alpha_1} + \overline{\alpha_2} + \overline{\alpha_2} = \overline{\alpha_1 + \alpha_2 + \alpha_3} = 0$$

because $\alpha_1 + \alpha_2 + \alpha_3 = 0$, since it is the coefficient of x^2 term of $f(x)$, which is 0. Hence the vectors $\phi(1)$ and $\phi(\alpha)$ in $\mathbb{C}^3$ are orthogonal.

(ii). For $\phi(1)$ and $\phi(\alpha^2)$, we have:

$$\phi(1) \cdot \phi(\alpha^2) = \overline{\alpha_1^2 + \alpha_2^2 + \alpha_3^2}$$

Here we have:

$$(\alpha_1 + \alpha_2 + \alpha_3)^2 = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + 2\alpha_1\alpha_2 + 2\alpha_2\alpha_3 + 2\alpha_1\alpha_3$$

Hence:

$$\phi(1) \cdot \phi(\alpha^2) = \overline{(\alpha_1 + \alpha_2 + \alpha_3)^2 - 2(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3)} = 0 - 2(3) = -6$$

To figure out the angle between them, we need $\|\phi(1)\|$ and $\|\phi(\alpha^2)\|$.

$$\|\phi(1)\| = \sqrt{1^2 + 1^2 + 1^2} = \sqrt{3}$$

and that:

$$\begin{aligned}\|\phi(\alpha^2)\| &= \sqrt{\alpha_1^2\overline{\alpha_1}^2 + \alpha_2^2\overline{\alpha_2}^2 + \alpha_3^2\overline{\alpha_3}^2}\\ &= \sqrt{\alpha_1^4 + 2\alpha_2^2\alpha_3^2}\\ &= \sqrt{\alpha_1^4 + 18/\alpha_1^2}\end{aligned}$$

This last equality is because $\alpha_1^2\alpha_2^2\alpha_3^2 = (-3)^2 = 9$. Then:

$$\begin{aligned}\|\phi(\alpha^2)\| &= \frac{1}{|\alpha_1|}\sqrt{\alpha_1^6 + 18} \\ &= \frac{1}{|\alpha_1|}\sqrt{(3\alpha_1+3)^2 + 18} \\ &= -\frac{1}{\alpha_1}\sqrt{9\alpha_1^2 + 18\alpha_1 + 27}\end{aligned}$$

By IVT, we must have $-9/10 < \alpha < -4/5$ and $\alpha_1^6 \approx 0$ so:

$$\|\phi(\alpha^2)\| \approx 4\sqrt{2}$$

Hence we have:

$$-6 \approx \sqrt{3}\cdot 4\sqrt{2}\cos\theta \implies \theta \approx 123^\circ$$

Lecture 8, 2024/05/22

(iii). For $\phi(\alpha)$ and $\phi(\alpha^2)$. We have:

$$\begin{aligned}\phi(\alpha)\cdot\phi(\alpha^2) &= \alpha_1\overline{\alpha_1}^2 + \alpha_2\overline{\alpha_2}^2 + \alpha_3\overline{\alpha_3}^2 \\ &= \alpha_1^3 + \alpha_2\alpha_3^2 + \alpha_3\alpha_2^2 \\ &= (-3\alpha_1 - 3) + \alpha_3\left(\frac{-3}{\alpha_1}\right) + \alpha_2\left(\frac{-3}{\alpha_1}\right) \\ &= -3\alpha_1 - 3 - \frac{3}{\alpha_1}(\alpha_2+\alpha_3) \\ &= -3\alpha_1 - 3 - \frac{3}{\alpha_1}(-\alpha_1) \\ &= -3\alpha_1 \approx \frac{12}{5}\end{aligned}$$

Also, we have:

$$\|\phi(\alpha)\| = \sqrt{\alpha_1\overline{\alpha_1} + \alpha_2\overline{\alpha_2} + \alpha_3\overline{\alpha_3}} = \sqrt{\alpha_1^2 - \frac{6}{\alpha_1}} \approx \sqrt{7.5}$$

It follows that:

$$\|\phi(\alpha)\|\|\phi(\alpha^2)\|\cos\theta = \phi(\alpha)\cdot\phi(\alpha^2)$$

Hence:

$$\sqrt{7.5}\cdot\sqrt{8}\cos\theta = \frac{12}{5} \implies \theta \approx 73^\circ$$

Example. Let $K = \mathbb{Q}(\sqrt{2},\sqrt{3})$. It turns out that:

$$\mathcal{O}_K = \mathbb{Z}\left[\sqrt{2},\sqrt{3},\frac{\sqrt{2}+\sqrt{6}}{2}\right]$$

A $\mathbb{Z}$-basis for $\mathcal{O}_K$ is $\{1, \sqrt{3}, \frac{\sqrt{2}+\sqrt{6}}{2}, \frac{\sqrt{2}-\sqrt{6}}{2}\}$. Automorphisms of $\mathbb{Z}^d$ are $d \times d$ matrices with integer entries and determinant ±1. The four embeddings of K in $\mathbb{C}$ are determined by:

$$\begin{cases} \sqrt{2} & \mapsto \pm\sqrt{2} \\ \sqrt{3} & \mapsto \pm\sqrt{3} \end{cases}$$

So we have:

$$\phi(1) = (1,1,1,1) \text{ and } \phi(\sqrt{3}) = (\sqrt{3}, -\sqrt{3}, \sqrt{3}, -\sqrt{3})$$

and that:

$$\phi\left(\frac{\sqrt{2}+\sqrt{6}}{2}\right) = \left(\frac{\sqrt{2}+\sqrt{6}}{2}, \frac{\sqrt{2}-\sqrt{6}}{2}, \frac{-\sqrt{2}-\sqrt{6}}{2}, \frac{-\sqrt{2}+\sqrt{6}}{2}\right)$$
$$\phi\left(\frac{\sqrt{2}-\sqrt{6}}{2}\right) = \left(\frac{\sqrt{2}-\sqrt{6}}{2}, \frac{\sqrt{2}+\sqrt{6}}{2}, \frac{-\sqrt{2}+\sqrt{6}}{2}, \frac{-\sqrt{2}-\sqrt{6}}{2}\right)$$

Note that all embeddings of K are real, and we say K is totally real.

(i). $\phi(1)$ is orthogonal to all the others.

(ii). For $\phi(\sqrt{3})$ we have:

$$\phi(\sqrt{3}) \cdot \phi\left(\frac{\sqrt{2}+\sqrt{6}}{2}\right) = \frac{\sqrt{6}+3\sqrt{2}}{2} + \frac{-\sqrt{6}+3\sqrt{2}}{2} + \frac{-\sqrt{6}-3\sqrt{2}}{2} + \frac{\sqrt{6}-3\sqrt{2}}{2} = 0$$

and similarly we have:

$$\phi(\sqrt{3}) \cdot \phi\left(\frac{\sqrt{2}-\sqrt{6}}{2}\right) = 0$$

So it is also orthogonal to all vectors.

(iii). For the other two, we have:

$$\phi\left(\frac{\sqrt{2}+\sqrt{6}}{2}\right) \cdot \phi\left(\frac{\sqrt{2}-\sqrt{6}}{2}\right) = -1-1-1-1 = -4$$

and:

$$\left|\phi\left(\frac{\sqrt{2}+\sqrt{6}}{2}\right)\right| = 2\sqrt{2}$$

which implies $\theta = 120°$, where θ is the angle between these two vectors. Let us now compute the trace and norm.

$$[T_{\sqrt{3}}] = \begin{pmatrix} 0 & 3 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & -1 \\ 0 & 0 & 1 & -2 \end{pmatrix}$$

so that:

$$\mathrm{Tr}_{K/\mathbb{Q}}(\sqrt{3}) = 0 \text{ and } N_{K/\mathbb{Q}}(\sqrt{3}) = 9$$

Lecture 9, 2024/05/24

1.7 Discriminants

Discriminant is an important invariant of number fields. It helps us calculate $|\mathcal{O}_K/I|$ where I is an ideal. Also, it helps us in guessing what $\mathcal{O}_K$ is.

Definition. Let V be a complex inner product space. Let $\{v_1, \cdots, v_n\} \subseteq V$. Define:

$$A = [v_1, \cdots, v_n]$$

with respect to a unitary basis for V. Define the **discriminant** of $\{v_1, \cdots, v_n\}$ to be:

$$\mathrm{disc}(v_1, \cdots, v_n) = (\det A)^2$$

If $n \neq \dim_{\mathbb{C}} V$, then we define $\mathrm{disc}(v_1, \cdots, v_n) = 0$.

Remark. This definition is independent of the choice of unitary basis because change in choice of unitary basis changes $\det A$ by $\det(\text{unitary}) = \pm 1$. Then squaring it is just 1.

Definition. The **discriminant** of a lattice Λ in V_K is $\mathrm{disc}(v_1, \cdots, v_n)$ for any choice of $\mathbb{Z}$-basis $\{v_1, \cdots, v_n\}$ of Λ.

Definition. The discriminant of a number field K is $\mathrm{disc}\, K = \mathrm{disc}\, \mathcal{O}_K$, where we identify $\mathcal{O}_K$ as a lattice of V_K.

Example. Let $K = \mathbb{Q}(i)$, then $\mathcal{O}_K = \mathbb{Z}[i] \subseteq V_K$. Then $\{1, i\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}_K$. We know that:

$$\mathbb{Z}^2 \cong \mathcal{O}_K \hookrightarrow \mathbb{C}^2$$

via the map:

$$1 \mapsto \begin{pmatrix} 1 \\ 1 \end{pmatrix} \text{ and } i \mapsto \begin{pmatrix} i \\ -i \end{pmatrix}$$

Hence the matrix A is defined by:

$$A = \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$$

It follows that $\mathrm{disc}\, K = \mathrm{disc}\, \mathbb{Z}[i] = (\det A)^2 = -4$.

Discriminants can be used to "discriminate" between number fields. It can be shown that:

$$\operatorname{disc}\mathbb{Q}(\sqrt{3}) = 12 \text{ and } \operatorname{disc}\mathbb{Q}(\sqrt{5}) = 5$$

Therefore $\mathbb{Q}(\sqrt{3})$ is not isomorphic to $\mathbb{Q}(\sqrt{5})$.

Theorem 1.19. Let K be a number field and $\{v_1, \cdots, v_n\} \subseteq K$, then:

$$\operatorname{disc}(v_1, \cdots, v_n) = \det B$$

where:

$$B = (\operatorname{Tr}_{K/\mathbb{Q}}(v_i v_j))_{i,j} = \begin{pmatrix} \operatorname{Tr}_{K/\mathbb{Q}}(v_1 v_1) & \cdots & \operatorname{Tr}_{K/\mathbb{Q}}(v_1 v_n) \\ \vdots & \ddots & \vdots \\ \operatorname{Tr}_{K/\mathbb{Q}}(v_n v_1) & \cdots & \operatorname{Tr}_{K/\mathbb{Q}}(v_n v_n) \end{pmatrix}$$

Proof: Let $\sigma_1, \cdots, \sigma_n : K \hookrightarrow \mathbb{C}$ be embeddings. Then $A = (\sigma_i(v_j))$ and $A^T A = (\sigma_j(v_i))(\sigma_i(v_j))$.

$$(i,j)\text{-entry} = \sum_k \sigma_k(v_i)\sigma_k(v_j) = \sum_k \sigma_k(v_i v_j) = \operatorname{Tr}_{K/\mathbb{Q}}(v_i v_j)$$

Hence $A^T A = B$ and $(\det A)^2 = \det B$. □

Theorem 1.20. Let K be a number field and $\Gamma \subseteq \Lambda \subseteq V_K$ be lattices. Suppose $\Gamma \subseteq \Lambda$ has index n, that is, $|\Lambda/\Gamma| = n$ as groups. Then $\operatorname{disc}\Gamma = n^2 \operatorname{disc}\Lambda$.

Proof: Consider the linear map $T : V_K \to V_K$ that takes $\mathbb{Z}$-basis of Λ to $\mathbb{Z}$-basis of Γ. Then T as a matrix has $\mathbb{Z}$-coefficients because $\Gamma \subseteq \Lambda$. Then:

$$\operatorname{disc}\Gamma = \det\begin{pmatrix}\text{matrix of} \\ \text{basis of } \Gamma\end{pmatrix}^2 = \det\left(T\begin{pmatrix}\text{matrix of} \\ \text{basis of } \Lambda\end{pmatrix}\right)^2 = (\det T)^2 \operatorname{disc}\Lambda$$

Here $\det T = n$ since $\Gamma \subseteq \Lambda$ has index n. □

Definition. Let $I = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$ be a lattice in V_K, the **(ideal) norm** of I is defined to be:

$$N(I) = \sqrt{\frac{\operatorname{disc}(v_1, \cdots, v_n)}{\operatorname{disc} K}}$$

Theorem 1.21. If $I \subseteq \mathcal{O}_K$ is an ideal and $0 \neq a \in \mathcal{O}_K$, then $N(aI) = |N_{K/\mathbb{Q}}(a)|N(I)$.

Proof: Let $\{v_1, \cdots, v_n\}$ be a basis for I, then $av_1, \cdots, av_n$ is a basis for aI. Then:

$$\operatorname{disc}(aI) = \det(av_1, \cdots, av_n)^2$$

We have scaled by $\sigma_i(a)$ in the i-th coordinate of V_K, so:

$$\begin{aligned}\operatorname{disc}(aI) &= \det(\operatorname{diag}(\sigma_1(a), \cdots, \sigma_n(a)))^2 \det(v_1, \cdots, v_n)^2 \\ &= N(a)^2 \operatorname{disc}(I)\end{aligned}$$

It follows that:

$$N(aI)^2 = \frac{\operatorname{disc}(aI)}{\operatorname{disc}(K)} = N(a)^2 N(I)^2$$

Thus $N(aI) = |N(a)|N(I)$, as desired. □

Corollary 1.22. For $a \in \mathcal{O}_K$, we have $N(a\mathcal{O}_K) = N((a)) = |N_{K/\mathbb{Q}}(a)|$.

Proof: Note that $N(\mathcal{O}_K) = 1$, and apply the above theorem. □

Discriminant allows us to guess what $\mathcal{O}_K$ is. In general, let $A \subseteq \mathcal{O}_K$ be a subring. We can compute $\operatorname{disc} A$. By Theorem 1.20 we have:

$$\operatorname{disc} A = [\mathcal{O}_K : A]^2 \operatorname{disc} \mathcal{O}_K$$

If $\operatorname{disc} A$ is squarefree, then we must have $[\mathcal{O}_K : A] = 1$, hence $A = \mathcal{O}_K$.

Lecture 10, 2024/05/27

Proposition 1.23. Let K be a number field and $I \subseteq \mathcal{O}_K$ be an ideal, then:

$$N(I) = |\mathcal{O}_K / I|$$

Example. Let $K = \mathbb{Q}(\alpha)$, where α is a root of $x^3 + x + 1$. Then $\operatorname{disc} \mathbb{Z}[\alpha] = -31$. Since $\mathbb{Z}[\alpha]$ has finite index in $\mathcal{O}_K$, we conclude that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

Definition. Let K be a field and $f(x) \in K[x]$ be a polynomial. The **discriminant** of $f(x)$ is:

$$\operatorname{disc} f(x) = \prod_{i<j} (\alpha_i - \alpha_j)^2$$

where $\alpha_1, \cdots, \alpha_n$ are all the roots of $f(x)$.

Theorem 1.24. Let $K = \mathbb{Q}(\alpha)$ be a number field and let $m(x)$ be the monic minimal polynomial of α over $\mathbb{Q}$, then we have that:

$$\operatorname{disc} \mathbb{Z}[\alpha] = \operatorname{disc} m(x)$$

Proof: A $\mathbb{Z}$-basis for $\mathbb{Z}[\alpha]$ is $\{1, \alpha, \cdots, \alpha^{d-1}\}$. Then:

$$\operatorname{disc} \mathbb{Z}[\alpha] = \det \begin{pmatrix} 1 & \cdots & 1 \\ \sigma_1(\alpha) & \cdots & \sigma_d(\alpha) \\ \vdots & \ddots & \vdots \\ \sigma_1(\alpha^{d-1}) & \cdots & \sigma_d(\alpha^{d-1}) \end{pmatrix}$$

This is exactly the Vandermonde determinant, which evaluates to:

$$\prod_{i<j}(\sigma_i(\alpha)-\sigma_j(\alpha))^2$$

which is exactly $\operatorname{disc} m(x)$, as desired. □

But how do we compute $\operatorname{disc} m(x)$? Answer: Resultant!

Definition. Let K be a field. The **resultant** of two polynomials $f(x)$ and $g(x)$ in $K[x]$ is an element of K, given as follow. Let:

$$P_n(x) = \{p(x) \in K[x] : \deg p(x) \leq n\}$$

As vector space over K we have $\dim P_{n-1}(x) = n$. Let us say:

$$\deg f(x) = d \text{ and } \deg g(x) = e$$

Define $T : P_{d-1}(x) \times P_{e-1}(x) \to P_{d+e-1}(x)$ by:

$$T(A, B) = Ag + Bf$$

It is easy to check this is well-defined and is a linear map. We define the resultant of f, g to be:

$$R(f, g) = \det T$$

Theorem 1.25. Let $m(x) \in K[x]$ be a monic polynomial and let $n = \deg(m(x))$, then:

$$\operatorname{disc} m(x) = (-1)^{\binom{n}{2}} R(m, m')$$

Before we prove this, we first prove a very important fact about resultants.

Theorem 1.26. Let f, g be nonconstant polynomials. Then $R(f, g) = 0$ if and only if f, g have a nontrivial common factor.

Proof: $(\Rightarrow)$. Assume $R(f, g) = 0$, then T has a nontrivial kernel, that is, there is a nonzero $(A, B) \in \operatorname{Ker} T$ such that:

$$Ag + Bf = 0$$

where $\deg A < \deg f$ and $\deg B < \deg g$. But $f \mid Ag$ implies $A = 0$ or $\gcd(f, g) \neq 1$ and $A = 0$ implies $f = 0$. Either way, we have $\gcd(f, g) \neq 1$.

$(\Leftarrow)$. Say $\gcd(f, g) = h(x)$ nonconstant.

$$T : P_{d-1} \times P_{e-1} \to P_{d+e-1}$$

The image of T is contained in the proper space $h(x)P_{d+e-1}$, thus T is not onto and $\det T = 0$. $\square$

Let us try to compute $R(f,g)$. Pick bases for $P_{d-1} \times P_{e-1}$ and P_{d+e-1}:

$$\mathcal{B} = \{(1,0),(x,0),\cdots,(x^{d-1},0),(0,1),(0,x),\cdots,(0,x^{e-1})\}$$

$$\mathcal{B}' = \{1,x,x^2,\cdots,x^{d+e-1}\}$$

Then we have:

$$[T]_{\mathcal{B}}^{\mathcal{B}'} = \big([T(1,0)]_{\mathcal{B}'} \cdots [T(x^{d-1},0)]_{\mathcal{B}'} \cdots [T(0,x^{e-1})]_{\mathcal{B}'}\big)$$

Suppose that:

$$f(x) = \sum_{0 \le i \le d} b_i x^i \text{ and } g(x) = \sum_{0 \le j \le e} a_j x^j$$

Then we have:

$$[T] = \begin{pmatrix} a_0 & 0 & \cdots & 0 & b_0 & 0 & \cdots & 0 \\ a_1 & a_0 & \cdots & 0 & b_1 & b_0 & \cdots & 0 \\ a_2 & a_1 & \ddots & 0 & b_2 & b_1 & \ddots & 0 \\ \vdots & \vdots & \ddots & a_0 & \vdots & \vdots & \ddots & b_0 \\ a_e & a_{e-1} & \cdots & \vdots & b_d & b_{d-1} & \cdots & \vdots \\ 0 & a_e & \cdots & \vdots & 0 & b_d & \ddots & \vdots \\ \vdots & \vdots & \ddots & a_{e-1} & \vdots & \vdots & \ddots & b_{d-1} \\ 0 & 0 & \cdots & a_e & 0 & 0 & \cdots & b_d \end{pmatrix}$$

Example. Let $f(x) = x^2 + 1$ and $g(x) = x^2 + 3$, then:

$$R(x^2+1, x^2-3) = \det \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 3 & 0 & -1 & 0 \\ 0 & 3 & 0 & 1 \end{pmatrix} = \det \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & -4 & 0 \\ 0 & 0 & 0 & -4 \end{pmatrix} = 16$$

Lecture 11, 2024/05/29

Theorem 1.27. Let f, g be nonconstant polynomials over an algebraically closure and write:

$$f(x) = a_0(x-\alpha_1)\cdots(x-\alpha_d)$$
$$g(x) = b_0(x-\beta_1)\cdots(x-\beta_e)$$

Then we have:

$$R(f,g) = a_0^e b_0^d \prod_{i,j}(\alpha_i - \beta_j) \tag{1}$$

Proof: WLOG suppose $a_0 = b_0 = 1$. Consider both sides of (1) as polynomials in $\{\alpha_i\} \cup \{\beta_j\}$. Both sides are 0 $\iff$ $\alpha_i = \beta_j$ for some i, j. This means $(\alpha_i - \beta_j) \mid R(f, g)$ for all i and j. (If we view $R(f, g)$ as a polynomial in α_i, then β_j is a root iff $(\alpha_i - \beta_j) \mid R(f, g)$). Both sides have same degree and RHS divides LHS, so they differ by a constant 1. □

Recall that our goal is to prove Theorem 1.25, let us know prove it.

Proof: Let $n = \deg(m(x))$. We have:

$$R(m, m') = \lambda \prod_{i,j} (\alpha_i - \beta_j)$$

where α_i are roots of $m(x)$ and β_j are roots of $m'(x)$. Then:

$$R(m, m') = \prod_i \prod_j (\alpha_i - \beta_j) = \prod_i m'(\alpha_i)$$

However we have:

$$m'(x) = \frac{m(x)}{x - \alpha_1} + \cdots + \frac{m(x)}{x - \alpha_n}$$

It implies:

$$m'(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j)$$

Thus:

$$R(m, m') = \prod_i \underbrace{\prod_{j \neq i} (\alpha_i - \alpha_j)}_{*}$$

The difference of $(*)$ and $\prod_{i<j} (\alpha_i - \alpha_j)^2$ is the number of minus signs, and there are $\binom{n}{2}$ ways. Hence we can conclude that:

$$R(m, m') = (-1)^{\binom{n}{2}} \prod_{i<j} (\alpha_i - \alpha_j)^2$$

As desired. □

Example. Let us compute the discriminant of $\mathbb{Z}[i]$. Using the old way we have:

$$\operatorname{disc} \mathbb{Z}[i] = \operatorname{disc}(1, i) = \det \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}^2 = (-2i)^2 = -4$$

Using the new method we have:

$$\operatorname{disc} \mathbb{Z}[i] = \operatorname{disc}(x^2 + 1) = (-1)^1 \det \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 1 & 0 & 2 \end{pmatrix} = -4$$

Let us find the general formula for the discriminant of quadratic and cubic polynomials.

Let $m(x) = x^2 + bx + c$, then $m'(x) = 2x + b$. We have:

$$\begin{aligned}\operatorname{disc}(x^2 + bx + c) = -R(x^2 + bx + c, 2x + b) = \det\begin{pmatrix} c & b & 0 \\ b & 2 & b \\ 1 & 0 & 2 \end{pmatrix} \\ = -(4c + b^2 - 2b^2) = b^2 - 4c\end{aligned}$$

Let $m(x) = x^3 + ax^2 + bx + c$, then $m'(x) = 3x^2 + 2ax + b$. We have:

$$\begin{aligned}\operatorname{disc}(x^3 + ax^2 + bx + c) &= (-1)R(x^3 + ax^2 + bx + c, 3x^2 + 2ax + b) \\ &= -\det\begin{pmatrix} c & 0 & b & 0 & 0 \\ b & c & 2a & b & 0 \\ a & b & 3 & 2a & b \\ 1 & a & 0 & 3 & 2a \\ 0 & 1 & 0 & 0 & 3 \end{pmatrix} \\ &= a^2b^2 - 4a^3c + 18abc - 4b^3 - 27c^2\end{aligned}$$

If there is no x^2 term, we have:

$$\operatorname{disc}(x^3 + bx + c) = -4b^3 - 27c^2$$

Lecture 12, 2024/05/31

2 Ideal Factorization

2.1 Prime Ideals

What are ideals of $\mathcal{O}_K$? It is complicated, but we will start by figuring out what $\mathcal{O}_K/I$ looks like for nonzero ideals $I \subseteq \mathcal{O}_K$.

We already know that $\mathcal{O}_K/I$ is a finite ring. It is also a Noetherian ring, so every prime ideal of $\mathcal{O}_K/I$ is maximal.

Definition. If I, J are ideals of a ring R, then IJ is the ideal generated by:

$$\{xy : x \in I, y \in J\}$$

Example. If $R = \mathbb{Z}$ and $I = (a)$ and $J = (b)$, then $IJ = (ab)$.

Example. If $R = \mathbb{R}[x,y]$ and $I = (x, y^2)$ and $J = (x^2, y)$. Then an element of IJ is a $\mathbb{R}$-linear combination of elements of the form:

$$\begin{aligned}(xp + y^2q)(x^2r + yt) &= x^3pr + x^2y^2qr + xypt + y^3qt \\ &= x^3(pr) + xy(xyqr + pt) + y^3(qt)\end{aligned}$$

Therefore $IJ = (x^3, xy, x^2y^2, y^3) = (x^3, xy, y^3)$.

In general, we have:

$$(a_1, \cdots, a_r)(b_1, \cdots, b_t) = (a_ib_j)$$

where the last ideal is generated by a_ib_j for $1 \le i \le r$ and $1 \le j \le t$.

Theorem 2.1. Let $I \subseteq \mathcal{O}_K$ be a nonzeroideal and $I \neq (1)$. Then there are prime ideals $P_1, \cdots, P_r$ of $\mathcal{O}_K$ such that:

$$\mathcal{O}_K/I \cong (\mathcal{O}_K/P_1^{a_1}) \times \cdots \times (\mathcal{O}_K/P_r^{a_r})$$

for $a_i \ge 1$ and $P_i \neq P_j$ for $i \neq j$.

Lemma 2.2. Let R be a finite ring, then there are prime ideals $P_1, \cdots, P_r$ of R such that:

$$P_1 \cdots P_r = 0$$

Proof: We will show that, for any ideal $I \subseteq R$, there are prime ideals $P_1, \cdots, P_r$ such that $P_1 \cdots P_r \subseteq I$. We want to induce on $\#I$, but the case we want is $\#I = 0$, so we induce on $\#R - \#I$. The base case $I = R$ is trivial. Now consider I, if I is prime then pick $P_1 = I$ and we are done. If not, pick $a, b \notin I$ but $ab \in I$, then:

$$\begin{aligned}I + aR &\supseteq Q_1 \cdots Q_u \\ I + bR &\supseteq Q_1' \cdots Q_t'\end{aligned}$$

where Q_i and Q_j' are all primes, by induction (since $I + aR$ and $I + bR$ are strictly bigger than I). Therefore:

$$\begin{aligned}Q_1 \cdots Q_u Q_1' \cdots Q_t' &\subseteq (I + aR)(I + bR) \\ &= I^2 + aI + bI + abR \subseteq I\end{aligned}$$

the abR is contained in I as $ab \in I$. As desired. □

Proof of Theorem 2.1: By the lemma, since $\mathcal{O}_K/I$ is finite, we have prime ideals $\overline{P_1}, \cdots, \overline{P_r}$ in $\mathcal{O}_K/I$ such that:

$$\overline{P_1} \cdots \overline{P_r} = 0$$

Let P_i be the lifting of $\overline{P_i}$, that is, $P_i = \pi^{-1}(\overline{P_i})$ where π is the reduction mod I map. Explicity:

$$P_i = \{x \in \mathcal{O}_K : x + I \in \overline{P_i}\}$$

If $\overline{P}$ is prime in $\mathcal{O}_K/I$, then:

$$\overline{P_1} \cdots \overline{P_r} \subseteq \overline{P}$$

implies that $\overline{P_i} \subseteq \overline{P}$ for some i. Also, since $\mathcal{O}_K/I$ is finite, both $\overline{P_i}$ and $\overline{P}$ are maximal, hence $\overline{P} = \overline{P_i}$. So every prime ideal of $\mathcal{O}_K/I$ is equal to $\overline{P_i}$ for some i. By the Chinese Remainder Theorem:

$$\begin{aligned}\mathcal{O}_K/I &\cong (\mathcal{O}_K/I)/\overline{P_1}^{a_1} \times \cdots \times (\mathcal{O}_K/I)/\overline{P_r}^{a_r} \\ &\cong (\mathcal{O}_K/P_1^{a_1}) \times \cdots \times (\mathcal{O}_K/P_r^{a_r})\end{aligned}$$

As desired. □

Lecture 13, 2024/06/03

Now, what are prime ideals of $\mathcal{O}_K$? Say $P \subseteq \mathcal{O}_K$ is a nonzero prime ideal, then $P \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ (this must be nonzero by a homework). So $P \cap \mathbb{Z} = p\mathbb{Z}$ for some prime $p \in \mathbb{Z}$. But P is always maximal, so $\mathcal{O}_K/P$ is a finite field. Also, $\mathcal{O}_K/P$ is a module over $\mathbb{F}_p$. We can add and subtract in the usual way, and multiplication by $\mathbb{F}_p$ is defined by:

$$(n + p\mathbb{Z})(\alpha + P) = n\alpha + P$$

this is well-defined because $p \in P$.

Example. Let $K = \mathbb{Q}(\sqrt{2})$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$. What are prime ideals of $\mathcal{O}_K$ that contain 5?

$$\mathcal{O}_K/(5) = \mathbb{Z}[\sqrt{2}]/(5) \cong \mathbb{Z}[x]/(x^2 - 2, 5) \cong \mathbb{F}_5[x]/(x^2 - 2)$$

Since $x^2 - 2$ has no roots mod 5, we know $x^2 - 2$ is irreducible in $\mathbb{F}_5[x]$ as it is quadratic, $\mathbb{F}_5[x]/(x^2 - 2) \cong \mathbb{F}_{25}$ is a finite field with 25 elements. Thus (5) is a prime ideal in $\mathcal{O}_K$. Since (5) is already prime, it must be the only prime ideal that contains 5, as all prime ideals are maximal.

Example. Let $K = \mathbb{Q}(\sqrt{2})$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$ again. What are prime ideals that contain 7?

$$\begin{aligned}\mathcal{O}_K/(7) &= \mathbb{Z}[\sqrt{2}]/(7) \\ &\cong \mathbb{Z}[x]/(x^2 - 2, 7) \\ &\cong \mathbb{F}_7[x]/(x^2 - 2) \\ &\cong \mathbb{F}_7[x]/(x-3)(x+3)\end{aligned}$$

Note that $(x-3)$ and $(x+3)$ are coprime ideals, since $-1=(x+3)-(x-3)\in\mathbb{F}_7[x]^*$, thus by the Chinese Remainder Theorem:

$$\begin{aligned}\mathcal{O}_K/(7)&\cong\mathbb{F}_7[x]/(x-3)\times\mathbb{F}_7[x]/(x+3)\\&\cong\mathbb{F}_7\times\mathbb{F}_7\end{aligned}$$

The prime ideals of $\mathbb{Z}[\sqrt{2}]$ containing (7) corresponds to the prime ideals of $\mathbb{Z}[\sqrt{2}]/(7)$. The only two prime ideals of $\mathbb{F}_7\times\mathbb{F}_7$ are $((1,0))$ and $((0,1))$. Let's see which prime ideal in $\mathcal{O}_K/(7)$ corresponds to $((1,0))$ in $\mathbb{F}_7\times\mathbb{F}_7$ through these isomorphisms.

$$((1,0))\subseteq\mathbb{F}_7\times\mathbb{F}_7$$

corresponds to:

$$((1,0))\subseteq\mathbb{F}_7[x]/(x-3)\times\mathbb{F}_7[x]/(x+3)$$

Then, we want to its corresponding ideal in $\mathbb{F}_7[x]/(x^2-2)$. Recall that this map is using the Chinese Remainder Theorem by $p(x)\mapsto(p(x)+(x+3),p(x)+(x-3))$, so we need $p(x)\in\mathbb{F}_7[x]$ such that:

$$p(x)\equiv1\pmod{x-3}\quad\text{and}\quad p(x)\equiv0\pmod{x+3}$$

Write $p(x)=q(x)(x+3)$ and we choose $\deg p(x)\le1$, so $q(x)=\lambda$ for some λ. So $p(x)=\lambda(x+3)$ and $p(3)=1$, so $\lambda=-1$, so the ideal $((1,0))$ corresponds to:

$$(-x-3)=(x+3)\subseteq\mathbb{F}_7[x]/(x^2-2)$$

This corresponds to $(\sqrt{2}+3)$ in $\mathbb{Z}[\sqrt{2}]/(7)$ by $x\mapsto\sqrt{2}$, and corresponds to $(\sqrt{2}+3,7)$ in $\mathbb{Z}[\sqrt{2}]$. The other ideal is $(\sqrt{2}-3,7)$ by similar technique.

Example. What are prime ideals of $\mathbb{Z}[\sqrt{2}]$ that contain 2?

$$\mathbb{Z}[\sqrt{2}]/(2)\cong\mathbb{F}_2[x]/(x^2-2)\cong\mathbb{F}_2[x]/(x^2)$$

It is not hard to show that the only prime ideal of $\mathbb{F}_2[x]/(x^2)$ is (x), so $(\sqrt{2},2)$ is the only prime ideal of $\mathbb{Z}[\sqrt{2}]$ that contains 2.

Let $m(x)$ be the minimal polynomial of $\alpha\in\mathcal{O}_K$. In general, the prime ideals of $\mathbb{Z}[\alpha]$ that contain p is computed this way:

$$\begin{aligned}\mathbb{Z}[\alpha]/(p)=\mathbb{Z}[x]/(m(x),p)&\cong\mathbb{F}_p[x]/(m(x))\\&\cong\mathbb{F}_p[x]/(m_1(x)^{a_1}\cdots m_r(x)^{a_r})\\&\cong\mathbb{F}_p[x]/(m_1(x)^{a_1})\times\cdots\times\mathbb{F}_p[x]/(m_r(x)^{a_r})\end{aligned}$$

where $m_1(x), \cdots, m_r(x)$ are distinct irreducible factors of $m(x)$ mod p. Thus, by the similar tricks from above, the prime ideals of $\mathbb{Z}[\alpha]$ containing p are:

$$P = (p, m_i(\alpha))$$

for $i = 1, \cdots, r$.

Lecture 14, 2024/06/05

2.2 Fractional Ideals

Note that $10 = 2 \cdot 5 = \sqrt{10} \cdot \sqrt{10}$, then:

$$N(10) = 100,\ N(2) = 4,\ N(5) = 25,\ N(\sqrt{10}) = 10$$

We cannot factor this further: For example, if $a+b\sqrt{10}$ has norm 2, then $N(a+b\sqrt{10}) = a^2 - 10b^2 = 2$ has no solutions in $\mathbb{Z}$. This means $2, 5, \sqrt{10}$ are not pairwise associated to each other. Therefore $\mathbb{Z}[\sqrt{10}]$ is not a UFD.

But it will turn out that we can factor a nonzero ideal of $\mathcal{O}_K$ into a product of prime ideals. Moreover, this factorization will be unique up to permutaion.

Recall that when we factor an integer, we first find a prime number that divide it and we divide it by that prime to get a smaller integer, and we continue this until we get 1. For ideals, suppose we start from I, we want to find a prime ideal P containing I, then "divide" I by P to get a bigger ideal, and continue doing this until we get the ideal (1).

So what does "divide" mean?

Definition. Let D be a Noetherian domain with fraction field K. A **fractional ideal** of D is a finitely generated D-submodule of K. An **integral ideal** of D is a finitely generated D-submodule of D! (That is, a normal ideal).

Example. Let $K = \mathbb{Q}$ and $D = \mathbb{Z}$. Let $I = a_1\mathbb{Z} + \cdots + a_r\mathbb{Z}$ with $a_i \in \mathbb{Q}$. Then $I = a\mathbb{Z}$ where $a = \gcd(a_1, \cdots, a_r) =$ the largest rational number such that each a_i is an integer multiple of a. For example:

$$\left(\frac{1}{2}\right)\mathbb{Z} + \left(\frac{2}{3}\right)\mathbb{Z} = \left(\frac{1}{6}\right)\mathbb{Z}$$

Therefore, all fractional ideals of $\mathbb{Z}$ are $\frac{a}{b}\mathbb{Z}$ for some $\frac{a}{b} \in \mathbb{Q}$.

Definition. Let I, J be fractional ideals in D, the **ideal quotient** of I by J is:

$$(I : J) = \{a \in K : aJ \subseteq I\}$$

Example. In $\mathbb{Z}$, we have:

$$(6\mathbb{Z} : 3\mathbb{Z}) = \{a \in \mathbb{Q} : (3a) \subseteq (6)\} = \{a \in \mathbb{Q} : 3a \in 6\} = 2\mathbb{Z}$$

And in general, we have:

$$(m\mathbb{Z} : n\mathbb{Z}) = \left(\frac{m}{n}\right)\mathbb{Z}$$

Theorem 2.3. If $J \neq 0$, then $(I : J)$ is a fractional ideal of D.

Proof: It is clear that $(I : J)$ is a D-submodule of K. Need to show that it is finitely generated. Note taht there is some $0 \neq a \in D$ such that $aI \subseteq D$ and $aJ \subseteq D$. So, WLOG suppose that $I, J \subseteq D$. Then we have:

$$(I : J) \subseteq (D : J) \subseteq (D : \alpha D)$$

for any $0 \neq \alpha \in J$. But $(D : \alpha D) = (1/\alpha)$ is finitely generated, so $(I : J) \subseteq (1/\alpha)$ is finitely generated as D is Noetherian. □

Example. If $D = \mathbb{Z}[\sqrt{10}]$ and $I = (2, \sqrt{10})$, then:

$$\begin{aligned}(D : I) &= \{a + b\sqrt{10} \in \mathbb{Q}(\sqrt{10}) : (a + b\sqrt{10})I \subseteq D\} \\ &= \left\{ a + b\sqrt{10} \in \mathbb{Q}(\sqrt{10}) : \begin{array}{c} (a + b\sqrt{10})2 \in D \\ (a + b\sqrt{10})\sqrt{10} \in D \end{array} \right\}\end{aligned}$$

And we have $2a + 2b\sqrt{10} \in D$ and $10b + a\sqrt{10} \in D$, which means:

$$2a, 2b, 10b, a \in \mathbb{Z}$$

Thus $a \in \mathbb{Z}$ and $2b \in \mathbb{Z}$, so:

$$(D : I) = \left\{ a + \frac{b}{2}\sqrt{10} : a, b \in \mathbb{Z} \right\} = \left(1, \frac{\sqrt{10}}{2}\right)$$

Lecture 15, 2024/06/07

To check this computation is correct, note that $(D : I) = ((1) : I)$ looks like 1 divide by I, so let us check what is $(D : I) \cdot I$:

$$(D : I)I = \left(1, \frac{\sqrt{10}}{2}\right)(2, \sqrt{10}) = (2, \sqrt{10}, \sqrt{10}, 5) = (1)$$

Now, let us try to factor the ideal (2) in $\mathbb{Z}[\sqrt{10}]$ in two ways:

$$\mathbb{Z}[\sqrt{10}]/(2) \cong \mathbb{F}_2[x]/(x^2)$$

Therefore $(2) = (2, \sqrt{10})^2$. We can also do it this way: We divide (2) by the prime ideal $I = (2, \sqrt{10})$ to get:

$$(2) \cdot (D : (2, \sqrt{10})) = (2) \cdot \left(1, \frac{\sqrt{10}}{2}\right) = (2, \sqrt{10})$$

Now we want to multiply by the "inverse" of $(D : (2, \sqrt{10}))$ both side. We have:

$$\left(D : \left(1, \tfrac{\sqrt{10}}{2}\right)\right) = \left\{a + b\sqrt{10} : \begin{array}{c} a + b\sqrt{10} \in D \\ (a + b\sqrt{10})\tfrac{\sqrt{10}}{2} \in D \end{array}\right\}$$

We need $a, b \in \mathbb{Z}$ with $\frac{a}{2} \in \mathbb{Z}$ and $5b \in \mathbb{Z}$, so:

$$J = (D : (1, \tfrac{\sqrt{10}}{2})) = \{2a + b\sqrt{10} : a, b \in \mathbb{Z}\} = (2, \sqrt{10})$$

Multiply by it on both sides, the $(D : (2, \sqrt{10}))$ becomes (1), thus:

$$(2) = (2, \sqrt{10})(2, \sqrt{10}) = (2, \sqrt{10})^2$$

which is the same as the factorization using the old method.

Example. Let $D = \mathbb{Z}[\sqrt{5}]$ and $P = (2, 1 + \sqrt{5})$, then:

$$\begin{aligned} D/P &= \mathbb{Z}[\sqrt{5}]/(2, 1 + \sqrt{5}) \\ &\cong \mathbb{Z}[x]/(x^2 - 5, 2, 1 + x) \\ &\cong \mathbb{F}_2[x]/(x^2 - 5, 1 + x) \\ &\cong \mathbb{F}_2[x]/(1 + x) \\ &\cong \mathbb{F}_2 \end{aligned}$$

Therefore P is a prime ideal. Then:

$$(D : P) = \left\{a + b\sqrt{5} \in \mathbb{Q}(\sqrt{5}) : \begin{array}{c} 2(a + b\sqrt{5}) \in D \\ (a + b\sqrt{5})(1 + \sqrt{5}) \in D \end{array}\right\}$$

We need $2a, 2b, a + 5b, a + b \in \mathbb{Z}$, which is equivalent to $a = \frac{m}{2}$ and $b = \frac{k}{2}$ with $m \equiv k \pmod 2$. Therefore:

$$\begin{aligned} (D : P) &= \left\{\frac{m}{2} + \frac{k}{2}\sqrt{5} : m \equiv k \ (\text{mod } 2)\right\} \\ &= \left\{m\left(\frac{1}{2}\right) + (m + 2\ell)\left(\frac{\sqrt{5}}{2}\right) : m, \ell \in \mathbb{Z}\right\} \\ &= \left\{m\left(\frac{1 + \sqrt{5}}{2}\right) + \ell\sqrt{5} : m, l \in \mathbb{Z}\right\} \\ &= \left(\frac{1 + \sqrt{5}}{2}, \sqrt{5}\right) \end{aligned}$$

However:

$$\begin{aligned} P\cdot(D:P) &= (2,1+\sqrt{5})\left(\frac{1+\sqrt{5}}{2},\sqrt{5}\right) \\ &= (1+\sqrt{5},3+2\sqrt{5},2\sqrt{5},5+\sqrt{5}) \\ &= (1+\sqrt{5},3+\sqrt{5}) \\ &= (1+\sqrt{5},2) \\ &= P \end{aligned}$$

This means we cannot divide by P, suppose we divide I by P, then $I(D:P)=J$ and multiplying by P gives $I\neq IP=JP$. This is because $\mathbb{Z}[\sqrt{5}]$ is NOT the ring of integers of $\mathbb{Q}(\sqrt{5})$!

Lecture 16, 2024/06/10

Proposition 2.4. Fractional ideals of K are isomorphic to $\mathbb{Z}^d$ where $d=[K:\mathbb{Q}]$.

Last time we saw the plan of dividing prime ideals does not work for $\mathbb{Z}[\sqrt{5}]$. The property that $\mathbb{Z}[\sqrt{5}]$ does not have is being integrally closed.

Theorem 2.5. Let K be a number field and $\mathcal{O}_K$ its ring of integers. Let $P\subseteq\mathcal{O}_K$ be a prime ideal, then $P(\mathcal{O}_K:P)=\mathcal{O}_K$.

Lemma 2.6. Let R be a Noetherian ring and $I\subseteq R$ an ideal. Then there are prime ideals $P_1,\cdots,P_r$ with $P_1\cdots P_r\subseteq I$.

Proof: Since R is Noetherian, suppose the lemma is wrong, there is some ideal I of R that is maximal with respect to the property that no product of prime ideals is contained in I. Then I is not prime, so $a,b\notin I$ but $ab\in I$, then:

$$(I+aR)(I+bR)\subseteq I$$

but each $I+aR$ and $I+bR$ is a product of prime ideals, contradiction. □

Proof of Theorem 2.5: First, $P(\mathcal{O}_K:P)$ is a fractional ideal. And $P(\mathcal{O}_K:P)\subseteq P$ by definition. Therefore $P(\mathcal{O}_K:P)$ is an integral ideal. Also, $P\subseteq P(\mathcal{O}_K:P)$ as $1\in(\mathcal{O}_K:P)$. Since P is maximal, so $P(\mathcal{O}_K:P)$ is either $\mathcal{O}_K$ or P. If $P(\mathcal{O}_K:P)=\mathcal{O}_K$, we are done. Suppose $P(\mathcal{O}_K:P)=P$, then:

Claim: $(\mathcal{O}_K:P)$ is a ring. (Warning: In real life $(\mathcal{O}_K:P)$ is never a ring, because in real life $P(\mathcal{O}_K:P)=P$ is never true!)

Proof (Claim): It is clear that $(\mathcal{O}_K:P)$ is closed under addition and subtraction and contains 0 and 1. It is enough to show that it is closed under multiplication. Let $a,b\in(\mathcal{O}_K:P)$, then we want to show $ab \in (\mathcal{O}_K : P)$, that is, $abP \subseteq \mathcal{O}_K$. Indeed, we have:

$$abP = a(bP) \subseteq aP \subseteq \mathcal{O}_K$$

here $bP \subseteq P$ as $b \in (\mathcal{O}_K : P)$ and $P(\mathcal{O}_K : P) = P$ by assumption. (QED Claim)

So $(\mathcal{O}_K : P)$ is a ring and it contains $\mathcal{O}_K$ and integral over $\mathcal{O}_K$. Since $\mathcal{O}_K$ is integrally closed and $(\mathcal{O}_K : P) \subseteq K$, we get $(\mathcal{O}_K : P) = \mathcal{O}_K$. Since $P \neq 0$, chooe $0 \neq \alpha \in P$. By Lemma 2.6, there are prime ideals $P_1, \cdots, P_r$ such that:

$$P_1 \cdots P_r \subseteq (\alpha)$$

here we can choose r to be minimal. Then $P_1 \cdots P_r \subseteq P$ as $\alpha \in P$. Since P is prime, we have $P_i = P$ for some i. WLOG suppose $P_1 = P$. Let:

$$J = P_2 \cdots P_r$$

Then $J \not\subseteq (\alpha)$ by minimality of r. Choose $y \in J \setminus (\alpha)$. Then:

$$yP \subseteq JP = JP_1 \subseteq (\alpha)$$

Therefore $(y/\alpha)P \subseteq \mathcal{O}_K$ and $y/\alpha \in (\mathcal{O}_K : P)$. Since $y \notin (\alpha)$, we get $y/\alpha \notin \mathcal{O}_K$, thus $(\mathcal{O}_K : P) \neq \mathcal{O}_K$, contradiction. □

This theorem allows us to confidently call $(\mathcal{O}_K : P)$ the inverse of P, since we have seen that $P(1 : P) = (1) = \mathcal{O}_K$, here 1 is the unit ideal (1).

Definition. For $I \subseteq \mathcal{O}_K$ nonzero ideal, we define the **inverse** of I to be $I^{-1} = (\mathcal{O}_K : I)$. We have seen that if $I = P$ is prime, then $PP^{-1} = (1) = \mathcal{O}_K$. In fact, it is also true for a general ideal I.

2.3 Factorization of Ideals

Recall that our plan to factor an ideal is to find a proper prime ideal containing I and divide by it, then continue.

How do we know which prime ideals to divide by? Let $I \subseteq \mathcal{O}_K$ be a nonzero ideal. There is some maximal ideal M that contains I. (This fact is true for a general ring under the assumption of Zorn's Lemma, but since $\mathcal{O}_K$ is Noetherian, we do not need Zorn's Lemma). Let $P = M$, and compute:

$$IP^{-1} = I(\mathcal{O}_K : P) \subseteq \mathcal{O}_K$$

and $I \subseteq IP^{-1}$ as $1 \in (\mathcal{O}_K : P)$. Once we have this, we can factor $IP^{-1} = Q_1 \cdots Q_t$, then multiply by P gives $I = PQ_1 \cdots Q_t$.

Lecture 17, 2024/06/12

Theorem 2.7. Let K be a number field with ring of integers $\mathcal{O}_K$. Let $I \subseteq \mathcal{O}_K$ be a nonzero ideal. Then I can be factored uniquely (up to permutation of factors) as:

$$I = P_1 \cdots P_r$$

where P_i are prime ideals of $\mathcal{O}_K$ (not necessarily distinct).

Lemma 2.8 (Nakayama). Let A be a ring and M a finitely generated A-module and $I \subseteq A$ an ideal. If $IM = M$, then there is some $a \in A$ with $a \equiv 1 \pmod{I}$ such that $aM = 0$.

Proof: Write $M = x_1A + \cdots + x_nA$ for some $x_1, \cdots, x_n \in M$. $IM = M$ implies that for each i, we have:

$$x_i = a_{1i}x_1 + \cdots + a_{ni}x_n \tag{1}$$

where $A_{ji} \in I$ for all i and j. Let:

$$B = I_n - (a_{ij})$$

Cramer's Rule implies there is a matrix B^* with entries in A with:

$$BB^* = (\det B)I_n$$

Define $a = \det B$ and note that $a \equiv 1 \pmod{I}$. Write $B^* = (c_{ij})$, then:

$$a\delta_{ik} = \sum_{j=1}^{n} c_{ij}(\delta_{kj} - a_{kj})$$

where δ_{ik} is the **Kronecker Delta** defined by:

$$\delta_{ik} = \begin{cases} 1 & \text{if } i = k \\ 0 & \text{if } i \neq k \end{cases}$$

Then we have:

$$\sum_{k=1}^{n}\sum_{j=1}^{n} c_{ij}(\delta_{kj} - a_{kj})x_k = \sum_{k=1}^{n} a\delta_{ik}x_k = ax_i$$

But the LHS is:

$$\begin{aligned}\sum_{j=1}^{n}\sum_{k=1}^{n} c_{ij}(\delta_{kj} - a_{kj})x_k &= \sum_{j=1}^{n}\left[\sum_{k=1}^{n} c_{ij}\delta_{kj}x_k - \sum_{k=1}^{n} c_{ij}a_{jk}x_k\right] \\ &= \sum_{j=1}^{n} c_{ij}\left(x_j - \sum_{k=1}^{n} a_{kj}x_k\right) \\ &= 0 && \text{(by (1))}\end{aligned}$$

Therefore $ax_i = 0$ for all i, thus $aM = 0$. □

Proof of Theorem 2.7: Let M be a maximal ideal that contains I. Let $P_1 = M$, then IP_1^{-1} is a subset of $\mathcal{O}_K$ that contains I, so we call it $I_1 = IP_1^{-1}$. Then I_1 is a nonzero ideal of $\mathcal{O}_K$. If $I_1 = \mathcal{O}_K$ then $I = P_1$ and we are done. Otherwise, let P_2 be a maximal ideal containing I, and let $I_2 = I_1P_2^{-1}$. Continue this way, we get an ascending chain:

$$I \subseteq I_1 \subseteq I_2 \subseteq \cdots$$

of ideals. Let $J = \bigcup_{n=1}^{\infty} I_n$, then J is an ideal of $\mathcal{O}_K$, so it is finitely generated as $\mathcal{O}_K$ is Noetherian. Write $J = (a_1, \cdots, a_r)$. Each $a_i \in I_{n_i}$ for some n_i, so there is I_m that contains all a_i. So $I_m = J$ and thus $I_{m+1} = I_m$, then:

$$I_{m+1} = I_mP_{m+1}^{-1} = I_m \implies I_m = I_mP_{m+1}$$

By Nakayama, there is $a \in \mathcal{O}_K$ with $a \equiv 1 \pmod{P_{m+1}}$ such that $aI_m = 0$. But this is impossible, so our process must have stopped with $I_m = \mathcal{O}_K$ for some m, thus $I = P_1 \cdots P_m$ as desired.

For uniqueness, say $P_1 \cdots P_r = Q_1 \cdots Q_t$ for nonzero prime ideals P_i and Q_j. They are all maximal and Q_t contains some P_i implies $Q_t = P_i$. So we can divide them on both side and one side becomes $\mathcal{O}_K$. That is, we can run out of P_i or Q_j, but if this happens, then we must run out of both P_i and Q_j together, otherwise we have a product of nonzero number of prime ideals equal to (1). □

Lecture 18, 2024/06/14

Example. Factor $(2-\sqrt{10})$ in $\mathbb{Z}[\sqrt{10}]$. Note that $(2-\sqrt{10})$ contains $(2-\sqrt{10})(2+\sqrt{10}) = -6$ and $-6 = -2 \cdot 3$. Therefore $(2-\sqrt{10})$ must be contained in two prime ideals such that one contains 2 and one contains 3. We know from a previous example that:

$$(2) = (2, \sqrt{10})^2$$

Since $2 - \sqrt{10} \in (2, \sqrt{10})$, let us divide $(2-\sqrt{10})$ by $(2, \sqrt{10})$.

$$(2, \sqrt{10})^{-1} = \left(1, \frac{\sqrt{10}}{2}\right)$$

Therefore:

$$\begin{aligned}(2-\sqrt{10})(2, \sqrt{10})^{-1} &= (2-\sqrt{10})\left(1, \frac{\sqrt{10}}{2}\right)\\ &= (2-\sqrt{10}, \sqrt{10}-5)\\ &= (2-\sqrt{10}, 3)\end{aligned}$$

If $(2-\sqrt{10},3)$ is a prime ideal, then we stop. Is it prime?

$$\begin{aligned}\mathbb{Z}[\sqrt{10}]/(2-\sqrt{10},3) &\cong \mathbb{Z}[x]/(x^2-10,3,2-x)\\ &\cong \mathbb{F}_3[x]/(2-x,x^2-10)\\ &\cong \mathbb{F}_3[x]/(6)\\ &\cong \mathbb{F}_3\end{aligned}$$

Therefore $(2-\sqrt{10},3)$ is maximal, thus:

$$(2-\sqrt{10})=(2,\sqrt{10})(3,2-\sqrt{10})$$

is the factorization into prime ideals.

3 Localization and DVR

3.1 Localization

Definition. Let D be a domain and $S\subseteq D\setminus 0$ be any subset. The **localization** of D at S is $D[S^{-1}]$ where $S^{-1}=\{\frac{1}{s}:s\in S\}$. That is, $D[S^{-1}]$ is the smallest subring of K (fraction field of D) that contains D and S^{-1}.

Example. $\mathbb{Z}$ localized at $\{6\}$ is $\mathbb{Z}[\frac{1}{6}]=\mathbb{Z}[\frac{1}{2},\frac{1}{3}]$.

Example. $\mathbb{C}[x]$ localized at x is $\mathbb{C}[x,\frac{1}{x}]$ is all rational functions on $\mathbb{C}$ that are defined everywhere except maybe at 0.

In general, we localize at a prime ideal. Let D be a domain and $P\subseteq D$ a prime ideal. The localization of D at P is the localization of D at $D\setminus P$.

$$D_P=D[(D\setminus P)^{-1}]=\left\{\frac{a}{b}:a,b\in D,\ b\notin P\right\}$$

There are plenty of $a/b\in D_P$ with $b\in P$. This is because there are some ways of writing a/b with $b\in P$. To show $a/b\in D_P$, it suffices to find such representation. To show $a/b\notin D_P$, we have to show no such expression a/b with $b\in P$ exists.

Example. Let $D=\mathbb{Z}$ and $P=(2)$. Then:

$$D_P=\mathbb{Z}_{(2)}=\left\{\frac{a}{b}:a,b\in\mathbb{Z},\ 2\nmid b\right\}$$

Note that $14/10\in\mathbb{Z}_{(2)}$ because $14/10=7/5$.

Example. Let $D = \mathbb{C}[x]$ and $P = (x)$. Then:

$$D_P = \mathbb{C}[x]_{(x)} = \left\{ \frac{p(x)}{q(x)} : q(x) \notin (x) \right\} = \left\{ \frac{p(x)}{q(x)} : q(0) \neq 0 \right\}$$
$$= \text{all rational functions that are defined at } 0$$

Example. $D_{(0)}$ is the whole fraction field, because we are inverting every nonzero element in D.

Note that the units of D_P are:

$$D_P^\times = \left\{ \frac{a}{b} : a, b \in D,\ a, b \notin P \right\}$$

Therefore, the non-units are exactly:

$$\left\{ \frac{a}{b} : a, b \in D,\ a \in P,\ b \notin P \right\} = PD_P = (P)$$

which is an ideal of D_P.

Definition. A **local ring** is a ring with a unique maximal ideal.

D_P is a local ring for prime ideals $P \subsetneq D$: It has a maximal ideal PD_P, the set of all non-units. Since every maximal ideal of D_P cannot contain units, so they are all contained in PD_P. Then by maximality, they are all equal to PD_P.

Lecture 19, 2024/06/17

3.2 Discrete Valution Rings

Definition. A **Discrete Valution Ring (DVR)** is a Noetherian domain whose maximal ideal is nonzero and principal. Any generator of the maximal ideal is called a **uniformizer**.

Example. Consider $\mathbb{Z}$ localized at (5):

$$\mathbb{Z}_{(5)} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z},\ b \notin (5) \right\}$$

The unique maximal ideal is:

$$\left\{ \frac{a}{b} : a, b \in \mathbb{Z},\ a \in (5),\ b \notin (5) \right\} = \left\{ 5 \cdot \frac{a}{b} : a, b \in \mathbb{Z},\ b \notin (5) \right\} = 5\mathbb{Z}_{(p)}$$

Therefore the unique maximal ideal is (5) in $\mathbb{Z}_{(5)}$, which is principal!

Example. Consider $\mathbb{C}[x]$ localized at (x):

$$\mathbb{C}[x]_{(x)} = \left\{ \frac{p(x)}{q(x)} : q(0) \neq 0 \right\}$$

is a DVR with a uniformizer x.

Example. Let $K = \mathbb{Q}(\sqrt{10})$ and $D = \mathcal{O}_K = \mathbb{Z}[\sqrt{10}]$. Let $P = (2, \sqrt{10})$ a prime ideal of D. Then P is not principal, but D_P is a DVR with uniformizer $\sqrt{10}$. Indeed:

$$D_P = \left\{ \frac{a + b\sqrt{10}}{c + d\sqrt{10}} : \begin{array}{c} a, b, c, d \in \mathbb{Z} \\ c + d\sqrt{10} \notin P \end{array} \right\}$$

So PD_P is the unique maximal ideal of D_P.

$$\begin{aligned} PD_P &= \left\{ \frac{a + b\sqrt{10}}{c + d\sqrt{10}} : a, b, c, d \in \mathbb{Z}, \begin{array}{c} a + b\sqrt{10} \in P \\ c + d\sqrt{10} \notin P \end{array} \right\} \\ &= \left\{ \frac{\alpha + 2\beta\sqrt{10}}{c + d\sqrt{10}} : \begin{array}{r} \alpha, \beta, c + d\sqrt{10} \in \mathbb{Z}[\sqrt{10}] \\ c + d\sqrt{10} \notin P \end{array} \right\} \\ &= \{2A + \sqrt{10}B : A, B \in D_P\} \end{aligned}$$

We claim that $\sqrt{10}$ is a uniformizer, so we need to show $2 \in \sqrt{10}D_P$, which is equivalent to show $2/\sqrt{10} \in D_P$. Indeed:

$$\frac{2}{\sqrt{10}} = \frac{2\sqrt{10}}{10} = \frac{\sqrt{10}}{5} \in D_P$$

Therefore $PD_P = \sqrt{10}D_P$ is principal.

What are the ideals of a DVR?

Theorem 3.1. Let D be a DVR with maximal ideal $M = (\pi)$. Let $I \subseteq D$ be a nonzero ideal, then $I = (\pi^n)$ for some $n \in \mathbb{Z}_{\geq 0}$.

Proof: Consider the fractional ideal $M^{-1}I = \pi^{-1}I$. Then $\pi^{-1}I \subseteq D$, so it is an integral ideal of D. Keep doing this, we get an ascending chain:

$$\pi^{-1}I \subseteq \pi^{-2}I \subseteq \cdots$$

D is Noetherian measn $\pi^{-n}I = \pi^{-(n+1)}$ or $\pi^{-n}I = D$. The first case violates Nakayama, then $I = \pi^n D = (\pi^n)$. □

In particular, every DVR is a PID.

Also it means that every $0 \neq x \in D$ is of the form $x = \pi^n u$ for some $n \geq 0$ and $u \in D^\times$ a unit. This is because $(x) = (\pi^n)$, so $x = \pi^n u$ for some unit u. Therefore, if K is the fraction field of D and $\alpha \in K$, then:

$$\alpha = \frac{\pi^n u_1}{\pi^m u_2} = \pi^\ell u$$

for some $\ell \in \mathbb{Z}$ and $u \in D^\times$.

Theorem 3.2. Let D be a Noetherian domain and $P \subseteq D$ a nonzero prime ideal. Then D_P is also Noetherian.

Proof: Say $I \subseteq D_P$ is an ideal, we want to show it is finitely generated. Let $J = I \cap D$, then $J = (x_1, \cdots, x_n)$ is finitely generated as D is Noetherian. We claim that $I = (x_1, \cdots, x_n)$, that is:

$$I = x_1 D_P + \cdots + x_n D_P$$

Say $\alpha \in I$, then $\alpha = a/b$ with $a, b \in D$ and $b \notin P$. Then $a = b\alpha \in I$ since I is an ideal and $\alpha \in I$. Therefore $a \in I \subseteq J$. Thus:

$$a = a_1 x_1 + \cdots + a_n x_n$$

for some $a_i \in D$. Therefore:

$$\alpha = \frac{a}{b} = \frac{a_1}{b} x_1 + \cdots + \frac{a_n}{b} x_n$$

which is in $(x_1, \cdots, x_n)$, as desired. □

Lecture 20, 2024/06/19

3.3 Applications to the Ideal Norm

Recall that for $\alpha \in K$, we define $T_\alpha : K \to K$ by $x \mapsto \alpha x$. And define:

$$\begin{aligned} \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) &= \mathrm{Tr}(T_\alpha) \\ N_{K/\mathbb{Q}}(\alpha) &= \det(T_\alpha) = |\mathcal{O}_K/(\alpha)| \end{aligned}$$

We later defined $N(I) = |\mathcal{O}_K/I|$ for any ideal $I \subseteq \mathcal{O}_K$. We proved that:

$$N_{K/\mathbb{Q}}(\alpha) = N((\alpha))$$

if $\alpha \neq 0$. We also know that $N_{K/\mathbb{Q}}(\alpha\beta) = N_{K/\mathbb{Q}}(\alpha) N_{K/\mathbb{Q}}(\beta)$. Our next goal is to prove that:

$$N(IJ) = N(I)N(J)$$

for any ideals I, J of $\mathcal{O}_K$.

Note that if I and J are coprime, that is, $I + J = \mathcal{O}_K$, then:

$$\begin{aligned} N(IJ) &= |\mathcal{O}_K/IJ| \\ &= |\mathcal{O}_K/I \times \mathcal{O}_K/J| \\ &= |\mathcal{O}_K/I| \cdot |\mathcal{O}_K/J| \\ &= N(I)N(J) \end{aligned}$$

This is easy. What if $I + J \neq \mathcal{O}_K$? Write:

$$I = P_1^{a_1} \cdots P_r^{a_r} \text{ and } J = P_1^{b_1} \cdots P_r^{a_r}$$

where $a_i, b_i \geq 0$ (If 0, then not in the facotrization, but a_i, b_i cannot both be 0 for same i). Then we have:

$$\begin{aligned} \mathcal{O}_K/IJ &= \mathcal{O}_K/P_1^{a_1+b_1} \cdots P_r^{a_r+b_r} \\ &\cong \mathcal{O}_K/P_1^{a_1+b_1} \times \cdots \times \mathcal{O}_K/P_r^{a_r+b_r} \end{aligned}$$

Also, we have:

$$\begin{aligned} \mathcal{O}_K/I &\cong \mathcal{O}_K/P_1^{a_1} \times \cdots \times \mathcal{O}_K/P_r^{a_r} \\ \mathcal{O}_K/I &\cong \mathcal{O}_K/P_1^{b_1} \times \cdots \times \mathcal{O}_K/P_r^{b_r} \end{aligned}$$

So it suffices to show the result for powers of prime ideals, that is:

$$|\mathcal{O}_K/P^{a+b}| = |\mathcal{O}_K/P^a| \cdot |\mathcal{O}_K/P^b|$$

Definition. Let A, B, C be R-modules and $f : A \to B$ and $g : B \to C$ be R-module homomorphisms, we say the sequence

$$\begin{tikzcd} A \arrow[r, "f"] & B \arrow[r, "g"] & C \end{tikzcd}$$

is **exact at** B if $\operatorname{Ker} g = \operatorname{Im} f$. A **short exact sequence** is a setup:

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "f"] & B \arrow[r, "g"] & C \arrow[r] & 0 \end{tikzcd}$$

that is exact at A, B, C.

(1) Exact at A means $\operatorname{Ker} f = \operatorname{Im} 0 = 0 \iff f$ is injective.

(2) Exact at C means $\operatorname{Im} g = \operatorname{Ker} 0 = C \iff g$ is surjective.

(3) Exact at B means $\operatorname{Im} f = \operatorname{Ker} g$.

Therefore, by the first isomorphism theorem we have:

$$B/A \cong /\operatorname{Im} f \cong B/\operatorname{Ker} g \cong \operatorname{Im} g = C$$

Hence $B/A \cong C$.

Now back to the goal of showing $|\mathcal{O}_K/P^{a+b}| = |\mathcal{O}_K/P^a| \cdot |\mathcal{O}_K/P^b|$.

If $P = (\pi)$ is a principal ideal, this is easy. Define:

$$f : \mathcal{O}_K/P^n \to \mathcal{O}_K/P^{n+1} \text{ by } f(x) = \pi x$$

Then f is a homomorphism of $\mathcal{O}_K$-modules and it is injective. Its image is P/P^{n+1}, therefore we get:

$$|\mathcal{O}_K/P^n| = |P/P^{n+1}| \tag{1}$$

In particular, we have $|\mathcal{O}_K/P| = |P/P^2|$. Then note that the sequence:

$$\begin{tikzcd} 0 \arrow[r] & P/P^2 \arrow[r, "i"] & \mathcal{O}_K/P^2 \arrow[r, "q"] & \mathcal{O}_K/P \arrow[r] & 0 \end{tikzcd}$$

is exact. Where i is the inclusion, and q is the reduction mod p map. It follows that:

$$\mathcal{O}_K/P \cong (\mathcal{O}_K/P^2)/(P/P^2) \tag{2}$$

Therefore by (2) and the special case of (1) we have:

$$|\mathcal{O}_K/P^2| = |\mathcal{O}_K/P| \cdot |P/P^2| = |\mathcal{O}_K/P| \cdot |\mathcal{O}_K/P| = |\mathcal{O}_K/P|^2$$

In general, we have:

$$|\mathcal{O}_K/P^n| = |\mathcal{O}_K/P|^n$$

if $P = (\pi)$. Hence it follows that:

$$|\mathcal{O}_K/P^{a+b}| = |\mathcal{O}_K/P|^{a+b} = |\mathcal{O}_K/P^a| \cdot |\mathcal{O}_K/P^b|$$

But this only works if $P = (\pi)$ is principal, what if it is not? If we can show:

(1) $(\mathcal{O}_K)_P$ is a DVR for every prime ideal P.

(2) $|\mathcal{O}_K/P^n| = |(\mathcal{O}_K)_P/P_P^n|$.

Here $P_P = P(\mathcal{O}_K)_P$, the ideal of $(\mathcal{O}_K)_P$ generated by P. Then P_P would be principal, so we could use the argument above to show that:

$$|(\mathcal{O}_K)_P/P_P^n| = |(\mathcal{O}_K)_P/P_P|^n$$

Using the second one we can deduce that:

$$|\mathcal{O}_K/P^n| = |\mathcal{O}_K/P|^n$$

Then we are done :)

Lecture 21, 2024/06/21

Theorem 3.3. Let A be a Noetherian. Let $P \subseteq A$ invertible prime ideal of A. Then A_P is a DVR.

Proof: Need to show that A_P is a Noetherian local dommain P_P is principal. Already checked Noetherian by Theorem 3.2 and we already know it is a local ring. It suffices to show that P_P is principal. Well, $PP^{-1} = A$, so:

$$1 = a_1 a_1' + \cdots + a_n a_n'$$

for $a_i \in P$ and $a_i \in P^{-1}$. Each $a_i a_i \in A$, but at least of them, say $a_1 a_1' \notin P$ (if all in P then $1 \in P$).

Claim: $P_P = (a_1) = a_1 A_P$.

Proof (Claim): Since $a_1 \in P$, we get $(a_1) \subseteq P_P$. Say $x \in P_P$, we want to show $x/a_1 \in A_P$. But $a_1 a_1' \in A_P \setminus P_P$, which implies $a_1 a_1'$ is a unit. In particular, write $x = (a_1 a_1')y$ for some $y \in P_P$ thus $x = a_1(a_1' y)$ but $a_1' y \in A_P$ because $a_1' \in P^{-1}$ and $y = c/d$ with $c \in P$ and $d \in A \setminus P$. Thus:

$$a_1' y = \frac{a_1' c}{d} \in A_P$$

as $a_1 c \in A$ and $d \notin P$. Thus $x/a_1 \in A_P$ and then $x \in (a_1) \implies P_P = a_1 A_P$. □

By an argument similar to last lecture, we have:

$$|(\mathcal{O}_K)_P / P_P^a| = |(\mathcal{O}_K)_P / P_P|^a$$

If we can show that:

$$|(\mathcal{O}_K)_P / P_P^a| = |\mathcal{O}_K / P^a| \text{ and } |(\mathcal{O}_K)_P / P_P|^a = |\mathcal{O}_K / P|^a$$

Then we have:

$$|\mathcal{O}_K / P^a| = |\mathcal{O}_K / P|^a$$

And then we are done! So it enough to show those two equalities.

Theorem 3.4. Let A be a Noetherian domain. Let $P \subsetneq A$ be a maximal ideal. Then we have $A/P^n \cong A_P / P_P^n$.

Proof: Define $f : A/P^n \to A_P/P_P^n$ by $f(\alpha + P^n) = \alpha + P_P^n$. This is clearly a homomorphism and we will show f is a bijection.

(Injective). If $f(\alpha + P^n) = 0$, then $\alpha \in P_P^n$ and then $\alpha = x/y$ with $x \in P^n$ and $y \in A \setminus P$. There are $t, u \in A$ and $z \in P^n$ with:

$$ty + uz = 1$$

Also, $t \notin P$ because $z \in P$. So:

$$\alpha = \frac{x}{y} = \frac{tx}{ty} = \frac{tx}{1 - uz}$$

which implies that:

$$\alpha = tx + uz\alpha \in P^n \implies \alpha + P^n = 0$$

Therefore f is injective.

Lecture 22, 2024/06/24

(Surjective). Say $\frac{a}{b} \in A_P$ with $a \in A$ and $b \notin P$. Want to find $x \in A$ such that:

$$f(x + P^n) = \frac{a}{b} + P_P^n$$

which is equivalent to $x - \frac{a}{b} \in P_P^n$. So it is enough to find $x \in A$ such that $bx - a \in P^n$. Since $b \notin P$, we get $(b) + P^n = (1)$. So there are $\alpha, \beta \in A$ such that $\alpha b + \beta y = 1$ for $y \in P^n$ and $\alpha \notin P$. Set $x = \alpha a$, then:

$$bx - a = \alpha ab - a = a(\alpha b - 1) = -\beta ya \in P^n$$

As desired. □

Theorem 3.5. Let D be a DVR with maximal ideal P. If D/P is finite, then:

$$|D/P^n| = |D/P|^n$$

Proof: Induce on n. If $n = 1$, we are done. In general, we have the following short exact sequence:

$$\begin{tikzcd}0 \arrow[r] & P/P^{n+1} \arrow[r, "i"] & D/P^{n+1} \arrow[r, "\pi"] & D/P^n \arrow[r] & 0\end{tikzcd}$$

where i is the inclusion and π is the reduction mod P map. All of these are vector spaces over D/P and the maps are linear maps. So:

$$\dim(D/P^{n+1}) = \dim(P^n/P^{n+1}) + \dim(D/P^n)$$

because we have $(D/P^{n+1})/(P^n/P^{n+1}) \cong D/P^n$. We know that $\dim(D/P^n) = n$ by induction. It suffices to show $\dim(P^n/P^{n+1}) = 1$. Since D is a DVR, $P = (\pi)$ is principal. So $P^n = (\pi^n)$. We have another short exact sequence:

$$\begin{tikzcd}0 \arrow[r] & P/P^{n+1} \arrow[r, "i"] & D/P \arrow[r, "f"] & P^n/P^{n+1} \arrow[r] & 0\end{tikzcd}$$

where i is inclusion and f is multiplication by π^n. The kernel of f is P, so this is an isomorphism. Therefore:

$$\dim(P^n/P^{n+1}) = \dim(D/P) = 1$$

Hence $\dim(D/P^{n+1}) = n + 1$ and $|D/P^{n+1}| = |D/P|^{n+1}$, as desired. □

Therefore we have $N(P^a) = N(P)^a$, it follows that:

Theorem 3.6. Let K be a number field with ring of integers $\mathcal{O}_K$. If I, J are two ideals of $\mathcal{O}_K$, then:

$$N(IJ) = N(I)N(J)$$

Example. Say $N(I) = 7 \cdot 29$ in $\mathcal{O}_K$, we know that:

$$I = P_1^{e_1} \cdots P_r^{e_r}$$

for some prime ideals $P_1, \cdots, P_r$. Thus:

$$N(I) = N(P_1)^{e_1} \cdots N(P_r)^{e_r} = 7 \cdot 29$$

Recall that $N(P)$ is always a prime power for any prime ideal P since $\mathcal{O}_K/P$ is a finite field. Therefore $N(P_i)^{e_i}$ are prime powers, it must be that:

$$I = P_7 \cdot P_{29}$$

where $N(P_7) = 7$ and $N(P_{29}) = 29$.

If I is a nonzero ideal of $\mathcal{O}_K$, then:

$$I = P_1^{e_1} \cdots P_r^{e_r}$$

for some prime ideals $P_1, \cdots, P_r$. In $(\mathcal{O}_K)_{P_i}$ we have:

$$I_{P_i} := I(\mathcal{O}_K)_{P_i} = (P_i)_{P_i}^{a_i}$$

This is because $P_2^{e_2} \cdots P_r^{e_r} \not\subseteq P_1$, so there exists $x \in P_2^{e_2} \cdots P_r^{e_r} \setminus P_1$, hence x is a unit in $(\mathcal{O}_K)_{P_i}$, making $(P_2^{e_2} \cdots P_r^{e_r})(\mathcal{O}_K)_{P_i}$ the unit ideal in $(\mathcal{O}_K)_{P_i}$. If I is a fractional ideal, then this all works exactly the same way, except some a_i might be negative.

Definition. Let $p \in \mathbb{Z}$ be a prime number. Let K be a number field, and write:

$$(p) = p\mathcal{O}_K = P_1^{e_1} \cdots P_r^{e_r}$$

The number e_i is called the **ramification index** of P_i in $\mathcal{O}_K$. We define f_i so that:

$$p^{f_i} = |\mathcal{O}_K/P_i| = N(P_i)$$

to be the **residue degree** of P_i.

Let $d = [K : \mathbb{Q}]$, then note that $N(p\mathcal{O}_K) = p^{[K:\mathbb{Q}]} = p^d$ and:

$$N(p\mathcal{O}_K) = N(P_1)^{e_1} \cdots N(P_r)^{e_r} = p^{e_1 f_1} \cdots p^{e_r f_r}$$

Therefore:

$$d = [K : \mathbb{Q}] = e_1 f_1 + \cdots + e_r f_r$$

Theorem 3.7. Let $A \subseteq \mathcal{O}_K$ be a subring of finite index m. If $P \subseteq A$ is a prime ideal with $\gcd(m, N(P)) = 1$ ($m \notin P$), then A_P is a DVR.

Proof: Let $I = P\mathcal{O}_K$ be the ideal of $\mathcal{O}_K$ generated by P. If $I = \mathcal{O}_K$, then there are $a_1, \cdots, a_n \in P$ and $b_1, \cdots, b_n \in \mathcal{O}_K$ such that:

$$a_1 b_1 + \cdots + a_n b_n = 1$$

Hence we have:

$$a_1(mb_1) + \cdots a_n(mb_n) = m$$

Here each $a_i \in P$. Also, since $|\mathcal{O}_K/A| = m$, every element in $\mathcal{O}_K/A$ has order dividing m, meaning $mx \equiv 0 \pmod{A}$ for all $x \in \mathcal{O}_K$, that is, $mx \in A$. Hence $mb_i \in A$ for all i. Therefore since P is an ideal in A, the LHS is in A. However $m \notin A$, contradiction. Therefore $I \subseteq Q$ for some maximal ideal $Q \subseteq \mathcal{O}_K$, then we have:

$$(\mathcal{O}_K)_Q = \left\{\frac{a}{b} : a, b \in \mathcal{O}_K,\ b \notin Q\right\} = \left\{\frac{ma}{mb} : a, b \in \mathcal{O}_K,\ b \notin Q\right\} \subseteq A_P$$

and that:

$$A_P = \left\{\frac{a}{b} : a, b \in A,\ b \notin P\right\} \subseteq (\mathcal{O}_K)_Q$$

here the last inclusion is because $A \cap Q = P$. So $A_P = (\mathcal{O}_K)_Q$ is a DVR. □

Theorem 3.8. Let $A \subseteq \mathcal{O}_K$ be a subring of finite index. Then $A = \mathcal{O}_K$ if and only if A_P is a DVR for all prime ideals $P \subseteq A$.

Lecture 23, 2024/06/26

Proof: ($\Rightarrow$) We have already seen this.

($\Leftarrow$). Want to show $A = \mathcal{O}_K$. Say $P \subseteq A$ is a nonzero prime ideal of A. Let $I = P\mathcal{O}_K$. If $I = \mathcal{O}_K$ then $1 \in I$. There is $\alpha \in P$ with $1/\alpha \in \mathcal{O}_K$. We know A_P is a DVR, so let $P_P = (\pi) = \pi A_P$. Write $\alpha = u\pi^n$ for $u \in A_P^\times$ and $n \geq 1$. Since $1/\alpha \in \mathcal{O}_K$ we know $1/\alpha$ is integral over $\mathbb{Z}$. So $u^{-1}\pi^{-n}$ is integral over $\mathbb{Z}$. So:

$$(u\pi^{n-1})(u^{-1}\pi^{-n}) = \pi^{-1}$$

is integral over A_P, which it is not: $\{1, \pi^{-1}, \pi^{-2}, \cdots\}$ is an infinite A_P-linearly independent set in $A_P[\pi^{-1}] = K$. So $I \neq \mathcal{O}_K$. That means $I \subseteq Q$ for some maximal ideal $Q \subseteq \mathcal{O}_K$, so $(\mathcal{O}_K)_Q$ contains A_P. Now let us prove a lemma first.

Lemma 3.9. Say D is a DVR with fraction field K. If A is a ring satisfying $D \subseteq A \subseteq K$, then $D = A$ or $A = K$.

Proof (Lemma): If $D \neq A$, then A contains $u\pi^n$ for $u \in D^\times$ and $n < 0$ in $\mathbb{Z}$. This gives $\pi^{-1} = (u^{-1}\pi^{-1-n})u\pi^n \in A$, so A contains $D[\pi^{-1}] = K$. □

Proof Continued: Say $x \in \mathcal{O}_K$, we want to show $x \in A$. Well, $x = a/b$ where $a, b \in A$ and $b \neq 0$. Define the set:

$$D = \{b \in A : bx \in A\}$$

to be the set of possible denominators of x. Note that:

$$D = (A : (x)) \cap A$$

We want to show $D = A$, that is, $1 \in D$. Suppose $D \neq A$, that is $D \subsetneq A$, so $D \subseteq P \subseteq A$ for some nonzero prime ideal P of A. But then $x \notin A_P = (\mathcal{O}_K)_Q$ for some prime ideal $Q \subseteq \mathcal{O}_K$. So $x \notin \mathcal{O}_K$, giving $D = A$ by contradiction. Thus $x \in A$. □

3.4 Ramification

Definition. A prime number $p \in \mathbb{Z}$ is **ramified** in K if:

$$(p) = p\mathcal{O}_K = P_1^{e_1} \cdots P_r^{e_r}$$

has $e_i \geq 2$ for some i. This is equivalent to $\mathcal{O}_K/(p)$ has nilpotent elements. We say p is **unramified** in K if not ramified.

Theorem 3.10. Let K be a number field and $p \in \mathbb{Z}$ a prime. Then p is ramified in $\mathcal{O}_K$ if and only if p divides $\operatorname{disc} K = \operatorname{disc} \mathcal{O}_K$. In particular, only finitely many primes ramify in K.

Proof: ($\Rightarrow$). Say $p\mathcal{O}_K = P_1^{e_1} \cdots P_r^{e_r}$ with $e_1 \geq 2$. Then $\mathcal{O}_K/p\mathcal{O}_K$ has nilpotent elements. It means the trace pairing on $\mathcal{O}_K/(p)$ is degenerate, so there is $x \in \mathcal{O}_K/(p)$ such that $\operatorname{Tr}(xy) = 0$ for all $y \in \mathcal{O}_K/(p)$. That is, there is $x \in \mathcal{O}_K$ such that:

$$\operatorname{Tr}(xy) \in (p) \text{ for all } y \in \mathcal{O}_K \tag{1}$$

Without loss of generality, suppose x is not divisible by any integer greate than 1. (If $n \mid x$, then replace x with x/n). Now we extend $\{x\}$ to a basis $\{x_1, a_1, \cdots, a_{d-1}\}$ of $\mathcal{O}_K$ over $\mathbb{Z}$. Then:

$$\operatorname{disc} K = \operatorname{disc} \mathcal{O}_K = \det \begin{pmatrix} \operatorname{Tr}(x^2) & \operatorname{Tr}(xa_1) & \cdots & \operatorname{Tr}(xa_{d-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \operatorname{Tr}(a_{d-1}x) & \operatorname{Tr}(a_{d-1}a_1) & \cdots & \operatorname{Tr}(a_{d-1}^2) \end{pmatrix}^2$$

By (1), we know the first row of the matrix is all in (p), so this determinant is 0 in (p), that is, we have $p \mid \operatorname{disc} K$.

Lecture 24, 2024/06/28

($\Leftarrow$). Suppose $p \mid \operatorname{disc} K$, then $p \mid \det(\operatorname{Tr}(x_i x_j))$ where $\{x_1, \cdots, x_n\}$ is a basis of $\mathcal{O}_K$ over $\mathbb{Z}$. So there are $a_1, \cdots, a_n \in \mathbb{Z}$ with:

$$a_1 \operatorname{Tr}(x_i x_1) + \cdots + a_n \operatorname{Tr}(x_i x_n) \equiv 0 \pmod{p}$$

for all i (a_i not all 0), which means:

$$\operatorname{Tr}((a_1x_1 + \cdots + a_nx_n)x_i) \equiv 0 \pmod{p}$$

for all i, so $\operatorname{Tr}(xy) \equiv 0 \pmod{p}$ for all $x \in \mathcal{O}_K$. Write $(p) = P_1^{e_1} \cdots P_r^{e_r}$. Suppose for a contradiction that $e_1 = \cdots = e_r = 1$, then:

$$\mathcal{O}_K/(p) \cong \mathcal{O}_K/P_1 \times \cdots \times \mathcal{O}_K/P_r$$

If y maps to $(y_1, \cdots, y_n)$ via this isomorphism, then if $y_i \neq 0$, let $(0, \cdots, \frac{b}{y_i}, \cdots, 0)$ correspond to $x \in \mathcal{O}_K$, where $b \in \mathcal{O}_K/P$ so $\operatorname{Tr}(b) \not\equiv 0 \pmod{p}$. So we get:

$$\operatorname{Tr}(xy) = \operatorname{Tr}(0, \cdots, b, \cdots, 0) \neq 0$$

so $e_1 = \cdots = e_r = 1$ is impossible, thus p ramifies in K. □

Let us see how do all these theorems help us to figure out what $\mathcal{O}_K$ is.

Example. Let $K = \mathbb{Q}(\alpha)$, where α is a root of $x^3 - x^2 - 2x - 8$. What is $\mathcal{O}_K$? Our first case is $\mathbb{Z}[\alpha]$.

$$\operatorname{disc} \mathbb{Z}[\alpha] = \operatorname{disc}(x^3 - x^2 - 2x - 8) = -2^2 \cdot 503$$

Thus $[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 1$ or 2. If $P \subseteq \mathbb{Z}[\alpha]$ is prime ideal with $2 \notin P$, then $\mathbb{Z}[\alpha]$ is a DVR. So it is enough to check the prime ideals that do contain 2.

$$\begin{aligned} \mathbb{Z}[\alpha]/(2) &\cong \mathbb{Z}[x]/(x^3 - x^2 - 2x - 8, 2) \\ &\cong \mathbb{F}_2[x]/(x^3 - x^2) \\ &\cong \mathbb{F}_2[x]/(x-1) \times \mathbb{F}_2[x]/(x^2) \end{aligned}$$

So the two prime ideals containing 2 are $P_1 = (2, \alpha - 1)$ and $P_2 = (2, \alpha)$. Now let us check if $\mathbb{Z}[\alpha]_{P_1}$ and $\mathbb{Z}[\alpha]_{P_2}$ are DVRs. Is $\mathbb{Z}[\alpha]_{P_1}$ a DVR?

$$\alpha - 1 = \frac{2\alpha + 8}{\alpha^2} = 2\left(\frac{\alpha + 4}{\alpha^2}\right) \in \mathbb{Z}[\alpha]_{P_1}$$

and $\alpha^2 \notin P_1$. Then $P_1\mathbb{Z}[\alpha]_{P_1} = (2)\mathbb{Z}[\alpha]_{P_1}$. Therefore it is a DVR. What about $\mathbb{Z}[\alpha]_{P_2}$? Suppose it is, then either $\alpha/2 \in \mathbb{Z}[\alpha]_{P_2}$ or $2/\alpha \in \mathbb{Z}[\alpha]_{P_2}$. Say:

$$\frac{\alpha}{2} = \frac{a\alpha^2 + b\alpha + c}{d\alpha^2 + e\alpha + f}$$

where $a, b, c, d, e, f \in \mathbb{Z}$, therefore:

$$\begin{aligned} & d\alpha^3 + e\alpha^2 + f\alpha = 2a\alpha^2 + 2b\alpha + 2c \\ \implies & d(\alpha^2 + 2\alpha + 8) + e\alpha^2 + f\alpha = 2a\alpha^2 + 2b\alpha + 2c \\ \implies & (d + e)\alpha^2 + (2d + f)\alpha + 8d = 2a\alpha^2 + 2b\alpha + 2c \end{aligned}$$

Therefore:

$$8d = 2c \text{ and } 2d + f = 2b$$

which implies that c, f are both even. So $a\alpha^2 + b\alpha + c, d\alpha^2 + e\alpha + f$ are both in $(2, \alpha)$. Therefore $\alpha/2$ and $2/\alpha$ cannot be rewritten without denominators in P_2. So $\mathbb{Z}[\alpha]_{P_2}$ cannot be a DVR. Hence $\mathbb{Z}[\alpha] \neq \mathcal{O}_K$ and $[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 2$. Therefore $\operatorname{disc} \mathcal{O}_K = -503$. Note that $2 \nmid 503$, so 2 does not ramify in $\mathcal{O}_K$. Since $N(2) = 2^3 = 8$ and (2) is not prime, we have:

$$(2) = PQR \text{ or } (2) = PQ$$

In the first case, all three prime ideals have norm 2. In the second case, one of the ideals has norm 4.

Lecture 25, 2024/07/03

Last time, we proved that $\mathbb{Z}[\alpha] \neq \mathcal{O}_K$, so there is $\beta \in \mathcal{O}_K \setminus \mathbb{Z}[\alpha]$. Well, we know $[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 2$, so $2\beta \in \mathbb{Z}[\alpha]$. Therefore:

$$\beta = \frac{a\alpha^2 + b\alpha + c}{2}$$

for some $a, b, c \in \mathbb{Z}$. By adding elements of $\mathbb{Z}[\alpha]$ to β, we keep $\beta \in \mathcal{O}_K \setminus \mathbb{Z}[\alpha]$, but we can make $a, b, c \in \{0, 1\}$. So we can choose β from:

$$\frac{0}{2}, \frac{1}{2}, \frac{\alpha}{2}, \frac{\alpha+1}{2}, \frac{\alpha^2}{2}, \frac{\alpha^2+\alpha}{2}, \frac{\alpha^2+\alpha+1}{2}$$

Note that $0/2 \in \mathbb{Z}[\alpha]$ and $1/2 \notin \mathcal{O}_K$, so they do not work. The minimal polynomial for $\alpha/2$ is:

$$(2x)^3 - (2x)^2 - 2(2x) - 8 = 8x^3 - 4x^2 - 4x - 8$$

Clear the leading coefficient, we get $x^3 - x^2/2 - x/2 - 1 \notin \mathbb{Z}[x]$, hence $\alpha/2 \notin \mathcal{O}_K$. Similarly $(\alpha+1)/2 \notin \mathcal{O}_K$. Also it turns out $(\alpha^2+1)/2, (\alpha^2+\alpha+1)/2 \notin \mathcal{O}_K$. Lastly, $\alpha^2/2 \notin \mathcal{O}_K$. Therefore we have $\beta = (\alpha^2+\alpha)/2$. Hence $\mathcal{O}_K = \mathbb{Z}[\alpha, \beta]$.

However, is there some $\gamma \in \mathcal{O}_K$ such that $\mathcal{O}_K = \mathbb{Z}[\gamma]$? Our first guess is $\gamma = \beta$. The minimal polynomial for β is $x^3 - 2x^2 + 3x - 10$. So:

$$\operatorname{disc}(\mathbb{Z}[\beta]) = \operatorname{disc}(x^3 - 2x^2 + 3x - 10) = -2^2 \cdot 503$$

So $\mathbb{Z}[\beta]$ also has index 2 in $\mathcal{O}_K$ as $\operatorname{disc} \mathcal{O}_K = -503$. So $\mathbb{Z}[\beta] \neq \mathcal{O}_K$. Note that:

$$\mathbb{Z}[\beta]/(2) \cong \mathbb{F}_2[x]/(x) \times \mathbb{F}_2[x]/(x+1)^2$$

So (2) is contained in $P_3 = (2, \beta)$ and $Q = (2, \beta+1)$ in $\mathbb{Z}[\beta]$. Note that $\mathbb{Z}[\beta]_{P_3}$ is a DVR since:

$$\beta = 2\left(\frac{5}{\beta^2 - 2\beta + 3}\right)$$

So 2 is a uniformizer of $P_3\mathbb{Z}[\beta]_{P_3}$. Therefore $\mathbb{Z}[\beta]_Q$ must not be a DVR! How does (2) factor in $\mathcal{O}_K$? We know $(2) \subseteq P_1$, where $P_1 = (2, \alpha+1)$. Recall that $(2, \alpha+1)$ in $\mathbb{Z}[\alpha]$ is a prime ideal, it turns out that $(2, \alpha+1)$ is also a prime ideal in $\mathcal{O}_K$. And we have $e(P_1) = 1$ since $2 \nmid \operatorname{disc} K$, and $f(P_1) = 1$ as $N(P_1) = 2$. Also, $P_3 = (2, \beta)$ has $e(P_3) = f(P_3) = 1$. Is $P_1 = P_3$? No, because:

$$P_1 + P_3 = (2, \alpha+1, \beta)$$

and note that:

$$\alpha\beta = \frac{\alpha^3 - \alpha^2}{2} = \frac{\alpha^2 + 2\alpha + 8 - \alpha^2}{2} = \alpha + 4 \in P_1 + P_3$$

Hence $\alpha + 4 - (\alpha+1) - 2 = 1 \in P_1 + P_3$. Hence $P_1 + P_3 = (1)$, which implies $P_1 \neq P_3$. Therefore $(2) \subseteq P_1, P_3$ and $P_1 \neq P_3$. If:

$$(2) = Q_1 Q_2 \cdots Q_r$$

then we have:

$$e(Q_1)f(Q_1) + \cdots + e(Q_r)f(Q_r) = 3$$

Let us say $Q_1 = P_1$ and $Q_2 = P_3$, so:

$$1 + 1 + e(Q_3)f(Q_3) + \cdots = 3$$

Hence $r = 3$ and $e(Q_3) = f(Q_3) = 1$. In other words, $(2) = P_1P_3Q_3$. What is Q_3? Maybe $Q_3 = (2, \alpha, \beta - 1)$. Its norm is at most 2, need to show $1 \notin Q_3$.

$$f(a + b\alpha + c\beta) = (a + c) \pmod 2$$

is a surjection from $\mathcal{O}_K$ to Q_3, showing that Q_3 is a prime ideal of norm 2. So $(2) = P_1P_3Q_3$, all idfferent. Now, say $\mathcal{O}_K = \mathbb{Z}[\gamma]$ and γ has minimal polynomial $m(x)$, then:

$$\begin{aligned}\mathcal{O}_K/(2) &\cong \mathbb{F}_2[x]/(m(x)) \\ &\cong F_2[x]/(\ell_1(x)) \times F_2[x]/(\ell_2(x)) \times F_2[x]/(\ell_3(x))\end{aligned}$$

where $\ell_1(x), \ell_2(x), \ell_3(x)$ are distinct irreducible factors of $m(x)$ mod 2, because (2) totally splits. However, $\deg m(x) = 3$, so $\ell_1(x), \ell_2(x), \ell_3(x)$ are linear polynomials in $\mathbb{F}_2[x]$. But! There are only two distinct linear irreducible polynomials in $\mathbb{F}_2[x]$, contradiction.

Therefore $\mathcal{O}_K = \mathbb{Z}[\alpha, \beta]$ and $\mathcal{O}_K \neq \mathbb{Z}[\gamma]$ for any $\gamma \in \mathcal{O}_K$!

Lecture 26, 2024/07/05

4 Class Groups

Questions: When is $\mathcal{O}_K$ a PID? Even if $K = \mathbb{Q}(\sqrt{d})$, we still do not know in general. For $d < 0$, we do know that $\mathcal{O}_K$ is a PID if and only if:

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163$$

Let $I = (a), J = (b)$ be two nonzero principal ideals of a ring R, then $a, b \neq 0$, so we have:

$$I = \frac{a}{b}(b) = \frac{a}{b}J$$

So we can say a PID is a domain with only 'one kind of ideals' in the sense that all ideals all the same up to scaling by an element of K.

4.1 Class Groups

Definition. The **ideal group** of $\mathcal{O}_K$ is the group of nonzero fractional ideals of $\mathcal{O}_K$ under multiplication. We call it $I(K)$.

This group is precisely the free abelian group on the prime ideals of $\mathcal{O}_K$, which is a boring group.

Definition. The **ideal class group of $\mathcal{O}_K$** (or the **class group of K**), denoted by $\mathrm{Cl}(K)$, is the quotient group of $I(K)$:

$$\mathrm{Cl}(K) = I(K)/P(K)$$

where $P(K)$ is the subgroup of nonzero principal ideals in $I(K)$. An element of the class group is called an **ideal class**.

Remark. Note that, for two elements $IP(K)$ and $JP(K)$ in $\mathrm{Cl}(K)$, we have:

$$\begin{aligned} IP(K) = JP(K) &\iff IJ^{-1} \in P(K) \\ &\iff IJ^{-1} = (a) \text{ for some } a \in K \\ &\iff I = aJ \text{ for some } a \in K \end{aligned}$$

Therefore, each ideal class contains ideals that are the same up to a scaling by some $a \in K$. Hence, $\mathcal{O}_K$ is a PID if and only if $\mathrm{Cl}(K)$ is the trivial group, that is, all ideals are the same up to a scaling.

Hence, the bigger $\mathrm{Cl}(K)$ is, the further $\mathcal{O}_K$ is from being a PID. But what if $\mathrm{Cl}(K)$ is an infinite group? Then we cannot measure how bad $\mathcal{O}_K$ fails to be a PID. Well, it turns out that $\mathrm{Cl}(K)$ is always finite!

4.2 Finiteness of Class Groups

Theorem 4.1. Let K be a number field, then $\mathrm{Cl}(K)$ is a finite group.

We will break the proof of this theorem into two steps. Our plan is:

(1) Find a constant $M_K > 0$ such that every ideal class contains an integral ideal of norm $\leq M_K$.

(2) Show that for every $B > 0$, there are only finitely many ideals of $\mathcal{O}_K$ of norm at most B.

Theorem 4.2. Let K be a number field of degree n with r real embeddings and s pairs of complex embeddings. Then every ideal class of $\mathcal{O}_K$ contains an integral ideal of norm at most M_K, where:

$$M_K = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(K)|}$$

Lecture 27, 2024/07/08

We will prove part (2) of the plan first.

Lemma 4.3. Let $B > 0$, then there are only finitely many ideals of $\mathcal{O}_K$ of norm at most B.

Proof: We first define:

$$\Lambda = \operatorname{lcm}(1, \cdots, [B])$$

where $[B]$ is the floor of B. Now we have the following claim:

Claim: If $I \subseteq \mathcal{O}_K$ is an integral ideal of norm $\leq B$, then $\Lambda \in I$.

Proof (Claim): Note that $N(I)$ divides Λ as integers, write $aN(I) = \Lambda$ for some $a \in \mathbb{Z}$. Also, we know $N(I) \subseteq I$, so $\Lambda = aN(I) \in I$, as desired.

Now, we let $(\Lambda) = P_1^{a_1} \cdots P_r^{a_r}$ be its factorization in $\mathcal{O}_K$. Since $(\Lambda) \subseteq I$, we have:

$$I = P_1^{b_1} \cdots P_r^{b_r}$$

where $0 \leq b_i \leq a_i$. Hence there are only $\prod (a_i + 1)$ many choices for I. □

Proof of Theorem 4.2: Ideals $I \sim J$ in $\mathrm{Cl}(K)$ if and only if $aI = J$ for some $a \in K^*$. So if $aI \subseteq \mathcal{O}_K$, we must have $a \in I^{-1}$. Also:

$$N(aI) \leq M_K \iff |N(a)|N(I) \leq M_K \iff |N(a)| \leq M_K N(I^{-1}) \tag{1}$$

We will show that any nonzero ideal $J \subseteq \mathcal{O}_K$ contains an element of norm $\leq M_K N(J)$. Define:

$$\Lambda = \{(v_1, \cdots, v_n) \in V_K : |v_1 \cdots v_n| < M_K N(J)\}$$

We want to show $\Lambda \cap \phi_K(J) \neq \{0\}$, where ϕ_K is the Minkowski map, hence this $v' = (v_1, \cdots, v_n) \in \Lambda \cap \phi_K(J)$ corresponds to $v_1 \in J$ and:

$$|N(v_1)| = |v_1 \cdots v_n| < M_K N(J)$$

Then let $J = I^{-1}$, then by (1) we have $N(v_1 I) \leq M_K$ and $(v_1 I)$ is an integral ideal of $\mathcal{O}_K$, and we are done.

Now, we have seen that this plan works. Our next goal is to show $\Lambda \cap \phi_K(J) \neq \{0\}$.

Lemma 4.4 (Minkowski). Let $L \subseteq \mathbb{R}^n$ be a lattice. Let $S \subseteq \mathbb{R}^n$ be symmetric (For all $v \in \mathbb{R}^n$, $v \in S \iff -v \in S$), convex and $\operatorname{Vol}(S) > 2^n|\det L|$. Then $S \cap L$ contains a nonzero vector. Here the volume of S is just:

$$\operatorname{Vol}(S) = \int_S 1$$

and $\det L$ is defined by $\det(v_1, \cdots, v_n)$ where $\{v_1, \cdots, v_n\}$ is a basis of L.

Proof: Google it. □

This lemma, tragically, does not apply to Λ directly. So we define a subset of Λ which the lemma does apply. Define:

$$S = \{(v_1, \cdots, v_n) \in V_K : |v_1| + \cdots + |v_n| < t\}$$

for some $t \in \mathbb{R}$ to be determined later. (This is the circle of radius t in V_K using the ℓ_1 norm). Then:

$$\operatorname{Vol}(S) = 2^r \pi^s \frac{t^n}{n!}$$

Also S is convex and symmetric, so to apply Minkowski's Lemma, we need its volume to be big enough. We need:

$$2^r \pi^s \frac{t^n}{n!} > 2^n |\det L| = 2^n N(J)\sqrt{|\operatorname{disc} K|}$$

which means:

$$\begin{aligned} t^n &> 2^{n-r}\pi^{-s} n! N(J)\sqrt{|\operatorname{disc} K|} \\ &= n! \left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc} K|} N(J) \end{aligned}$$

To ensure $S \subseteq \Lambda$, we need:

$$\left(\frac{t}{n}\right)^n \leq M_K N(J)$$

which implies:

$$t^n \leq n! \left(\frac{4}{\pi}\right)^2 \sqrt{|\operatorname{disc} K|}$$

For all $B > M_K N(J)$, there is a nonzero vector in J of norm $\leq B$. But J is discrete and closed, so J contains a nonzero vector of norm $\leq M_K N(J)$ as well. □

Lecture 28, 2024/07/10

4.3 Computing the Class Groups

Example. Let $K = \mathbb{Q}(\sqrt{10})$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt{10}]$.

We know that every ideal of $\mathcal{O}_K$ is a product of prime ideals. We know $N(IJ) = N(I)N(J)$ and we know that every ideal in $\mathcal{O}_K$ is aI for some $a \in K^\times$ and $I \subseteq \mathcal{O}_K$ with $N(I) \leq M_K$. Therefore $\mathrm{Cl}(K)$ is generated by the prime ideals of norm $\leq M_K$.

Our first step is to find all prime ideals of norm $\leq M_K$. The minimal polynomial for $\alpha = \sqrt{10}$ is $m(x) = x^2 - 10$, so:

$$\mathrm{disc}(K) = \mathrm{disc}(\mathbb{Z}[\sqrt{10}]) = \mathrm{disc}(x^2 - 10) = 40$$

Therefore we have:

$$M_K = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\,\mathrm{disc}(K)|} = \frac{2!}{2^2}\left(\frac{4}{\pi}\right)^0 \sqrt{40} = \sqrt{10} < 4$$

Let us compute $m(n)$ for $|n| < 4$, which will be useful later.

$$\begin{aligned} m(-3) &= m(3) = -1 \\ m(-2) &= m(2) = -6 = -2 \cdot 3 \\ m(-1) &= m(1) = -9 = -3^2 \\ m(0) &= -10 = -2 \cdot 5 \end{aligned}$$

Theorem 4.5. Say $\alpha \in \mathcal{O}_K$ with $K = \mathbb{Q}(\alpha)$ and α has the monic minimal polynomial $m(x) \in \mathbb{Z}[x]$ over $\mathbb{Q}$. Then for any $n \in \mathbb{Z}$ we have:

$$N_{K/\mathbb{Q}}(\alpha - n) = (-1)^{\deg(m)} m(n)$$

Proof: The minimal polynomial for $(\alpha - n)$ is $m(x + n)$, write:

$$m(x + n) = x^r + \cdots + a_1 x + a_0$$

So we have:

$$N_{K/\mathbb{Q}}(\alpha - n) = (-1)^{\deg(m)} a_0 = (-1)^{\deg(m)} m(n)$$

As desired. □

Back to the example. We know $N(\alpha) = -10$, so:

$$(\alpha) = P_2 P_5$$

for prime ideals P_2, P_5 with $2 \in P_2$ and $5 \in P_5$. Note that $2 \mid \operatorname{disc}(K) = 40$, so 2 ramifies in K. Hence we must have $(2) = P_2^2$ in $\mathcal{O}_K$, because $[K : \mathbb{Q}] = 2$. By the theorem:

$$N(\alpha + 2) = (-1)^2 m(-2) = -6$$

Therefore:

$$(\alpha + 2) = P_2 P_3$$

where $3 \in P_3$ and $N(P_3) = 3$. Since $N(3) = 9$, we have $(3) = P_3 Q_3$ with $N(Q_3) = 3$. Since $3 \nmid 40$, we know 3 is unramified in K, so $P_3 \neq Q_3$. Therefore, all prime ideals of norm ≤ 3 are:

$$P_2, P_3, Q_3$$

Hence, $\operatorname{Cl}(K)$ is generated by P_2, P_3, Q_3. What are the relations? First note that:

$$(\alpha + 2) = P_2 P_3 \implies P_2 = P_3^{-1} \text{ in } \operatorname{Cl}(K)$$

This is because $(\alpha + 2)$ is a principal ideal, so it is 1 in $\operatorname{Cl}(K)$. Similarly:

$$(\alpha + 1) = Q_3^2 \implies Q_3^2 = 1 \text{ in } \operatorname{Cl}(K)$$

$$(3) = P_3 Q_3 \implies P_3 = Q_3^{-1} \text{ in } \operatorname{Cl}(K)$$

Therefore $P_3 = Q_3^{-1}$ and $P_2 = Q_3$, which means $\operatorname{Cl}(K)$ is generated by Q_3. Since $Q_3^2 = 1$ we know it has order 1 or 2. Which is it?

$$\operatorname{ord}(Q_3) = \begin{cases} 1 & \text{if } Q_3 \text{ is principal} \\ 2 & \text{if } Q_3 \text{ is not} \end{cases}$$

Now, suppose $Q_3 = (\gamma)$ for some $\gamma \in \mathcal{O}_K$. Then $|N(\gamma)| = N(Q_3) = 3$. Say $\gamma = a + b\sqrt{10}$, then:

$$N(\gamma) = a^2 - 10b^2 = \pm 3$$

However, this implies:

$$a^2 \equiv \pm 3 \pmod 5$$

which never happens! Therefore Q_3 is not principal and thus $\operatorname{Cl}(K)$ is generated by Q_3 which has order 2. It follows that $\operatorname{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$.

It would be better if we can figure out what Q_3 is:

$$N_{K/\mathbb{Q}}(\alpha - 2) = (-1)^2 m(2) = -6 = -2 \cdot 3$$

Hence $(\alpha - 2) = P_2 Q_3$. Recall that $(3) = P_3 Q_3$, so:

$$(\alpha - 2) + (3) = P_2 Q_3 + P_3 Q_3 = (P_2 + P_3) Q_3 = Q_3$$

It follows that $Q_3 = (3, \alpha - 2)$. Therefore, every ideal of $\mathcal{O}_K = \mathbb{Z}[\sqrt{10}]$ is up to scaling:

$$(1) \quad \text{or} \quad (3, \sqrt{10} - 2)$$

Lecture 29, 2024/07/12

Example. What is $\mathrm{Cl}(K)$ for $K = \mathbb{Q}(\alpha)$ where the minimal polynomial of α is $m(x) = x^3 - 3x + 3$. What is $\mathcal{O}_K$? Maybe it is $\mathbb{Z}[\alpha]$.

$$\operatorname{disc} \mathbb{Z}[\alpha] = \operatorname{disc}(x^3 - 3x + 3) = -3^3 \cdot 5$$

So $\mathbb{Z}[\alpha]$ is either $\mathcal{O}_K$ or has index 3 in $\mathcal{O}_K$. So any local ring of $\mathbb{Z}[\alpha]$ at a prime ideal that does not contain 3 is a DVR. It is enough to check the prime ideals that contain 3.

$$\mathbb{Z}[\alpha]/(3) \cong \mathbb{F}_3[x]/(x^3 - 3x + 3) \cong \mathbb{F}_3[x]/(x^3)$$

Hence, the only such prime ideal is $Q = (\alpha, 3)$. Note that $\alpha^2 - 3\alpha = 3$, so $(\alpha, 3) = (\alpha)$. Hence $\mathbb{Z}[\alpha]_Q$ is a DVR. It follows that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

Now we can start computing $\mathrm{Cl}(K)$. Note that $\operatorname{disc} m(x) < 0$, so $m(x)$ has 1 real root and 2 complex roots. Hence $r = 1$ and $s = 1$:

$$M_K = \frac{3!}{3^3}\left(\frac{4}{\pi}\right)\sqrt{135} < 4$$

So $\mathrm{Cl}(K)$ is generated by prime ideals of norm $2, 3$. Again, let us compute some values of $m(n)$:

n	-2	-1	0	1	2
$m(n) = n^3 - n - 51$	1	5	3	1	5

Using $n = 0, 1$, we see that $m(x)$ has no root mod 2, thus $(2) = P_2$ is already a prime ideal, and $N(P_2) = 8$. Using $n = 0, 1, 2$, we see that $m(x)$ has 1 root mod 3. Since $3 \mid \operatorname{disc} K$ we know it ramifies. Hence $(3) = P_3^3$ and $N(P_3) = 3$.

At this point, we know the only prime ideal of $\mathbb{Z}[\alpha]$ of norm $\leq M_K$ is P_3. Since $P_3 = (3, \alpha) = (\alpha)$ is principal, it means $\mathrm{Cl}(K) = \{1\}$.

But, for fun, let us factor (5). Using the entire table (a complete list of representatives mod 5), we see that $m(x)$ has 2 roots mod 5. Also $5 \mid \operatorname{disc} K$ so it ramifies. So we can factor:

$$(5) = (5, \alpha + 1)(5, \alpha - 2)P_5$$

where $P_5 = (5, \alpha + 1)$ or $P_5 = (5, \alpha - 2)$. Let us figure out what P_5 is. in $\mathbb{F}_5[x]$, write:

$$x^3 - 3x + 3 = (x + 1)(x - 2)(x - a)$$

The constant term is $2a = 3$, so $a = -1 \pmod 5$. Hence $P_5 = (5, \alpha + 1)$ and:

$$(5) = (5, \alpha + 1)^2(5, \alpha - 2)$$

Lecture 30, 2024/07/15

5 Structure of Units

5.1 Dirichlet's Unit Theorem

Theorem 5.1 (Dirichlet's Unit Theorem). Let K be a number field and $\mathcal{O}_K$ its ring of integers. Say $[K:\mathbb{Q}] = n$ and $n = r + 2s$ as usual. Then:

$$\mathcal{O}_K^* \cong T \times \mathbb{Z}^{r+s-1}$$

where $\mathcal{O}_K^*$ is the group of units of $\mathcal{O}_K$, and $T = \{\text{roots of unity in } K\}$.

Note that T is finite:

First, the roots of unity are the roots of $x^n - 1$, so they are algebraic integers. Also recall that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$ where ζ_n is the primitive n-th root of unity. To show T is finite, it is enough to show for every $B \in \mathbb{R}$, the set:

$$\{n \in \mathbb{Z} : \phi(n) < B\}$$

is finite. Fix such $B \in \mathbb{R}$, for any $n \in \mathbb{Z}$ write $n = p_1^{e_1} \cdots p_r^{e_r}$, then:

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) = n \prod_{p|n} \frac{p-1}{p}$$

If $\phi(n) < B$, then:

$$n \prod_{p|n} \frac{p-1}{p} < B$$

Whcih implies that:

$$n \prod_{p|n} (p-1) < B \prod_{p|n} p \leq nB \implies \prod_{p|n} (p-1) \leq B$$

So there are only finitely many prime numbers $\{p_1, \cdots, p_r\}$ that divide any n with $\phi(n) < B$. For each i, we have $p_i^{b_i - 1} > B$ for some $b_i \geq 1$. Then:

$$n \cdot \frac{\prod_{p|n}(p-1)}{\prod_{p|n} p} < B \implies p_i^{e_i - 1} < B \implies e_i < b_i$$

It follows that there are only finitely many possible exponents with finitely many primes, so T is finite.

Theorem 5.2. Let $\alpha \in \mathcal{O}_K$, then $\alpha \in \mathcal{O}_K^*$ if and only if $N(\alpha) = \pm 1$.

Proof: ($\Rightarrow$). If $\alpha \in \mathcal{O}_K^*$, then $\alpha\beta = 1$ for some $\beta \in \mathcal{O}_K$, so $N(\alpha\beta) = 1$. This means $N(\alpha)N(\beta) = 1$, thus $N(\alpha) = \pm 1$.

($\Leftarrow$). Say $N(\alpha) = \pm 1$, then $N((\alpha)) = 1$. So $\mathcal{O}_K/(\alpha)$ has only 1 element. In particular, $1 \in (\alpha)$ and thus α must be a unit. □

Define a set:

$$U_K = \{(v_1, \cdots, v_n) \in V_K : v_1 \cdots v_n \neq 0\}$$

Define a map $\psi : U_K \to \mathbb{R}^n$ by:

$$\psi(v_1, \cdots, v_n) = (\log|v_1|, \cdots, \log|v_n|)$$

This is a homomorphism of groups from $(U_K, \cdot)$ to $(\mathbb{R}^n, +)$. Note that the image of $\mathcal{O}_K \setminus \{0\}$ in V_K lies in U_K because:

$$\begin{aligned} 0 \neq N(\alpha) &= \text{product of the conjugates of } \alpha \\ &= \text{product of the coordinates of the image of } \alpha \text{ in } V_K \end{aligned}$$

Theorem 5.3. Let $\alpha \in \mathcal{O}_K$, then $\alpha \in T$ if and only if $|\sigma_i(\alpha)| = 1$ for all embeddings $\sigma_i : K \hookrightarrow \mathbb{C}$.

Proof: ($\Rightarrow$). Easy, conjuages of α are also roots of unity.

($\Leftarrow$). Say $|\sigma_i(\alpha)| = 1$ for all i, then $|\sigma_i(\alpha^n)| = 1$ for all $n \in \mathbb{Z}$. Thus the set $\{\alpha^n\}$ is bounded in V_K. Therefore $\{\alpha^n\}$ is finite, giving $\alpha^n = \alpha^m$ for some $n \neq m$. So $\alpha^{n-m} = 1$, done. □

By this theorem, we notice that $\operatorname{Ker}\psi|_{\mathcal{O}_K^*} = T$, because $\log|v_i| = 0 \iff |v_i| = 1$.

Proof of Dirichlet Unit: We will start by showing $\psi(\mathcal{O}_K^*)$ is discrete in $\mathbb{R}^n$. By this we mean for all $x \in \psi(\mathcal{O}_K^*)$, there is $\epsilon > 0$ such that for all $y \in \psi(\mathcal{O}_K^*)$ we have $x \neq y$ implies $|x - y| \geq \epsilon$.

Lemma 5.4. Say $L \subseteq \mathbb{R}^n$ is a discrete subgroup. That is, L is discrete in $\mathbb{R}^n$ with the usual Euclidean metric, and is a subgroup of $\mathbb{R}^n$ as an additive group. Then L is finitely generated by at most n elements.

Lecture 31, 2024/07/17

Proof: Let $A \subseteq L$ be a finitely generated subgroup of L. It suffices to show A can be generated by n elements. Let $\{v_1, \cdots, v_m\}$ be a basis of A as a $\mathbb{Z}$-module. Assume $m > n$. Reorder v_i so that $\{v_1, \cdots, v_k\}$ is a maximal linearly independent subset of $\mathbb{R}^n$. Write:

$$v_{k+1} = a_1 v_1 + \cdots + a_k v_k$$

for $a_1, \cdots, a_k \in \mathbb{R}$. And WLOG, assume $a_1 \notin \mathbb{Q}$ (because $\{v_1, \cdots, v_k, v_{k+1}, \cdots, v_m\}$ is linearly independent over $\mathbb{Z}$). Let:

$$B = \operatorname{Span}_{\mathbb{Z}}\{v_1, \cdots, v_k\} \subseteq A$$

and let $D = \{x_1 v_1 + \cdots + x_k v_k : x_i \in [0,1]\}$. So if V is the $\mathbb{R}$-span of A, every $v \in V$ can be written as $v = x + b$ for $x \in D$ and $b \in B$. Consider the set $\{v_{k+1}, 2v_{k+1}, \cdots\}$. Write:

$$\begin{aligned} v_{k+1} &= a_1 v_1 + \cdots + a_k v_k \\ 2v_{k+1} &= 2a_1 v_1 + \cdots + 2a_k v_k \end{aligned}$$

also, write $\{x\} = x - [x]$ to be the fractional part of x. So the sequence $(\{ra_1\})$ is infinite because $a \notin \mathbb{Q}$. Now, we define:

$$P_r = \{ra_1\}v_1 + \cdots + \{ra_k\}v_k$$

Then $\{P_r\}$ is also infinite. But D is compact, so $\{P_r\}$ has a cluster point. In particular, for any $\epsilon > 0$ there are P_r, P_t such that $|P_r - P_t| < \epsilon$. But since $P_r - P_t \in A$, this means A contains vectors of arbitrary positive length, which it does not. □

So $\psi(\mathcal{O}_K^*)$ is a free abelian group of rank at most n. This is too big, how do we do better?

$$\psi(v_1, \cdots, v_n) = (\log|v_1|, \cdots, \log|v_n|)$$

Since $v_1, \cdots, v_r \in \mathbb{R}$ and $v_i = \overline{v_{i+1}}$ for $i \geq r$, so:

$$\begin{gathered} \log|v_{r+1}| = \log|v_{r+2}| \\ \vdots \\ \log|v_{n-1}| = \log|v_n| \end{gathered}$$

Hence $\psi(\mathcal{O}_K^*)$ satisfies s additional constraints. And $|N(u)| = 1$ if $u \in \mathcal{O}_K^*$, so $\psi(\mathcal{O}_K^*)$ also satisfies:

$$\log|v_1| + \cdots + \log|v_n| = 0$$

So $\psi(\mathcal{O}_K^*) \subseteq H$, where:

$$H = \left\{x_{r+1} = x_{r+2}, \cdots, x_{n-1} = x_n, \sum x_i = 0\right\}$$

and $\dim_{\mathbb{R}} H = r + s - 1$. Thus $\psi(\mathcal{O}_K^*)$ is a free abelian group of ranke $\leq r + s - 1$. Next, we want to show the rank of $\psi(\mathcal{O}_K^*)$ is $\geq r + s - 1$.

Our plan is to find a compact subset D such that every element of H is equal to $d + u$ for some $d \in D$ and $u \in \psi(\mathcal{O}_K^*)$. First we justify the awesomeness of our plan.

Lemma 5.5. A lattice $L \subseteq V$ spans V (as a $\mathbb{R}$-vector space) if and only if there is a bounded set B such that:

$$V = \bigcup_{\gamma \in L} (\gamma + B)$$

Proof: ($\Rightarrow$). Let $\dim V = n$ and $\{v_1, \cdots, v_n\}$ a basis of L and let:

$$B = \{a_1 v_1 + \cdots + a_n v_n : a_i \in [0,1]\}$$

then we are done.

($\Leftarrow$). Let $W = \operatorname{Span} L$ in V. Let $v \in V$, we want to show $v \in W$. Well:

$$nv = \gamma_n + b_n \text{ where } \gamma_n \in L,\ b_n \in B$$

Then we have:

$$v = \frac{\gamma_n}{n} + \frac{b_n}{n}$$

hence:

$$v = \lim_{n\to\infty} v = \lim_{n\to\infty}\left(\frac{\gamma_n}{n} + \frac{b_n}{n}\right) = \lim_{n\to\infty}\frac{\gamma_n}{n} + \underbrace{\lim_{n\to\infty}\frac{b_n}{n}}_{=0}$$

Therefore $v = \lim\limits_{n\to\infty} \frac{\gamma_n}{n} \in W$, as desired. □

Lecture 32, 2024/07/19

So far, we know that $\mathcal{O}_K^* \cong T \cong \mathbb{Z}^t$ with $t \leq r + s - 1$. And we know $\psi(\mathcal{O}_K^*)$ is discrete in H, where H is defined by:

$$H = \left\{x_{r+1} = x_{r+2}, \cdots, x_{n-1} = x_n, \sum x_i = 0\right\}$$

Now we need to show that $t \geq r + s - 1$. Now choose $c = (c_1, \cdots, c_n) \in V_K$ so that $c_i > 0$ and $c_{r+1} = c_{r+2}, \cdots, c_{n-1} = c_n$ and $A = c_1 \cdots c_n$. Choose c so that:

$$A > \left(\frac{4}{\pi}\right)^s |\operatorname{disc} K|$$

Let $X = \{(v_1, \cdots, v_n) \in V_K : |v_i| < c_i\}$. For $y = (y_1, \cdots, y_n) \in V_K$, define:

$$X_y = \{(v_1, \cdots, v_n) : |v_i| < c_i |y_i|\}$$

If $y_1 \cdots y_n = 1$ and $y_{r+1} = y_{r+2}, \cdots, y_{n-1} = y_n$, then $\operatorname{Vol}(X_y) = \operatorname{Vol}(X) = A$.

Now, Minkowski's Lemma gives us a nonzero vector $a \in \mathcal{O}_K \cap X_y$. There is a finite set $\{b_1, \cdots, b_t\} \subseteq \mathcal{O}_K$ such that if $x \in \mathcal{O}_K$ satisfies $N(x) < A$, then $x = ub_j$ for some j and some $u \in \mathcal{O}_K^*$. The existence of the b_i derives from the fact that there are only finitely many ideals of norm $< A$, and two elements generating the same ideal are associative. Define:

$$B = \underbrace{\psi^{-1}(H)}_{\text{closed}} \cap \underbrace{\bigcup_j X_{b_j^{-1}}}_{\text{compact}} \subseteq U_K$$

Therefore B is compact. If $y \in \psi^{-1}(H)$, want to show $y \in u^{-1}B$ for some $u \in \mathcal{O}_K^*$. There is some nonzero $a \in \mathcal{O}_K \cap X_{y^{-1}}$, which implies:

$$\begin{aligned} ay \in X \implies N(a) < A &\implies a = ub_j \text{ for some } u \in \mathcal{O}_K^* \\ &\implies y \in X_{a^{-1}} = X_{u^{-1}b_j^{-1}} \\ &\implies y \in u^{-1}(X_{b_j^{-1}}) \subseteq u^{-1}B \end{aligned}$$

Thus $\psi(B)$ is the compact set we seek. □

Lecture 33, 2024/07/22

Example. Let $[K : \mathbb{Q}] = 2$ be a quadratic extension.

If $K/\mathbb{Q}$ is imaginary, then $r = 0$ and $s = 1$. Then:

$$\mathcal{O}_K^* = T \cong \begin{cases} \mathbb{Z}/4\mathbb{Z} & \text{if } K = \mathbb{Q}(i) \\ \mathbb{Z}/6\mathbb{Z} & \text{if } K = \mathbb{Q}(\sqrt{-3}) \\ \mathbb{Z}/2\mathbb{Z} & \text{otherwise} \end{cases}$$

Together with $\mathbb{Q}$, these are the only K such that $\mathcal{O}_K^*$ is finite.

If $K/\mathbb{Q}$ is real, then $r = 2$ and $s = 0$. So:

$$\mathcal{O}_K^* \cong T \times \mathbb{Z} = \{\pm 1\} \times \mathbb{Z}$$

In other word, there is a unit $u \in \mathcal{O}_K^*$ such that every element $x \in \mathcal{O}_K^*$ can be written as $\pm u^n$. And this isomorphism from $\mathcal{O}_K^*$ to $\{\pm 1\} \times \mathbb{Z}$ is given by:

$$\mathcal{O}_K^* \to \{\pm 1\} \times \mathbb{Z} \ \text{ by } \ su^n \mapsto (s, n)$$

where $s \in \{\pm 1\}$. Such u is called a **fundamental unit**.

Remark. In general, Dirichlet's Theorem says:

$$\mathcal{O}_K^* \cong T \cong \mathbb{Z}^{r+s-1}$$

This means there are fundamental units $u_1, \cdots, u_m$ where $m = r + s - 1$ such that every $x \in \mathcal{O}_K^*$ can be written as $x = \zeta u_1^{n_1} \cdots u_m^{n_m}$, where $\zeta \in \mathcal{O}_K$ is a root of unity. The isomorphism is given by:

$$\mathcal{O}_K^* \to T \cong \mathbb{Z}^{r+s-1} \ \text{ by } \ \zeta u_1^{n_1} \cdots u_m^{n_m} \mapsto (\zeta, n_1, \cdots, n_m)$$

Let us go back to quadratic extensions. What does a fundamental unit look like?

Number Fields	$\mathbb{Q}(\sqrt{2})$	$\mathbb{Q}(\sqrt{93})$	$\mathbb{Q}(\sqrt{94})$	$\mathbb{Q}(\sqrt{95})$
Fundamental Unit	$1+\sqrt{2}$	$13+3\left(\frac{1+\sqrt{19}}{2}\right)$	$2143295+221064\sqrt{94}$	$39+4\sqrt{95}$

If $a+b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]^*$ is a unit, then:

$$a^2 - db^2 = \pm 1$$

This is called the **Pell's Equation**. In fact, finding fundamental units is the same as finding the "fundamental solutions" to this Pell's Equation.

Example. If $[K:\mathbb{Q}] = 3$, two cases:

$$\begin{aligned}(r,s) = (1,1) &\implies \mathcal{O}_K^* \cong T \times \mathbb{Z} \\ (r,s) = (3,0) &\implies \mathcal{O}_K^* \cong T \times \mathbb{Z}^2\end{aligned}$$

Example. If $[K:\mathbb{Q}] = 4$, three cases:

$$\begin{aligned}(r,s) = (0,2) &\implies \mathcal{O}_K^* \cong T \times \mathbb{Z} \\ (r,s) = (2,1) &\implies \mathcal{O}_K^* \cong T \times \mathbb{Z}^2 = \{\pm 1\} \times \mathbb{Z}^2 \\ (r,s) = (4,0) &\implies \mathcal{O}_K^* \cong T \times \mathbb{Z}^3 = \{\pm 1\} \times \mathbb{Z}^3\end{aligned}$$

5.2 Cyclotomic Fields

Let $K = \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n-th root of unity. What is $\mathcal{O}_K$? Our first guess is $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$. We know that disc $\mathbb{Z}[\zeta_n]$ is a divisor of n^n, so if $n \notin P$ then $\mathbb{Z}[\zeta_n]_P$ is a DVR. So assume P is a prime ideal with $n \in P$. If we can prove that $\mathbb{Z}[\zeta_n]_P$ is a DVR, then $\mathcal{O}_k = \mathbb{Z}[\zeta_n]$.

First, assume $n = p^a$. Then we may assume $p \in P$, and we have:

$$\mathbb{Z}[\zeta_n]/(p) \cong \mathbb{F}_p[x]/(\Phi_n(x)) \cong \mathbb{F}_p[x]/(x-1)^{\phi(n)}$$

where $\Phi_n(x)$ is the n-th cyclotomic polynomial. Hence $P = (p, 1-\zeta_n)$. But $|N(1-\zeta_n)| = p$ because:

$$|N(1-\zeta_n)| = |\Phi_n(1)| = |\Phi_{p^a}(1)|$$

And $\Phi_{p^a}(1) = p$ as $\Phi_{p^a}(x) = (x^{p^a})^{p-1} + (x^{p^a})^{p-2} + \cdots + 1$. Hence $P = (1-\zeta_n)$ is principal, so $\mathbb{Z}[\zeta_n]_P$ is a DVR. Therefore, if $n = p^a$ then $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$.

Lecture 34, 2024/07/24

Theorem 5.6. Say K, L are Galois number fields with $\gcd(\operatorname{disc} K, \operatorname{disc} L) = 1$. If $\mathcal{O}_K$ and $\mathcal{O}_L$ have integral basese $\{v_1, \cdots, v_n\}$ and $\{w_1, \cdots, w_m\}$, respectively. Then the composition field KL has ring of integer $\mathcal{O}_{KL}$ with integral basis $\{v_i w_j\}$.

Proof: Note that $[KL : \mathbb{Q}] = [K : \mathbb{Q}][L : \mathbb{Q}]$, so $\{v_i w_j\}$ has the correct number of elements to be a basis of $\mathcal{O}_{KL}$, namely nm. So if we can show it spans $\mathcal{O}_{KL}$, they must be a basis. So let $\alpha \in \mathcal{O}_{KL}$, since $\{v_i w_j\}$ is a basis of $KL/\mathbb{Q}$, we can write:

$$\alpha = \sum \alpha_{ij} v_i w_j \tag{1}$$

for $\alpha_{ij} \in \mathbb{Q}$. We want to show $\alpha_{ij} \in \mathbb{Z}$ for all i, j. Let $\beta_j = \sum_i \alpha_{ij} v_i$, the coefficient of w_j in (1). Now, we write:

$$\operatorname{Gal}(KL/L) = \{\sigma_1, \cdots, \sigma_n\}$$
$$\operatorname{Gal}(KL/K) = \{\tau_1, \cdots, \tau_m\}$$

Let T be the matrix $(\tau_i w_j)$ and:

$$v = (\tau_1 \alpha, \cdots, \tau_m \alpha) \quad \text{and} \quad w = (\beta_1, \cdots, b_m)$$

Then we have $(\det T)^2 = \operatorname{disc} L$. And $v = Tw$ implies $T^* v = (\det T) w$ by Cramer's Rule. So $(\det T)\beta_j \in \mathcal{O}_{KL}$ for all j, which means:

$$\operatorname{disc} L \cdot \beta \in \mathcal{O}_{KL} \ \text{ for all } \ j \implies \operatorname{disc} L \cdot \alpha_{ij} \in \mathcal{O}_K \ \text{ for all } \ i, j$$

Thus we have $\operatorname{disc} L \cdot \alpha_{ij} \in \mathbb{Z}$ for all i, j. Switch the role of K and L gives us that $\operatorname{disc} K \cdot \alpha_{ij} \in \mathbb{Z}$ for all i, j. Since $\gcd(\operatorname{disc} K, \operatorname{disc} L) = 1$, this implies $\alpha_{ij} \in \mathbb{Z}$ for all i, j. As desired. □

Now we will show that the ring of integers of $\mathbb{Q}(\zeta_n)$ is $\mathbb{Z}[\zeta_n]$. Note that if:

$$n = p_1^{a_1} \cdots p_r^{a_r}$$

then $\mathbb{Q}(\zeta_n)$ is the compositum of fields:

$$\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{p_1^{a_1}}) \cdots \mathbb{Q}(\zeta_{p_r^{a_r}})$$

The discriminant of $\mathbb{Q}(\zeta_{p_i^{a_i}})$ are powers of p_i, so they are pairwise coprime. By applying the theorem $r-1$ times, we find the irng of integers of $\mathbb{Q}(\zeta_n)$ has integral basis:

$$\left\{ \zeta_{p_1^{a_1}}^{b_1}, \cdots, \zeta_{p_r^{a_r}}^{b_r} \right\}$$

for $0 \leq b_i \leq a_i - 1$. Every element in the set is a power of ζ_n, so the ring of integers of $\mathbb{Q}(\zeta_n)$ is contained in $\mathbb{Z}[\zeta_n]$. Since $\mathbb{Z}[\zeta_n]$ is integral over $\mathbb{Z}$, we must have $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$.

So what are the units of $\mathbb{Z}[\zeta_n]$? Well, for $n \geq 3$ we have $r = 0$ and $s = \phi(n)/2$. Hence:

$$\mathbb{Z}[\zeta_n]^* \cong T \times \mathbb{Z}^{\frac{\phi(n)}{2} - 1}$$

The T parts are the roots of unity, whcih are $\{\pm\zeta_n^a\}$ for $a \in \mathbb{Z}$. The free part is harder to get hold of. Let us specialize to the case when $n = p$ is prime. Define:

$$\epsilon_a = \zeta_{2p}^{1-a} \left(\frac{1 - \zeta_p^a}{1 - \zeta_p} \right)$$

for $a \in \{1, \cdots, p-1\}$. We can show ϵ_a is a unit. First, $\epsilon_a \in \mathbb{Z}[\zeta_p]$ because $(1 - \zeta_p) \mid (1 - \zeta_p^a)$ and:

$$\frac{1}{\epsilon_a} = \zeta_{2p}^{a-1} \left(\frac{1 - \zeta_p}{1 - \zeta_p^a} \right)$$

Since $(a, p) = 1$, we know ζ_p is a power of ζ_p^a, so $(1 - \zeta_p^a) \mid (1 - \zeta_p)$ and hence $1/\epsilon_a \in \mathbb{Z}[\zeta_p]$. Also, $\phi(p) = p - 1$ so $s = (p-1)/2$. There are $(p-1)$ $\epsilon_a' s$, so they must satisfy some relations.

$$\begin{aligned}
\epsilon_a &= \zeta_{2p}^{-a-1} \left(\frac{1 - \zeta_p^{-a}}{1 - \zeta_p} \right) \\
&= \zeta_{2p}^{-a-1} \left(\frac{\zeta_p^a - 1}{\zeta_p^a - \zeta_p^{a+1}} \right) \\
&= \zeta_{2p}^{a+1} \zeta_{2p}^{-2a} \left(\frac{\zeta_p^a - 1}{1 - \zeta_p} \right) \\
&= \zeta_{2p}^{1-a} \left(\frac{1 - \zeta_p^a}{1 - \zeta_p} \right) (-1) \\
&= -\epsilon_a
\end{aligned}$$

So we are left with $(p-1)/2$ ϵ_a's that are not obviously dependent. Lastly,

$$\epsilon_1 = \zeta_{2p}^0 \left(\frac{1 - \zeta_p}{1 - \zeta_p} \right) = 1$$

Lecture 35, 2024/07/26

Example. Say $K = \mathbb{Q}(\alpha)$ with $\alpha^3 - 2\alpha^2 + 7\alpha + 1 = 0$. The polynomial $m(x) = x^3 - 2x^2 + 7x + 1$ has one real root. So $r = 1$ and $s = 1$. We have $\operatorname{disc} \mathbb{Z}[\alpha] = -1423$. This is prime, so $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Is the ideal $(3, \alpha + 1)$ principal? Dirichlet's Unit Theorem implies:

$$\mathcal{O}_K^* \cong \{\pm 1\} \times \mathbb{Z}$$

We can first show this ideal $P = (3, \alpha + 1)$ is prime.

$$\begin{aligned}\mathbb{Z}[\alpha]/(3, \alpha+1) &\cong \mathbb{Z}[x]/(3, x+1, x^3 - 2x^2 + 7x + 1) \\ &\cong \mathbb{F}_3[x]/(x+1, x^3 - 2x^2 + 7x + 1) \\ &\cong \mathbb{F}_3[x]/(x+1, -9) \\ &\cong \mathbb{F}_3\end{aligned}$$

Also we have $N(P) = 3$. If P is principal, then it is generated by an element of norm 3. How to find elements of norm 3? First, $N(\alpha) = 1$ so $\alpha \in \mathcal{O}_K^*$. The Minkowski maps:

$$\alpha \mapsto \left(\frac{1}{7}, 1 + \frac{5}{2}i, 1 - \frac{5}{2}i\right) \text{ in } V_K$$

roughly. Say $y \in \mathcal{O}_K$ has $N(y) = 3$, write $y = (y_1, y_2, \overline{y_2})$ in V_K. By multiplying by an appropriate $\pm\alpha^n$, we can make $1 \leq y_1 \leq 7$. Since $N(y) = 3$, we have $y_1|y_2|^2 = 3$, hence $|y_2| \leq \sqrt{3}$ because $y_1 \geq 1$. Therefore:

$$y \in [1, 7] \times \{|z| \leq \sqrt{3}\} \times \{|z| \leq \sqrt{3}\}$$

We want to look for points in $\{a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{Z}\}$ in this box, and check if they have norm 3. It turns out there are not any, so P is not principal.

6 p-adic numbers

Say A is a DVR with maximal ideal P. Let K be the fractional field of A. If $0 \neq x \in K$, define:

$$\operatorname{ord}_P(x) = \max_n \{n : x \in P^n\}$$

and define $\operatorname{ord}_P(0) = \infty$. In other words, recall that in a DVR any x can be written as $x = u\pi^n$ for some $u \in A^*$ and π an uniformizer. We define $n = \operatorname{ord}_P(x)$.

Example. In $A = \mathbb{Z}_{(5)}$, an uniformizer is $\pi = 5$. Since $25 = 5^2$ and $65 = 13 \cdot 5$, so:

$$\operatorname{ord}_5(25) = 2 \quad \text{and} \quad \operatorname{ord}_5(65) = 1$$

Also, since $17/25 = 17 \cdot 5^{-2}$ and $3/4 = 3 \cdot 2^{-2}$, we have:

$$\operatorname{ord}_5\left(\frac{17}{25}\right) = -2 \quad \text{and} \quad \operatorname{ord}_5\left(\frac{3}{4}\right) = 0$$

This ord_P is called the **discrete valuation** of the Discrete Valuation Ring A.

Definition. If $A = (\mathcal{O}_K)_P$ for some number field K and a prime ideal $P \subseteq \mathcal{O}_K$. We define:

$$\|x\|_P = N(P)^{-\operatorname{ord}_P(x)}$$

for $x \in K$. For example, we have:

$$\|25\|_5 = 5^{-2} \quad \text{and} \quad \left\|\frac{3}{4}\right\|_5 = 1$$

It can be shown that this $\|\cdot\|_P$ is a norm because it satisfies:

(1) $\|x\|_P\|y\|_P = \|xy\|_P$.

(2) $\|x\|_P = 0$ if and only if $x = 0$.

(3) $\|x+y\|_P \leq \|x\|_P + \|y\|_P$.

This is called the ***P*-adic norm** on K.

Say $P \neq Q$ are prime ideals of $\mathcal{O}_K$. Are $\|\cdot\|_P$ and $\|\cdot\|_Q$ equivalent norms? NO! If $P \neq Q$, take $x \in P \setminus Q$ and $y \in Q \setminus P$. Hence:

$$\left\|\frac{x}{y}\right\|_P < 1 \quad \text{and} \quad \left\|\frac{x}{y}\right\|_Q > 1$$

Then we have:

$$\lim_{n\to\infty}\left\|\left(\frac{x}{y}\right)^n\right\|_P = 0 \text{ and } \lim_{n\to\infty}\left\|\left(\frac{x}{y}\right)^n\right\|_Q = \infty$$

which means $\|\cdot\|_P$ and $\|\cdot\|_Q$ cannot be equivalent norms.

Theorem 6.1 (Ostrowski). Any norm on K is equivalent to $\|\cdot\|_P$ for some $P \subseteq \mathcal{O}_K$ or is equivalent to the norm induced from some embeddings $K \to \mathbb{C}$.

Say $K = \mathbb{Q}$ and $p \in \mathbb{Z}$ a prime. For any $n \in \mathbb{Z}$, we write it in base p:

$$n = a_0 + a_1 p + \cdots + a_r p^r$$

where $a_i \in \{0, \cdots, p-1\}$. So the series:

$$\sum_{i=0}^{\infty} a_i p^i$$

converges for any $a_i \in \{0, \cdots, p-1\}$ in the p-adic norm, because $\|p\|_p = p^{-1} < 1$.

Definition. The ***p*-adic integers** is defined by:

$$\mathbb{Z}_p = \left\{\sum_{i=0}^{\infty} a_i p^i : a_i \in \{0, \cdots, p-1\}\right\}$$

These are numbers of the form:

$$\cdots a_5 a_4 a_3 a_2 a_1 a_0$$

Definition. The field of p**-adic numbers** is defined by:

$$\mathbb{Q}_p = \left\{ \sum_{i=-k}^{\infty} a_i p^i : a_i \in \{0, \cdots, p-1\} \right\}$$

These are numbers of the form:

$$\cdots a_5 a_4 a_3 a_2 a_1 a_0 . a_{-1} \cdots a_{-k}$$

It is basically a p-adic integer with finitely many digits after the dot.

Remark. But, how do we distinguish positive and negative numbers? In $\mathbb{Z}_3$, define:

$$x = \cdots 22222$$

with $x = \sum a_i 3^i$ with $a_i = 2$ for all i. Then $x + 1 = 0$, because adding 1 in the first digit will result in carrying 1 in all the other digits. Therefore $x = -1$. In general, if we define:

$$x = \sum_{i=0}^{\infty} a_i p^i = \sum_{i=0}^{\infty} (p-1) p^i$$

Then $x + 1 = 0$ in $\mathbb{Z}_p$, so x is the additive inverse of 1 in $\mathbb{Z}_p$.

Lecture 36, 2024/07/29

In $\mathbb{Z}_p$, an element is of the form:

$$\cdots a_3 a_2 a_1 a_0 = x$$

We can think of a_0 as $x \pmod p$, think of $a_1 a_0$ as $x \pmod{p^2}$. In general, we have a correspondence:

$$x \leftrightarrow (b_1, b_2, b_3, \cdots)$$

with $b_n \in \mathbb{Z}/p^n\mathbb{Z}$ and $b_{n+m} \equiv b_m \pmod{p^n}$. So we can identify $\mathbb{Z}_p$ as a subring of:

$$\mathbb{Z}_p \subseteq \prod_{n=1}^{\infty} (\mathbb{Z}/p^n\mathbb{Z})$$

And addition and multiplication are component-wise.

Proposition 6.2. The polynomial $x^2 + 1$ splits in $\mathbb{Q}_5$.

Proof: We need to find a 5-adic number $x = (b_1, b_2, \cdots)$ with $x^2 = -1$ in $\mathbb{Q}_5$. Since multiplication is component-wise, we need $b_1^2 \equiv -1 \pmod 5$, so we can take $b_1 = 2$. For b_2, we need:

$$b_2^2 \equiv -1 \pmod{25}$$
$$b_2 \equiv 2 \pmod 5$$

This is possible because $4 \mid \phi(25)$, where ϕ is the Euler's function. Similarly, we need:

$$b_3^2 \equiv -1 \pmod{125}$$
$$b_3 \equiv b_2 \pmod{5}$$

This is also possible since $4 \mid \phi(125)$. Continue this way, since $4 \mid \phi(5^n)$ for all $n \geq 1$, we can construct $x = (2, b_2, b_3, \cdots)$ such that $x^2 = -1$ in $\mathbb{Q}_5$. As desired. □

Lemma 6.3 (Hensel). Say $f(x) \in \mathbb{Z}_p[x]$ is monic with no repeated factors. If $f(x) \equiv 0 \pmod{p}$ has a solution, then $f(x) = 0$ has a solution in $\mathbb{Z}_p$. (Equivalently, if $f(x)$ has a root mod p, then it has a solution mod p^n for every $n \geq 1$).