Math Comps Fall 2023

Alistair Pattison | October 23, 2023

1 Goals

Finiteness of class group (proved as a corrolary to Theorem 35 on page 91 of chapter 5.

Dirichlet's unit theorem (Theorem 38 on page 100 of chapter 5).

2 Chapter 1

Algebraic number theory is the study of number fields: finite extensions of the rationals $\mathbb{Q}(a_1, \ldots, a_n)$.

***Example* 2.0.1.** The extension $\mathbb{Q}[i]$

Theorem 2.1 (Fermat's Last Theorem)**.** *For $n > 2$, the equation $x^n + y^n = z^n$ has no solutions.*

Definition 2.2 (Class number)**.** *Let p be a prime and take ω to be the pth root of unity $e^{2\pi i/p}$. Then, the* class number of the ring $\mathbb{Z}[\omega]$ (or the *class number of p) is the number of equivalence classes under the following relation on the ideals of $\mathbb{Z}[\omega]$:*

$$A \sim B \text{ iff } \alpha A = \beta B \text{ for some } \alpha, \beta \in \mathbb{Z}[\omega].$$

Let $h : ¶ \to \mathbb{N}$ be the function that gives the class number for a prime p.

The relation $\sim$ above is an equivalence relation.

***Example* 2.2.1.**

Definition 2.3 (Regular primes)**.** *A prime p is* regular if $p \nmid h$

Definition 2.4 (Ideal class group)**.**

3 Number Fields and Number Rings

Definition 3.1 (Number field)**.** *A* number field is a field $K \subset \mathbb{C}$ with $\deg_{\mathbb{Q}} K$ finite.

Theorem 3.2. *Every number field has the form $\mathbb{Q}[\alpha]$ for some algebraic number $\alpha \in \mathbb{C}$.Furthermore, if d is the degree of the minimal polynomial of α, then the set $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ is a basis for $\mathbb{Q}[\alpha]$.*

Proof. Given in Appendix B of Marcus. □

Definition 3.3 (Cyclomatic field)**.** *Let $\omega_p = e^{2\pi i/m}$ for some $m \in \mathbb{N}$. Then, the field $\mathbb{Q}[\omega_p]$ is the* mth cyclomatic field.

Theorem 3.4. *The degree of the mthe cyclomatic field is $\varphi(m)$.*

Definition 3.5 (Quadratic field)**.** *A* quadratic field is a field of the form $\mathbb{Q}[\sqrt{m}]$ for any non-square $m \in \mathbb{Z}$. If $m < 0$, we call $Q[\sqrt{m}]$ an imaginary quadratic field. If $m > 0$, we call $Q[\sqrt{m}]$ a real quadratic field.

Theorem 3.6. *All quadratic fields have degree 2 over $\mathbb{Q}$ with basis $\{1, \sqrt{m}\}$.*

Theorem 3.7. *Quadratic fields for squarefree m are all distinct.*

***Example* 3.7.1.** $\mathbb{Q}[\sqrt{-3}] = Q[\omega_6]$

Definition 3.8 (Algebraic integer)**.** *A number $\alpha \in \mathbb{C}$ is an* algebraic integer if it's the root of a monic polynomial $f \in \mathbb{Z}[x]$. We denote the sum of all algebraic integers as $\mathcal{A}$.

Theorem 3.9. *Let α be an algebraic integer with a monic vanishing polynomial $f \in \mathbb{Z}[x]$ of minimal degree. Then f is irredicible over $\mathbb{Q}$.*

Theorem 3.10. *The followign are equivalent for $a \in \mathbb{C}$*

(i) α is an algebraic integer,

(ii) The (addative) group $\mathbb{Z}[\alpha]$ is finitely generated,

(iii) α is a member of some subring R of $\mathbb{C}$ where $(R, +)$ is finitely generated,

(iv) $\alpha A \subset A$ for some finitely-generated additive subgroup $A \subset \mathbb{C}$.

Corrolary 3.11. *If $\alpha, \beta \in \mathbb{A}$, then $\alpha + \beta, \alpha\beta \in \mathbb{A}$.*

Definition 3.12 (Number ring)**.** *The* number ring of a number field K is the ring $R = \mathbb{A} \cap K$.

***Example* 3.12.1.** The corresponding number ring for the cyclomatic field $\mathbb{Q}[\omega]$ is $\mathbb{A} \cup \mathbb{Q}[\omega] = \mathbb{Z}[\omega]$.

Definition 3.13 (Embeddings)**.** *An embedding of a field K in a field F is a ring homomorphism $\sigma : K \to F$.*

Theorem 3.14. *Any embedding is injective.*

Definition 3.15 (Trace and norm)**.** *Let K be a number field with embeddings $\sigma_1, \ldots, \sigma_n : K \to \mathbb{C}$ with $n = [K : \mathbb{C}]$. Then, the trace of some element $\alpha \in K$ is*

$$T(\alpha) = \sigma_1(\alpha) + \cdots \sigma_n(\alpha) \tag{1}$$

and the norm is

$$N(\alpha) = \sigma_1(\alpha) \cdots \sigma_n(\alpha). \tag{2}$$

Definition 3.16.

$$t(n) = \tag{3}$$

Theorem 3.17. *Let K be a number field with an element $\alpha \in K$ Let d be the degree of α and $n = [K : \mathbb{C}]$. Then,*

$$T(\alpha) = \frac{n}{d} t(\alpha) \tag{4}$$

and

$$N(\alpha) = (n(\alpha))^{n/d}. \tag{5}$$

Corrolary 3.18. *$T(\alpha)$ and $N(\alpha)$ are rational.*

Corrolary 3.19. *If α is an algebraic integer, then $T(\alpha)$ and $N(\alpha)$ are integers.*

Definition 3.20 (Relative trace and norm)**.** *Let $K \subset L$ be two number fields and let $\sigma_1, \ldots, \sigma_n$ be the $n = [K : L]$ embeddings of L in $\mathbb{C}$ that fix K pointwise. Then, for $\alpha \in L$, the relative trace is*

$$T_K^L(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_n(\alpha) \tag{6}$$

and the relative norm is

$$N_K^L(\alpha) = \sigma_1(\alpha) \cdots \sigma_n(\alpha). \tag{7}$$

Theorem 3.21. *Let $\alpha \in L$ and take $d \coloneqq \deg_K(\alpha)$. Then,*

Corrolary 3.22. *The relative trace and norm of α are in K. If $\alpha \in \mathbb{A} \cap L$, then they are in $\alpha \cap K$.*

Theorem 3.23 (Transitivity of the trace and norm)**.** *Let $K \subset L \subset M$ be number fields. Then, for all $\alpha \in M$,*

$$T_K^L(T_L^M(\alpha)) = T_K^M(\alpha), \tag{8}$$

$$N_K^L(N_L^M(\alpha)) = N_K^M(\alpha). \tag{9}$$

Proof. □

Definition 3.24 (Discriminant)**.** *Let K be a number field of with degree n over $\mathbb{Q}$. Let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K in $\mathbb{C}$. Then, the discriminant of $\alpha_1, \ldots, \alpha_n \in K$ is*

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i(\alpha_j))^2 \quad = \det \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \\ \sigma_n(\alpha_1) & & \sigma_n(\alpha_n) \end{pmatrix}^2. \tag{10}$$

Theorem 3.25 (Discriminant with respect to the trace)**.**

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det\left(T(a_i a_j)\right)_{ij} \tag{11}$$

Theorem 3.26 (Discriminant of linearly dependent numbers)**.** $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = 0$ *iff $\alpha_1, \ldots, \alpha_n$ are linearly dependent.*

4 Prime Decompositions

Definition 4.1 (Integral)**.** *Let $S \subseteq R$ be rings with $\alpha \in R$. Then, b is integral over S if there exists a monic $f \in S[x]$ such that $f(\alpha) = 0$.*

Definition 4.2 (Dedekind domain)**.** *A Dedekind domain is an integral domain R such that*

(i) every ideal is finitely generated,

(ii) every nonzero prime ideal is maximal,

(iii) R is integrally closed in its fraction field $K = \{a/b : a, b \in R, b \neq 0\}$.

Theorem 4.3. *Number rings are Dedekind domains.*

Theorem 4.4. *For all ideals I of a Dedekind domain R, there exists an ideal $J \subset R$ such that IJ is principal.*

Corrolary 4.5. *With chapter 1, exercise 32, this implies that the ideal class group is a group.*

Corrolary 4.6. *If A and B are ideals, then $A \mid B$ iff $A \supset B$.*

Theorem 4.7 (Unique factorization)**.** *Every ideal in a Dedekind domain R uniquely factors into primes ideals.*

Theorem 4.8 (Every Dedekind ideal is generated by two elements)**.** *Let I be an ideal of a Dedekind domain R and let $\alpha \in R$ be arbitrary. Then, there exists a $\beta \in R$ such that $R = (\alpha, \beta)$.*

Theorem 4.9. *A Dedekind domain is a UFD iff it's a PFD.*

Theorem 4.10. *Let $K \subset L$ be fields and $P \subset R = \mathcal{O}_K$ and $Q \subset S = \mathcal{O}_L$ be prime ideals of their corresponding number rings. Then, the following are equivalent*

(i) $Q \mid PS$,

(ii) $Q \supset PS$,

(iii) $Q \supset P$,

(iv) $Q \cap R = P$,

(v) $Q \cap K = P$.

List of Theorems

List of Figures

List of Tables