Math Comps Fall 2023

Alistair Pattison | October 4, 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 $h : \P \to \mathbb{N}$ 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 m*th cyclomatic field.

Theorem 3.4. *The degree of the $m$the 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 $R = \mathbb{A} \cup K$.

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

List of Theorems

List of Figures

List of Tables