E/Ea Thompson(they/them)

Math 641: Algebraic Number Theory

– In Pursuit of Abstract Nonsense –

Wednesday 30$^{\text{th}}$ August, 2023

Springer Nature

Preface

This is a collection of notes associated with Math 641 (Algebraic Number Theory) taken at the University of Calgary.

University of Calgary,

E/Ea Thompson (They/Them)
Wednesday 30th August, 2023

Contents

Notation

List of common notations used in these notes.

$\mathbb{N}$	Natural numbers
$\mathbb{Z}$	Integers
$\mathbb{Q}$	Rational numbers
$\mathbb{R}$	Real numbers
$\mathbb{C}$	Complex numbers

Chapter 1

Number Fields

Abstract Summary of material in chapter (to be completed after chapter)

1.1 Basic Concepts

A **number field** is a subfield of $\mathbb{C}$ having finite degree over $\mathbb{Q}$. Every such field has the form $\mathbb{Q}(\alpha)$ for some algebraic number $\alpha \in \mathbb{C}$. Note as the extension is finite $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$. If α is a root of an irreducible polynomial over $\mathbb{Q}$ having degree n, then

$$\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_i \in \mathbb{Q}\}$$

and $\{1, \alpha, ..., \alpha^{n-1}\}$ is a basis for $\mathbb{Q}[\alpha]$ as a vector space over $\mathbb{Q}$.

Consider $\omega = e^{2\pi i/m}$. The field $\mathbb{Q}[\omega]$ is called the m^{th} **cyclotomic field**. In general, for odd m, the m^{th} cyclotoic field is equal to the $2m^{th}$. On the other hand, cyclotomic fields for m even, $m > 0$, are all distinct.

Another infinite class of number fields consists of the **quadratic fields** $\mathbb{Q}[\sqrt{m}]$, $m \in \mathbb{Z}$, m not a perfect square. These fields have degree 2 over $\mathbb{Q}$, having basis $\{1, \sqrt{m}\}$. We need only consider squarefree m since, for example, $\mathbb{Q}[\sqrt{12}] = \mathbb{Q}[\sqrt{3}]$. The $\mathbb{Q}[\sqrt{m}]$, for m squarefree, are all distinct. The $\mathbb{Q}[\sqrt{m}]$, $m > 0$, are called the **real quadratic fields**; the $\mathbb{Q}[\sqrt{m}]$, $m < 0$, the **imaginary quadratic fields**.

Definition 1.1.1 A complex number is an **algebraic integer** if and only if it is a root of some monic (leading coefficient 1) polynomial with coefficients in $\mathbb{Z}$.

Note we do note require the polynomial to be irreducible over $\mathbb{Q}$.

Theorem 1.1.2 Let α be an algebraic integer, and let f be a monic polynomial over $\mathbb{Z}$ of least degree having α as a root. Then f is irreducible over $\mathbb{Q}$.

Lemma 1.1.3 Let f be a monic polynomial with coefficients in $\mathbb{Z}$, and suppose $f = gh$ where g and g are monic polynomials with coefficients in $\mathbb{Q}$. Then g and h actually have coefficients in $\mathbb{Z}$.

Proof Let m (resp. n) be the smallest positive integer such that mg (resp. nh) has coefficients in $\mathbb{Z}$. Then the coefficients of mg have no common factor. The same is true of the coefficients of nh. Using this, we can show that $m = n = 1$: If $mn > 1$, take any prime p dividing mn and consider the equation $mnf = (mg)(nh)$. Reducing coefficients $\mod p$, we obtain $0 \equiv (mg)(nh) \mod p$. But $\mathbb{Z}_p[x]$ is an integral domain, so either $mg \equiv 0$ or $nh \equiv 0 \mod p$. But then p divides all coefficients of either mg or nh; as we showed above, this is impossible. Thus $m = n = 1$, and hence $g, h \in \mathbb{Z}[x]$. □

We now can prove the preceding theorem.

Proof If f is not irreducible, then $f = hg$ where $g, h \in \mathbb{Q}[x]$ are nonconstant polynomials. Without loss of generality we can assume that g, h are monic. Then $g, h \in \mathbb{Z}[x]$ by the lemma. But α is a root of either g or h, and both have degree less than that of f. This is a contradiction. □

Corollary 1.1.4 The only algebraic integers in $\mathbb{Q}$ are the ordinary integers.

Corollary 1.1.5 Let m be a squarefree integer. The set of algebraic integers in the quadratic field $\mathbb{Q}[\sqrt{m}]$ is

$$\{a + b\sqrt{m} : a, b \in \mathbb{Z}\}, \quad \text{if } \; m \equiv 2 \text{ or } 3 \mod 4$$

$$\left\{\frac{a + b\sqrt{m}}{2} : a, b \in \mathbb{Z}, a \equiv b \mod 2\right\}, \quad \text{if } m \equiv 1 \mod 4$$

Proof Let $\alpha = r + s\sqrt{m}, r, s \in \mathbb{Q}$. If $s \neq 0$, then the monic irreducible polynomial over $\mathbb{Q}$ having α as a root is

$$x^2 - 2rx + r^2 - ms^2$$

Thus α is an algebraic integer if and only if $2r$ and $r^2 - ms^2$ are both integer. This can be used to obtain the result. □

Theorem 1.1.6 The following are equivalent for $\alpha \in \mathbb{C}$:

(1) α is an algebraic integer;
(2) $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module;
(3) There exists a subring B of $\mathbb{C}$ containing α which is finitely generated as a $\mathbb{Z}$-module;
(4) $\alpha A \subseteq A$ for some finitely generated $\mathbb{Z}$-submodule of $\mathbb{C}$.

Proof (1) implies (2) follows from the fact that α is a root of a monic polynomial over $\mathbb{Z}$ of some degree n, so $\mathbb{Z}[\alpha]$ is generated by $1, \alpha, ..., \alpha^{n-1}$. (2) implies (3) implies (4) is immediate.
Suppose (4). Let $a_1, ..., a_n$ generate A over $\mathbb{Z}$. Expressing each αa_i as a linear combination of $a_1, ..., a_n$ with coefficients in $\mathbb{Z}$ we obtain $\alpha a = Ma$, for $a = (a_1, ..., a_n)$, where M is an $n \times n$ matrix over $\mathbb{Z}$. Equivalently, $(\alpha I - M)a = 0$. Since the a_i are not all zero, it follows that $\alpha I - M$ has determinant zero when we multiply on the left of by the adjugate. Expressing this determinant in terms of the n^2 coordinates of $\alpha I - M$ we obtain a monic polynomial in α with coefficients in $\mathbb{Z}$. Thus α is a algebraic integer. □

Corollary 1.1.7 If α, β are algebraic integers, then so are $\alpha + \beta, \alpha\beta$.

Proof We know that $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finitely generated $\mathbb{Z}$-modules. Then so is the ring $\mathbb{Z}[\alpha, \beta]$. Finally, $\mathbb{Z}[\alpha, \beta]$ contains $\alpha + \beta$ and $\alpha\beta$. By the previous theorem this implies that they are algebraic integers. □

Hence the set of algebraic integers in $\mathbb{C}$ is a ring, which we denote by $\mathbb{A}$. In particular $\mathbb{A} \cap K$ is the subring of algebraic integers in K for any number field K.

1.2 The Cyclotomic Fields

Let $\omega = e^{2\pi i/m}$.

Theorem 1.2.1 All ω^k, $1 \leq k \leq m$, $\gcd(k, m) = 1$, are conjugates of ω.

Proof It will be enough to show that for each $\theta = \omega^k$, and for each prime p not dividing m, θ^p is a conjugate of θ. Let f be a monic irreducible polynomial for θ over $\mathbb{Q}$. Then $x^m - 1 = f(x)g(x)$ for some monic $g \in \mathbb{Q}[x]$, and from before we know $f, g \in \mathbb{Z}[x]$. Note θ^p is a root of $x^m - 1$, so θ^p is a root of f or g. Suppose θ^p is a root of g. Then θ is a root of the polynomial $g(x^p)$. It follows that $g(x^p)$ is divisible by $f(x)$ in $\mathbb{Q}[x]$. Applying the lemma again we obtain that $g(x^p)$ is divisible by $f(x)$ in $\mathbb{Z}[x]$. Reducing coefficients $\mod p$, we obtain $g(x^p) + (p)$ is divisible by $f(x) + (p)$. But $g(x^p) + (p) = (g(x))^p + (p)$, and $\mathbb{Z}_p[x]$ is a UFD; it follows that $f + (p)$ and $g + (p)$ have a common factor h in $\mathbb{Z}_p[x]$. Then $h^2 | fg + (p) = x^m - 1 + (p)$. This implies that h divides the derivative of $x^m - 1$, which is $mx^{m-1} + (p)$. Since p does not divide m, $m + (p) \neq 0 + (p)$; then in fact $h(x)$ is just a monomial. But this is impossible since $h | x^m - 1 + (p)$. □

Corollary 1.2.2 $\mathbb{Q}[\omega]$ has degree $\varphi(m)$ over $\mathbb{Q}$.

Proof ω has $\varphi(m)$ conjugates, hence the irreducible polynomial for ω over $\mathbb{Q}$ has degree $\varphi(m)$. □

Corollary 1.2.3 The Galois group of $\mathbb{Q}[\omega]$ over $\mathbb{Q}$ is isomorphic to the multiplicative group of integers $\mod m$

$$\mathbb{Z}_m^* = \{k : 1 \leq k \leq m, \gcd(k, m) = 1\}$$

For each $k \in \mathbb{Z}_m^*$, the corresponding automorphism in the Galois group sends ω to ω^k.

Proof An automorphism of $\mathbb{Q}[\omega]$ is uniquely determined by the image of ω, and by our previous results ω can be sent to any of the ω^k, $\gcd(k, m) = 1$. This establishes the one-to-one correspondence between the Galois group and the multiplicative group $\mod m$. □

Corollary 1.2.4 Let $\omega = e^{2\pi i/m}$. If m is even, the only roots of 1 in $\mathbb{Q}[\omega]$ are the m^{th} roots of 1. If m is odd, the only ones are the $2m^{th}$ roots of 1.

Proof It is enough to prove the statement for even m. Suppose θ is a primitive kth root of unity in $\mathbb{Q}[\omega]$. Then $\mathbb{Q}[\omega]$ contains a primitive rth root of unity, where r is the least common multiple of k and m. But then $\mathbb{Q}[\omega]$ contains the rth cyclotomic field, implying $\varphi(r) \leq \varphi(m)$. This is a contradiction unless $r = m$. Hence $k|m$ and θ is an mth root of unity. □

Corollary 1.2.5 The mth cyclotomic fields, for m even, are all distinct and in fact pairwise non-isomorphic.

1.3 Embeddings in $\mathbb{C}$

Let K be a number field of degree n over $\mathbb{Q}$. Since this is a separable extension there are exactly n embeddings of K into $\mathbb{C}$.

Example:

The quadratic field $\mathbb{Q}[\sqrt{m}]$, m squarefree, has two embeddings in $\mathbb{C}$: the identity mapping, and also the one which sends $a + b\sqrt{m} \mapsto a - b\sqrt{m}$.

Example:

The mth cyclotomic field has $\varphi(m)$ embeddings in $\mathbb{C}$, the $\varphi(m)$ automorphisms.

If K, L are two number fields with $K \subset L$, then we know that every embedding of K in $\mathbb{C}$ extends to exactly $[L : K]$ embeddings of L in $\mathbb{C}$. In particular, L has $[L : K]$ embeddings in $\mathbb{C}$ which leave each point of K fixed. To replace embeddings of a number field K with automorphisms is to extend K to a normal extension L of $\mathbb{Q}$; each embedding of K extends to $[L : K]$ embeddings of L, all of which are automorphisms of L since L is normal.

1.4 The Trace and the Norm

Let K be a number field throughout. We define two functions $T := T_{K/\mathbb{Q}}$ and $N := N_{K/\mathbb{Q}}$ (the **trace** and the **norm**) on K, as follows: Let $\sigma_1, ..., \sigma_n$ denote the embeddings of K in $\mathbb{C}$, where $n = [K : \mathbb{Q}]$. For each $\alpha \in K$, set

$$T(\alpha) = \sum_i \sigma_i(\alpha), \; N(\alpha) = \prod_i \sigma_i(\alpha)$$

From the definition we obtain $T(\alpha+\beta) = T(\alpha) + T(\beta)$ and $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in K$. Moreover, for $r \in \mathbb{Q}$ we have $T(r) = nr, N(r) = r^n$. Also for $r \in \mathbb{Q}$ and $\alpha \in K$, $T(r\alpha) = rT(\alpha)$ and $N(r\alpha) = r^n N(\alpha)$.

Let α have degree d over $\mathbb{Q}$. Let $t(\alpha)$ and $n(\alpha)$ denote the sum and product, respectively, of the d conjugates of α over $\mathbb{Q}$. Then we have

Theorem 1.4.1 $T(\alpha) = \frac{n}{d} t(\alpha)$ and $N(\alpha) = (n(\alpha))^{n/d}$ where $n = [K : \mathbb{Q}]$. Note $n/d = [K : \mathbb{Q}(\alpha)]$.

Proof $t(\alpha)$ and $n(\alpha)$ are the trace and norm $T_{\mathbb{Q}[\alpha]/\mathbb{Q}}$ and $N_{\mathbb{Q}[\alpha]/\mathbb{Q}}$ of α. Each embedding of $\mathbb{Q}[\alpha]$ in $\mathbb{C}$ extends to exactly n/d embeddings of K in $\mathbb{C}$. This establishes the formulas. □

Corollary 1.4.2 $T(\alpha)$ and $N(\alpha)$ are rational.

If α is an algebraic integer, then its monic irreducible polynomial over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$; hence we obtain

Corollary 1.4.3 If α is an algebraic integer, then $T(\alpha)$ and $N(\alpha)$ are integers.

Example:

For the quadratic field $K = \mathbb{Q}[\sqrt{m}]$, we have

$$T(a + b\sqrt{m}) = 2a$$

and

$$N(a + b\sqrt{m}) = a^2 - mb^2$$

for $a, b \in \mathbb{Q}$.

Problems

1.1 A given problem or Excercise is described here. The problem is described here. The problem is described here.