Properties of the Number Fields $\mathbb{Q}(\sqrt{-7})$ and $\mathbb{Q}(\zeta_n)$

Alex Klee, Mason Hill, Joshua Cidron

Introduction

We study two classical number fields: the imaginary quadratic field $\mathbb{Q}(\sqrt{-7})$ and the cyclotomic field $\mathbb{Q}(\zeta_n)$, where ζ_n denotes a primitive nth root of unity. The field $\mathbb{Q}(\sqrt{-7})$ is a quadratic extension of $\mathbb{Q}$ whose elements take the form $a + b\sqrt{-7}$, with $a, b \in \mathbb{Q}$. The cyclotomic field $\mathbb{Q}(\zeta_n)$ is generated by adjoining ζ_n to $\mathbb{Q}$ and contains all $\mathbb{Q}$-linear combinations of powers of ζ_n.

1 Vector Space Basis over $\mathbb{Q}$

The field $\mathbb{Q}(\sqrt{-7})$ admits the natural $\mathbb{Q}$-basis $\{1, \sqrt{-7}\}$, since each element can be uniquely expressed as $a + b\sqrt{-7}$.

In the case of $\mathbb{Q}(\zeta_n)$, where ζ_n is a primitive nth root of unity, the degree of the extension over $\mathbb{Q}$ is $\phi(n)$, Euler's totient function. Therefore, a basis is given by

$$\{1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{\phi(n)-1}\}.$$

2 Integrality over $\mathbb{Z}$

An element $x \in \mathbb{Q}(\sqrt{-7})$ is integral over $\mathbb{Z}$ if it satisfies a monic polynomial with coefficients in $\mathbb{Z}$. Since $\mathbb{Q}(\sqrt{-7})$ is a finite extension of $\mathbb{Q}$, all elements are algebraic, but only some are integral.

Similarly, all elements of $\mathbb{Q}(\zeta_n)$ are algebraic, and those that satisfy monic polynomials with integer coefficients are integral. In particular, ζ_n is a root of the nth cyclotomic polynomial:

$$\Phi_n(x) = \prod_{\substack{1 \le k < n \\ \gcd(k,n)=1}} \left(x - \zeta_n^k\right),$$

which is irreducible and monic with integer coefficients, so ζ_n is integral. Hence, all elements of $\mathbb{Z}[\zeta_n]$ are integral.

3 The Ring of Integers $\mathcal{O}_K$

Let $K = \mathbb{Q}(\sqrt{d})$, where d is a squarefree integer. Then:

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \not\equiv 1 \pmod 4, \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

For $K = \mathbb{Q}(\sqrt{-7})$, since $-7 \equiv 1 \pmod 4$, we have

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right].$$

For $K = \mathbb{Q}(\zeta_n)$, it follows from the properties of cyclotomic polynomials that $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$.

4 Integral Bases and Generators

The ring of integers of $\mathbb{Q}(\sqrt{-7})$ has the integral basis:

$$\left\{1, \frac{1+\sqrt{-7}}{2}\right\},$$

so any element of $\mathcal{O}_{\mathbb{Q}(\sqrt{-7})}$ can be written as $a + b\frac{1+\sqrt{-7}}{2}$ for $a, b \in \mathbb{Z}$.

For $\mathbb{Q}(\zeta_n)$, a $\mathbb{Z}$-basis of $\mathcal{O}_K$ is given by:

$$\{1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{\phi(n)-1}\}.$$

5 Trace and Norm

Let K be a number field and $a \in K$. The *trace* of a is the sum of its Galois conjugates (embeddings into $\mathbb{C}$), and the *norm* is their product.

Case 1: $K = \mathbb{Q}(\sqrt{-7})$

For $a = \alpha + \beta\sqrt{-7}$, the embeddings are a and its conjugate $\alpha - \beta\sqrt{-7}$. Thus,

$$\mathrm{Tr}(a) = 2\alpha, \quad \mathrm{N}(a) = \alpha^2 + 7\beta^2.$$

Case 2: $K = \mathbb{Q}(\zeta_n)$

Let $a = \sum_{i=0}^{\phi(n)-1} \alpha_i \zeta_n^i$. Then,

$$\mathrm{Tr}(a) = \sum_{k\in(\mathbb{Z}/n\mathbb{Z})^*} \sum_{i=0}^{\phi(n)-1} \alpha_i \zeta_n^{ik}, \quad \mathrm{N}(a) = \prod_{k\in(\mathbb{Z}/n\mathbb{Z})^*} \sum_{i=0}^{\phi(n)-1} \alpha_i \zeta_n^{ik}.$$

6 Prime Splitting in $\mathcal{O}_K$

Let p be an odd prime.

In $\mathbb{Q}(\sqrt{-7})$

The discriminant of $\mathbb{Q}(\sqrt{-7})$ is -7. The prime p behaves as follows:

- **Ramified** if $p \mid 7$
- **Split** if $\left(\frac{-7}{p}\right) = 1$
- **Inert** if $\left(\frac{-7}{p}\right) = -1$

In $\mathbb{Q}(\zeta_n)$

The prime p ramifies in $\mathbb{Q}(\zeta_n)$ if and only if $p \mid n$. If $p \nmid n$, then the number of prime ideals above p in $\mathcal{O}_{\mathbb{Q}(\zeta_n)}$ is:

$$\frac{\phi(n)}{f_p},$$

where f_p is the multiplicative order of p modulo n.

7 Unique Factorization

The ring $\mathcal{O}_{\mathbb{Q}(\sqrt{-7})}$ is a principal ideal domain (PID) by the Stark–Heegner theorem, since -7 is one of the nine discriminants for which the ring of integers of $\mathbb{Q}(\sqrt{d})$ is a PID:

$$d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

Hence, $\mathcal{O}_{\mathbb{Q}(\sqrt{-7})}$ is also a unique factorization domain (UFD).

However, $\mathbb{Z}[\sqrt{-7}] \subsetneq \mathcal{O}_K$ is not integrally closed and thus not a UFD. For example:

$$8 = 2^3 = (1 + \sqrt{-7})(1 - \sqrt{-7}).$$

For cyclotomic fields $\mathbb{Q}(\zeta_n)$, the structure of O_K depends on the class number. If the class number is one, then O_K is a UFD. The full list of such n is unknown, but known cases include:

$$n = 1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, \ldots$$

References

[1] Marcus, D. A. *Number Fields*. Springer, 2018.

[2] Lang, S. *Algebraic Number Theory*. Springer, 2014.

[3] Erickson, C. *Cyclotomic Fields III*. University of Pittsburgh.

[4] Bruck, C. *A Concrete Example of Prime Behavior in Quadratic Fields*. Union College.

[5] Jakhar, A., Khanduja, S. K., & Sangwan, N. (2005). *On Integral Basis of Pure Number Fields*.