Algebraic number theory **LTCC 2008**

Lecture notes, Part 1

1. Introduction

We write

$$\mathbb{N} = \{1, 2, 3, \dots\}$$

for the set of natural numbers and

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$$

for the set of integers. Then $\mathbb{Z}$ is a commutative ring. We recall the definition.

Definition 1.1. A *commutative ring* R is a set R with two binary operations $+$ and $\cdot$ such that

- $(R, +)$ is an abelian group (the additive identity will be denoted by 0 and the additive inverse of $\alpha \in R$ by $-\alpha$)
- $\cdot$ is associative and commutative, and there is a multiplicative identity (denoted by 1)
- the distributivity law $\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$ holds.

In this course by a ring we will always mean a commutative ring. We will usually omit $\cdot$ and parentheses when it does not cause any confusion. The ring $\mathbb{Z}$ is contained in the field of rational numbers

$$\mathbb{Q} = \{\alpha/\beta : \alpha, \beta \in \mathbb{Z}, \beta \neq 0\}.$$

(Recall that a ring R is called a *field* if $|R| \geq 2$ and every $\alpha \in R \setminus \{0\}$ has a multiplicative inverse, i.e. there exists $\alpha^{-1} \in R$ such that $\alpha\alpha^{-1} = 1$.)

In algebraic number theory one considers certain field extensions K of $\mathbb{Q}$ and defines a ring $R_K \subset K$ which is a generalisation of the ring $\mathbb{Z} \subset \mathbb{Q}$.

$$\begin{array}{ccc} R_K & \subset & K \\ | & & | \\ \mathbb{Z} & \subset & \mathbb{Q} \end{array}$$

2. Algebraic extensions

A *field extension* K of $\mathbb{Q}$ (often denoted by $K/\mathbb{Q}$) is a field K which contains $\mathbb{Q}$. For example the field of complex numbers $\mathbb{C}$ is a field extension of $\mathbb{Q}$. In this course one can usually assume that field extensions K of $\mathbb{Q}$ are contained in $\mathbb{C}$ (for the fields we are interested in this is not a serious restriction). If K is a field extension of $\mathbb{Q}$ then in particular we can consider K as a vector space over $\mathbb{Q}$. The *degree* of the extension $K/\mathbb{Q}$ (denoted by $[K : \mathbb{Q}]$) is defined to be the dimension of the $\mathbb{Q}$-vector space K.

Definition 2.1. Let $K/\mathbb{Q}$ be a field extension. An element $\alpha \in K$ is called *algebraic* over $\mathbb{Q}$ if α satisfies a polynomial equation

$$X^n + c_{n-1}X^{n-1} + \dots + c_1X + c_0 = 0$$

where $c_0, c_1, \dots, c_{n-1} \in \mathbb{Q}$.

Definition 2.2. A field extension $K/\mathbb{Q}$ is called *algebraic* if every element $\alpha \in K$ is algebraic over $\mathbb{Q}$.

Theorem 2.3. *Let $K/\mathbb{Q}$ be a field extension and $\alpha, \beta \in K$. If α and β are algebraic over $\mathbb{Q}$ then so are $\alpha + \beta$ and $\alpha\beta$. If $\alpha \neq 0$ is algebraic over $\mathbb{Q}$ then so is α^{-1}. Hence the set of elements of K that are algebraic over $\mathbb{Q}$ form a field.*

Proof. This follows immediately from [2, V, Prop. 1.6]. Alternatively, to show that $\alpha + \beta$ and $\alpha\beta$ are algebraic over $\mathbb{Q}$ one can use the proof of Theorem 3.2 in the next section with $\mathbb{Z}$ replaced by $\mathbb{Q}$, and it is an easy exercise to show that α^{-1} is algebraic over $\mathbb{Q}$. We omit the details. $\square$

Definition 2.4. An *algebraic number field* is a field K which is finite over $\mathbb{Q}$, i.e. a field extension K of $\mathbb{Q}$ such that $[K : \mathbb{Q}] < \infty$.

Lemma 2.5. *Let K be an algebraic number field. Then the field extension $K/\mathbb{Q}$ is algebraic.*

Proof. Let $\alpha \in K$. Since K is a finite dimensional $\mathbb{Q}$-vector space there exists an $n \in \mathbb{N}$ such that $1, \alpha, \alpha^2, \ldots, \alpha^n$ are linearly dependent. Choose the minimal such n. Then there exist $c_0, c_1, c_2, \ldots, c_n \in \mathbb{Q}$ with $c_n \neq 0$ such that $c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_n\alpha^n = 0$. Hence α is a root of the polynomial $X^n + c_{n-1}/c_n X^{n-1} + \cdots + c_1/c_n X + c_0/c_n \in \mathbb{Q}[X]$ and therefore algebraic over $\mathbb{Q}$. $\square$

For $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ we let $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ denote the smallest field extension of $\mathbb{Q}$ which contains $\alpha_1, \alpha_2, \ldots, \alpha_n$. One can show that if $\alpha_1, \alpha_2, \ldots, \alpha_n$ are algebraic over $\mathbb{Q}$ then the field $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is algebraic over $\mathbb{Q}$.

An important class of examples is given by quadratic fields.

Definition 2.6. An algebraic number field K with $[K : \mathbb{Q}] = 2$ is called a *quadratic field.*

An integer $m \in \mathbb{Z}$ is called *square-free* if m is not divisible by the square of a prime number.

Lemma 2.7. *Let $m \neq 1$ be a square-free integer. Then $\mathbb{Q}(\sqrt{m})$ is a quadratic field and one has $\mathbb{Q}(\sqrt{m}) = \mathbb{Q} + \mathbb{Q}\sqrt{m}$.*

Proof. It is easy to see that $\sqrt{m} \notin \mathbb{Q}$ so that $\mathbb{Q} + \mathbb{Q}\sqrt{m}$ is 2-dimensional as a vector space over $\mathbb{Q}$. Clearly one has $\mathbb{Q} + \mathbb{Q}\sqrt{m} \subseteq \mathbb{Q}(\sqrt{m})$. To show equality it suffices to show that $\mathbb{Q} + \mathbb{Q}\sqrt{m}$ is a field, but this is straightforward to verify. $\square$

Lemma 2.8. *Let K be a quadratic field. Then there exists a unique square-free integer $m \neq 1$ such that $K = \mathbb{Q}(\sqrt{m})$.*

Proof. If $\alpha \in K \setminus \mathbb{Q}$ then clearly $K = \mathbb{Q}(\alpha)$. Furthermore $1, \alpha, \alpha^2$ are linearly dependent over $\mathbb{Q}$, so there exist $c_0, c_1, c_2 \in \mathbb{Q}$ with $c_2 \neq 0$ such that $c_0 + c_1\alpha + c_2\alpha^2 = 0$. Dividing by c_2 gives $\alpha^2 + a\alpha + b = 0$ for some $a, b \in \mathbb{Q}$, hence $(\alpha + a/2)^2 = a^2/4 - b$. Since $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha + a/2)$ we find that $K = \mathbb{Q}(\sqrt{a^2/4 - b})$. Now there exists a non-zero $c \in \mathbb{Q}$ such that $m = c^2(a^2/4 - b)$ is a square-free integer, and as $\mathbb{Q}(\sqrt{a^2/4 - b}) = \mathbb{Q}(c\sqrt{a^2/4 - b})$ it follows that $K = \mathbb{Q}(\sqrt{m})$ as required.

Uniqueness of m is left as an exercise. $\square$

A quadratic field $K = \mathbb{Q}(\sqrt{m})$ is called *real quadratic* if $m > 0$ and *complex quadratic* if $m < 0$.

Lemma 2.9. *Let $m \neq 1$ be a square-free integer and $K = \mathbb{Q}(\sqrt{m}) = \mathbb{Q} + \mathbb{Q}\sqrt{m}$. Then the map $\tau : K \to K$, $\tau(a + b\sqrt{m}) = a - b\sqrt{m}$ (where $a, b \in \mathbb{Q}$) is an automorphism of the field K, i.e. τ is bijective and preserves the operations $+$ and $\cdot$ of K. Furthermore τ fixes $\mathbb{Q}$, i.e. $\tau(\alpha) = \alpha$ if $\alpha \in \mathbb{Q} \subset K$.*

Proof. Bijectivity is obvious, and a simple computation shows that τ preserves $+$ and $\cdot$, e.g. $\tau((a + b\sqrt{m}) \cdot (c + d\sqrt{m})) = \tau((ac + mbd) + (ad + bc)\sqrt{m}) = (ac + mbd) - (ad + bc)\sqrt{m} = (a - b\sqrt{m}) \cdot (c - d\sqrt{m}) = \tau(a + b\sqrt{m}) \cdot \tau(c + d\sqrt{m})$. $\square$

3. Algebraic integers

Definition 3.1. Let $K/\mathbb{Q}$ be a field extension. An element $\alpha \in K$ is called *integral* over $\mathbb{Z}$ (or an *algebraic integer*) if α satisfies a polynomial equation

$$X^n + c_{n-1}X^{n-1} + \cdots + c_1 X + c_0 = 0$$

where $c_0, c_1, \ldots, c_{n-1} \in \mathbb{Z}$.

Theorem 3.2. *Let $K/\mathbb{Q}$ be a field extension and $\alpha, \beta \in K$. If α and β are integral over $\mathbb{Z}$ then so are $\alpha + \beta$ and $\alpha\beta$.*

Proof. Since α is integral over $\mathbb{Z}$ it is a root of $X^d + c_{d-1}X^{d-1} + \cdots + c_1 X + c_0 = 0$ with $c_0, c_1, \ldots, c_{d-1} \in \mathbb{Z}$. Similarly since β is integral over $\mathbb{Z}$ it is a root of a monic polynomial of degree $e \geq 1$ with integer coefficients. Consider the $\mathbb{Z}$-module $M \subset K$ spanned by $\alpha^i\beta^j$ for $0 \leq i \leq d-1$, $0 \leq j \leq e-1$, that is

$$M = \left\{ \sum_{i,j} c_{i,j}\alpha^i\beta^j : c_{i,j} \in \mathbb{Z}, 0 \leq i \leq d-1, 0 \leq j \leq e-1 \right\}.$$

We first show that $(\alpha+\beta)M \subseteq M$. This is equivalent to showing that $(\alpha+\beta)\alpha^i\beta^j = \alpha^{i+1}\beta^j + \alpha^i\beta^{j+1} \in M$ for $0 \leq i \leq d-1$, $0 \leq j \leq e-1$. If $i \neq d-1$ then clearly $\alpha^{i+1}\beta^j \in M$. If $i = d-1$ then $\alpha^{i+1}\beta^j = (-c_{d-1}\alpha^{d-1} - \cdots - c_1\alpha - c_0)\beta^j \in M$. So in all cases $\alpha^{i+1}\beta^j \in M$ and a similar argument shows that $\alpha^i\beta^{j+1} \in M$. Thus $(\alpha+\beta)\alpha^i\beta^j \in M$ as claimed.

We have shown that there exists a finitely generated $\mathbb{Z}$-module $M \subset K$ such that $(\alpha+\beta)M \subseteq M$. Let $m_1, m_2, \ldots, m_n \in M$ be any finite set of generators of M (for example we can take $m_1, m_2, \ldots, m_n$ to be the elements $\alpha^i\beta^j$ for $0 \leq i \leq d-1$, $0 \leq j \leq e-1$). Then for each index k we have $(\alpha+\beta)m_k \in M$, so $(\alpha+\beta)m_k = \sum_{l=1}^n c_{kl}m_l$ for some $c_{kl} \in \mathbb{Z}$. This can also be written as

$$(1) \qquad (\alpha+\beta)\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} c_{11} & \ldots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{n1} & \ldots & c_{nn} \end{pmatrix} \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}.$$

Now M is non-trivial and $m_1, \ldots, m_n$ generate M, therefore we have $(m_1, \ldots, m_n) \neq (0, \ldots, 0)$. Hence (1) implies that $\alpha+\beta$ is an eigenvalue of the matrix $C = \big(c_{kl}\big)_{1 \leq k,l \leq n}$. Therefore $\alpha+\beta$ is a root of the characteristic polynomial $\det(X \cdot \mathbf{1}_n - C)$ where $\mathbf{1}_n$ denotes the $n \times n$ unit matrix. But it is easy to see that $\det(X \cdot \mathbf{1}_n - C)$ is a monic polynomial with integer coefficients and that therefore $\alpha+\beta$ is integral over $\mathbb{Z}$.

The proof that $\alpha\beta$ is integral over $\mathbb{Z}$ is similar using that $\alpha\beta M \subseteq M$. □

If K is an algebraic number field then the set of all elements of K that are integral over $\mathbb{Z}$ is denoted by R_K. (Remark: Often the notation $\mathcal{O}_K$ is used instead of R_K.) By Theorem 3.2 the set R_K is a ring. It is called the *ring of integers* of K.

Lemma 3.3. *A number $\alpha \in \mathbb{Q}$ is integral over $\mathbb{Z}$ if and only if $\alpha \in \mathbb{Z}$, i.e. $R_{\mathbb{Q}} = \mathbb{Z}$.*

Proof. If $\alpha \in \mathbb{Z}$ then α is integral over $\mathbb{Z}$ because it is a root of $X - \alpha = 0$.

Conversely assume that $\alpha \in \mathbb{Q}$ is integral over $\mathbb{Z}$, so α satisfies a polynomial equation

$$(2) \qquad \alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0$$

with $c_0, c_1, \ldots, c_{n-1} \in \mathbb{Z}$. Write $\alpha = r/s$ with $r \in \mathbb{Z}$, $s \in \mathbb{N}$ and $\gcd(r,s) = 1$. Multiplying (2) by s^n gives

$$r^n + c_{n-1}r^{n-1}s + \cdots + c_1 rs^{n-1} + c_0 s^n = 0,$$

hence $s \mid r^n$. If $s \neq 1$ then s has a prime factor p. But $p \mid r^n$ implies $p \mid r$, contradicting $\gcd(r,s) = 1$. Hence $s = 1$ and $\alpha = r \in \mathbb{Z}$ as required. □

Lemma 3.4. *Let K be an algebraic number field and $\alpha \in K$. Then there exists $n \in \mathbb{N}$ such that $n\alpha \in R_K$.*

Proof. Exercise. □

Corollary 3.5. *Let K be an algebraic number field. Then K is the field of fractions of R_K, i.e. $K = \{\alpha/\beta : \alpha, \beta \in R_K, \beta \neq 0\}$.*

Proof. This is immediate from Lemma 3.4. □

Lemma 3.6. *Let $m \neq 1$ be a square-free integer and let $K = \mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{m} : a, b \in \mathbb{Q}\}$. Then*

$$R_K = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{m} & \text{if } m \not\equiv 1 \pmod 4, \\ \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{m}}{2} & \text{if } m \equiv 1 \pmod 4. \end{cases}$$

Proof. We consider the case $m \not\equiv 1 \pmod 4$, the other case is left as exercise.

If $\alpha \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$ then $\alpha = a + b\sqrt{m}$ with $a, b \in \mathbb{Z}$. Then α is a root of the monic polynomial $X^2 - 2aX + (a^2 - mb^2) \in \mathbb{Z}[X]$ and therefore $\alpha \in R_K$.

Conversely assume that $\alpha \in R_K$. Write $\alpha = a + b\sqrt{m}$ with $a, b \in \mathbb{Q}$. We want to show that $a, b \in \mathbb{Z}$. Recall that in Lemma 2.9 we defined an automorphism τ of K by $\tau(a + b\sqrt{m}) = a - b\sqrt{m}$. Now $\alpha \in R_K$ implies that $\tau(\alpha) \in R_K$ because we have an equation $\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0$ with $c_0, c_1, \ldots, c_{n-1} \in \mathbb{Z}$ and applying τ to this equation gives $\tau(\alpha)^n + c_{n-1}\tau(\alpha)^{n-1} + \cdots + c_1\tau(\alpha) + c_0 = 0$. Since R_K is a ring it follows that $2a = \alpha + \tau(\alpha)$ is integral over $\mathbb{Z}$ and lies in $\mathbb{Q}$, hence by Lemma 3.3 we have $2a \in \mathbb{Z}$. Similarly $a^2 - mb^2 = \alpha\tau(\alpha) \in \mathbb{Z}$. We now distinguish the cases $a \in \mathbb{Z}$ and $a \notin \mathbb{Z}$.

If $a \in \mathbb{Z}$ then $mb^2 \in \mathbb{Z}$ which implies $b \in \mathbb{Z}$ because m is square-free, so $\alpha \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$ as required.

If $a \notin \mathbb{Z}$ then $a = c/2$ with $c \in \mathbb{Z}$ odd, so $c^2 \equiv 1 \pmod 4$. From $(c/2)^2 - mb^2 \in \mathbb{Z}$ it follows that $c^2 - m(2b)^2 \in \mathbb{Z}$ and moreover $c^2 - m(2b)^2 \equiv 0 \pmod 4$. Now $m(2b)^2 \in \mathbb{Z}$ implies $2b \in \mathbb{Z}$ because m is square-free, so $(2b)^2 \equiv 0$ or $1 \pmod 4$. Hence the assumption $m \not\equiv 1 \pmod 4$ implies that $c^2 - m(2b)^2 \equiv 1, 2$ or $3 \pmod 4$, contradicting $c^2 - m(2b)^2 \equiv 0 \pmod 4$. Therefore the case $a \notin \mathbb{Z}$ cannot arise. □

Theorem 3.7. *Let K be an algebraic number field. Then the ring R_K has an integral basis, i.e. there exist elements $\beta_1, \beta_2, \ldots, \beta_n \in R_K$ such that every $\alpha \in R_K$ can be written uniquely in the form $\alpha = a_1\beta_1 + a_2\beta_2 + \cdots + a_n\beta_n$ where $a_1, a_2, \ldots, a_n \in \mathbb{Z}$.*

Proof. See for example [1, §II.1, p. 51]. □

4. Ideals

We first recall some definitions from commutative algebra.

Definition 4.1. Let R be a commutative ring.

(1) A subset $A \subseteq R$ is called an *ideal* of R if A is a subgroup with respect to addition (i.e. $0 \in A$ and if $\alpha, \beta \in A$ then $\alpha - \beta \in A$) and if $\alpha \in R$, $\beta \in A$ then $\alpha\beta \in A$.
(2) An ideal $A \subseteq R$ is called *prime* if $A \neq R$ and if whenever $\alpha\beta \in A$ for some $\alpha, \beta \in R$ then $\alpha \in A$ or $\beta \in A$.
(3) An ideal $A \subseteq R$ is called *maximal* if $A \neq R$ and if there is no ideal B which lies strictly between A and R (i.e. $A \subseteq B \subseteq R$ implies $B = A$ or $B = R$).

Definition 4.2. Let R be a commutative ring and let $\alpha_1, \alpha_2, \ldots, \alpha_n \in R$. Then the set

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) := \{\lambda_1\alpha_1 + \lambda_2\alpha_2 + \cdots + \lambda_n\alpha_n : \lambda_1, \lambda_2, \ldots, \lambda_n \in R\}$$

is an ideal of R. It is called the ideal generated by $\alpha_1, \alpha_2, \ldots, \alpha_n$.

An ideal $A \subseteq R$ is called a *principal ideal* if there exists an $\alpha \in R$ such that $A = (\alpha)$.

Definition 4.3. Let R be a commutative ring and let A and B be ideals of R. We define the *product* AB to be the ideal

$$AB = \{\alpha_1\beta_1 + \alpha_2\beta_2 + \cdots + \alpha_n\beta_n : n \in \mathbb{N}, \alpha_1, \alpha_2, \ldots, \alpha_n \in A, \beta_1, \beta_2, \ldots, \beta_n \in B\}.$$

Lemma 4.4. *Let R be a commutative ring.*

(1) *If $A = (\alpha_1, \ldots, \alpha_m)$ and $B = (\beta_1, \ldots, \beta_n)$ then*

$$AB = (\alpha_1\beta_1, \alpha_1\beta_2, \ldots, \alpha_1\beta_n, \alpha_2\beta_1, \ldots, \alpha_m\beta_n).$$

In particular if $A = (\alpha)$ and $B = (\beta)$ are principal then $AB = (\alpha\beta)$ is principal.

(2) *The product of ideals is associative and commutative. The ideal R is the identity for the product of ideals.*

Proof. Exercise. □

Next we describe the ideals, prime ideals and maximal ideals of the ring $\mathbb{Z}$.

Lemma 4.5. (1) *Every ideal A of $\mathbb{Z}$ is principal, more precisely there exists an integer $\alpha \geq 0$ such that $A = (\alpha)$.*

(2) *An ideal $A = (\alpha)$ of $\mathbb{Z}$ (with $\alpha \geq 0$) is a prime ideal if and only if $\alpha = 0$ or α is a prime number.*

(3) *An ideal $A = (\alpha)$ of $\mathbb{Z}$ (with $\alpha \geq 0$) is a maximal ideal if and only if α is a prime number.*

Proof. Exercise. □

Recall that the fundamental theorem of arithmetic states that every positive integer can be expressed as a product of prime numbers, and that this product representation is unique up to the order of the factors. Since every non-zero ideal of $\mathbb{Z}$ is generated by a unique positive integer, one can easily deduce a corresponding statement for ideals of $\mathbb{Z}$: if A is a non-zero ideal of $\mathbb{Z}$ then A can be written as a product of prime ideals of $\mathbb{Z}$, and this product representation is unique up to the order of the factors.

Now let K be an algebraic number field. The ring R_K is a generalisation of the ring $\mathbb{Z}$ and we therefore want to study if R_K has similar properties as $\mathbb{Z}$. In general some of the properties described above fail for R_K: in general not every ideal of R_K is principal (an example for this will be given later), and non-zero elements of R_K can in general not be written uniquely as a product of prime elements. However some properties of $\mathbb{Z}$ also hold for the rings R_K.

Theorem 4.6. *Let K be an algebraic number field and A an ideal of the ring R_K. Then A is a maximal ideal if and only A is a non-zero prime ideal.*

Proof. It is not difficult to show that maximal ideals are prime (this is true for any commutative ring), and since R_K is not a field the maximal ideals are non-zero. For the converse see for example [1, Corollary to Theorem 5, p. 48] which shows that R_K is a Dedekind domain, and one condition of a Dedekind domain is that all its non-zero prime ideals are maximal (compare [1, Definition (II.1.1), p. 36]). □

Theorem 4.7. *Let K be an algebraic number field. Then every non-zero ideal A of R_K can be written as a product $A = P_1 \cdots P_n$ of prime ideals P_i of R_K. Moreover this product representation is unique up to the order of the factors.*

Proof. See for example [1, Theorem 2, p. 37]. □

References

[1] A. Fröhlich, M.J. Taylor, *Algebraic number theory*, CUP, 1991.
[2] S. Lang, *Algebra*, 3rd edition, Springer, 2002.