Chapter 3

Algebraic numbers and algebraic number fields

Literature:
S. Lang, Algebra, 2nd ed. Addison-Wesley, 1984. Chaps. III,V,VII,VIII,IX.
P. Stevenhagen, Dictaat Algebra 2, Algebra 3 (Dutch).

We have collected some facts about algebraic numbers and algebraic number fields that are needed in this course. Many of the results are stated without proof. For proofs and further background, we refer to Lang's book mentioned above, Peter Stevenhagen's Dutch lecture notes on algebra, and any basic text book on algebraic number theory. We do not require any pre-knowledge beyond basic ring theory. In the Appendix (Section 3.4) we have included some general theory on ring extensions for the interested reader.

3.1 Algebraic numbers and algebraic integers

A number $\alpha \in \mathbb{C}$ is called *algebraic* if there is a non-zero polynomial $f \in \mathbb{Q}[X]$ with $f(\alpha) = 0$. Otherwise, α is called *transcendental*. We define the *algebraic closure* of $\mathbb{Q}$ by

$$\overline{\mathbb{Q}} := \{\alpha \in \mathbb{C} : \alpha \text{ algebraic}\}.$$

Lemma 3.1. *(i) $\overline{\mathbb{Q}}$ is a subfield of $\mathbb{C}$, i.e., sums, differences, products and quotients of algebraic numbers are again algebraic;*

(ii) $\overline{\mathbb{Q}}$ *is algebraically closed, i.e., if* $g = X^n + \beta_1 X^{n-1} \cdots + \beta_n \in \overline{\mathbb{Q}}[X]$ *and* $\alpha \in \mathbb{C}$ *is a zero of* g*, then* $\alpha \in \overline{\mathbb{Q}}$*.*
(iii) If $g \in \overline{\mathbb{Q}}[X]$ *is a monic polynomial, then* $g = (X - \alpha_1) \cdots (X - \alpha_n)$ *with* $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$*.*

Proof. This follows from some results in the Appendix (Section 3.4). Proposition 3.24 in Section 3.4 with $A = \mathbb{Q}$, $B = \mathbb{C}$ implies that $\overline{\mathbb{Q}}$ is a ring. To prove that $\overline{\mathbb{Q}}$ is a field we have to show that if α is a non-zero algebraic number then also α^{-1} is algebraic. Indeed, for such α there are $a_0, \ldots, a_d \in \mathbb{Q}$ with such that $a_0\alpha^d + a_1\alpha^{d-1} + \cdots + a_0 = 0$ and $a_0 a_d \neq 0$. But then, $a_0\alpha^{-d} + \cdots + a_d = 0$. This proves part (i). Part (ii) follows at once from Proposition 3.24, while (iii) is a consequence of (ii). □

Let $\alpha \in \overline{\mathbb{Q}}$. Among all polynomials with rational coefficients having α as a root there is a unique one of minimal degree that is monic (indeed, take two monic polynomials in $\mathbb{Q}[X]$ of minimal degree, say d, having α as a root; then their difference has degree $< d$, hence must be 0). This polynomial is called the *minimal polynomial of* α, notation f_α.

Lemma 3.2. *Let* $\alpha \in \overline{\mathbb{Q}}$*. Then* f_α *is irreducible in* $\mathbb{Q}[X]$ *and* f_α *divides all polynomials in* $g \in \mathbb{Q}[X]$ *with* $g(\alpha) = 0$*.*

Proof. The irreducibility of f_α is clear since otherwise α were a zero of a polynomial in $\mathbb{Q}[X]$ of degree strictly smaller than that of f_α. Let $g \in \mathbb{Q}[X]$ have $g(\alpha) = 0$. By division with remainder, we have $g = qf_\alpha + r$ for certain $q, r \in \mathbb{Q}[X]$ with $r = 0$ or $\deg r < \deg f_\alpha$. But $r(\alpha) = 0$, so $r \neq 0$ is impossible. □

Let $\alpha \in \overline{\mathbb{Q}}$. The *degree* of α, notation $\deg \alpha$, is by definition the degree of f_α. We can factorize f_α over $\overline{\mathbb{Q}}$ as

$$(X - \alpha^{(1)}) \cdots (X - \alpha^{(d)}).$$

These $\alpha^{(1)}, \ldots, \alpha^{(d)}$ are called the *conjugates* of α. They are necessarily distinct, for otherwise, f_α and its derivative f'_α would have a root in common, which would then be a root of the greatest common divisor of f_α and f'_α. But this is impossible because since f_α is irreducible, this gcd is 1.

An algebraic number α is called *totally real* if all $\alpha^{(i)}$ are in $\mathbb{R}$, and *totally complex*, if all $\alpha^{(i)}$ are in $\mathbb{C} \setminus \mathbb{R}$. In general, some of the $\alpha^{(i)}$ may be in $\mathbb{R}$ and some not in

$\mathbb{R}$. For instance, $\alpha = \sqrt[3]{2}$ has minimal polynomial $X^3 - 2$, and conjugates $\sqrt[3]{2}$, $\zeta\sqrt[3]{2}$, and $\zeta^2\sqrt[3]{2}$, where ζ is a primitive cube root of unity.

If $\alpha^{(i)}$ is a non-real conjugate of an algebraic number α, then so is its complex conjugate $\overline{\alpha^{(i)}}$. Hence the non-real conjugates of an algebraic number occur in pairs of complex conjugates, and so their number is even.

Suppose $f_\alpha = X^d + b_1X^{d-1} + \cdots + b_{d-1}X + b_d$; then $b_1, \ldots, b_d \in \mathbb{Q}$. Let $a_0 \in \mathbb{Z}_{>0}$ be the least common multiple of the denominators of $b_1, \ldots, b_d$. Put $F_\alpha := a_0 f_\alpha$. Then

$$F_\alpha = a_0X^d + a_1X^{d-1} + \cdots + a_d, \quad \text{with } a_0, \ldots, a_d \in \mathbb{Z},\ \gcd(a_0, \ldots, a_d) = 1.$$

We call F_α the *primitive minimal polynomial* of α (terminology invented by the author; not used in general!). We define the *height* of α by

$$H(\alpha) := \max(|a_0|, \ldots, |a_d|).$$

Examples. 1. Let $\alpha = a/b$ with $a, b \in \mathbb{Z}$, $b > 0$, $\gcd(a, b) = 1$. Then α has primitive minimal polynomial $bX - a$, hence $H(\alpha) = \max(|a|, b)$.

2. Let $\alpha = \frac{1}{5}(1 + 2\sqrt{3})$. Then

$$f_\alpha = (X - \tfrac{1}{5}(1 + 2\sqrt{3}))(X - \tfrac{1}{5}(1 - 2\sqrt{3})) = X^2 - \tfrac{2}{5}X - \tfrac{11}{25},$$
$$F_\alpha = 25X^2 - 10X - 11, \quad H(\alpha) = 25.$$

Exercise 3.1. *Let $\alpha \in \overline{\mathbb{Q}}$ be non-zero and of degree d.*
(i) Prove that $H(\alpha^{-1}) = H(\alpha)$.
(ii) Prove that $(H(\alpha) + 1)^{-1} \leqslant |\alpha| \leqslant H(\alpha) + 1$.

Definition. A number $\alpha \in \mathbb{C}$ is called an *algebraic integer* if there is a *monic* polynomial $f \in \mathbb{Z}[X]$ such that $f(\alpha) = 0$. Elements of $\mathbb{Z}$ are sometimes called *rational integers*. A number $\alpha \in \mathbb{C}$ is called an *algebraic unit* if both α, α^{-1} are algebraic integers.

We define

$$\overline{\mathbb{Z}} := \{\alpha \in \mathbb{C} : \alpha \text{ algebraic integer}\}, \quad \overline{\mathbb{Z}}^* := \{\alpha \in \mathbb{C} : \alpha \text{ algebraic unit}\}.$$

Lemma 3.3. *(i) $\overline{\mathbb{Z}}$ is a ring, i.e., sums, differences and products of algebraic integers are again algebraic integers. Further, $\overline{\mathbb{Z}}^*$ is the multiplicative group of units*

(invertible elements) of $\overline{\mathbb{Z}}$.
(ii) $\overline{\mathbb{Z}}$ *is integrally closed, i.e., if* $g = X^n + \beta_1 X^{n-1} \cdots + \beta_n \in \overline{\mathbb{Z}}[X]$ *and* $\alpha \in \mathbb{C}$ *is a zero of* g*, then* $\alpha \in \overline{\mathbb{Z}}$.

Proof. Apply Proposition 3.24 in Section 3.4 with $A = \mathbb{Z}$, $B = \mathbb{C}$. □

Lemma 3.4. *Let* $\alpha \in \overline{\mathbb{Q}}$.
(i) $\alpha \in \overline{\mathbb{Z}} \iff f_\alpha \in \mathbb{Z}[X]$.
(ii) $\alpha \in \overline{\mathbb{Z}}^* \iff f_\alpha \in \mathbb{Z}[X]$ *and* $f_\alpha(0) = \pm 1$.

Proof. (i) $\Leftarrow$ is clear. To prove $\Rightarrow$, take a monic polynomial $g \in \mathbb{Z}[X]$ with $g(\alpha) = 0$. The polynomial f_α divides g in $\mathbb{Q}[X]$. By factorizing g in $\mathbb{Z}[X]$, we get $g = h_1 h_2$ where $h_1, h_2 \in \mathbb{Z}[X]$ and where h_1 is a constant multiple of f_α. But the leading coefficient of h_1 divides that of g, hence is ± 1, and so $f_\alpha = \pm h_1 \in \mathbb{Z}[X]$.

(ii) $\Leftarrow$ is again clear. To prove $\Rightarrow$, we already know that both $f_\alpha \in \mathbb{Z}[X]$ and $f_{\alpha^{-1}} \in \mathbb{Z}[X]$. Further, $f_{\alpha^{-1}}(0) = f_\alpha(0)^{-1} \in \mathbb{Z}$, hence $f_\alpha(0) = \pm 1$. □

Lemma 3.5. $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$.

Proof. Let $\alpha \in \overline{\mathbb{Z}} \cap \mathbb{Q}$. Then $f_\alpha = X - \alpha \in \mathbb{Z}[X]$, hence $\alpha \in \mathbb{Z}$. □

An important observation in many Diophantine approximation proofs is that if a is a non-zero rational integer (i.e., in $\mathbb{Z}$) then $|a| \geqslant 1$. This cannot be extended to algebraic integers. For instance, $\alpha := \frac{1}{2}(1 - \sqrt{5})$ is a non-zero algebraic integer (being a root of $X^2 - X - 1$) but $|\alpha| < 1$. However, we have the following.

Lemma 3.6. *Let* α *be a non-zero algebraic integer. Then* α *has a conjugate* $\alpha^{(i)}$ *with* $|\alpha^{(i)}| \geqslant 1$.

Exercise 3.2. *Prove this.*

Lemma 3.7. *Let* α *be an algebraic number, and let* $F = a_0 X^d + a_1 X^{d-1} + \cdots + a_d \in \mathbb{Z}[X]$ *be a polynomial with* $F(\alpha) = 0$. *Then* $a_0\alpha$ *is an algebraic integer.*

Proof. We clearly have

$$0 = a_0^{d-1} F(\alpha) = (a_0\alpha)^d + a_1(a_0\alpha)^{d-1} + \cdots + a_0^{d-1} a_d,$$

hence $a_0\alpha$ is a zero of a monic polynomial from $\mathbb{Z}[X]$. □

Definition. Given a non-zero algebraic number α, we define the *denominator* of α to be the smallest positive $a \in \mathbb{Z}$ such that $a\alpha$ is an algebraic integer, notation $\mathrm{den}(\alpha)$.

Exercise 3.3. *(i) Let $G = b_0X^m + b_1X^{m-1} + \cdots + b_m$ where $b_0, \ldots, b_m$ are algebraic integers with $b_0 \neq 0$. Let $\alpha \in \mathbb{C}$ with $G(\alpha) = 0$. Prove that $G/(X - \alpha)$ is a polynomial whose coefficients are algebraic integers.*
Hint. *Induction on m. In the induction step, use that $b_0\alpha$ is an algebraic integer, after having showed this. Use Lemma 3.3.*

(ii) We can express the primitive minimal polynomial of an algebraic number α as $F_\alpha = a_0 \prod_{i=1}^{d}(X - \alpha^{(i)})$, where $\alpha^{(1)}, \ldots, \alpha^{(d)}$ are the conjugates of α. Prove that for each subset $\{i_1, \ldots, i_k\}$ of $\{1, \ldots, d\}$, the number $a_0\alpha^{(i_1)} \cdots \alpha^{(i_k)}$ is an algebraic integer.

3.2 Algebraic number fields

We first recall a few generalities from field theory. We call $K \supset k$ a field extension, or K an extension of k, if k is a subfield of K, that is, k is a field with the addition and multiplication coming from K. Note that in this case, K is a k-vector space, since it is closed under addition and under scalar multiplication with elements from k (but of course K has much more structure).

Definition. A field extension $K \supset k$ is called *finite* (or K is a finite extension of k) if K is finite dimensional as a k-vector space. In this case, the *degree* of $K \supset k$, notation $[K : k]$, is defined to be the dimension of K as a k-vector space.

Examples. 1. $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$. So $\mathbb{C} \supset \mathbb{R}$ is finite, and $[\mathbb{C} : \mathbb{R}] = 2$.

2. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. Verify that this is a field, in particular that it is closed under division. Clearly, $\mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$ is finite, and $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Definition. A(n algebraic) number field is a finite extension of $\mathbb{Q}$.

Lemma 3.8. *Let $L \supset K \supset k$ be a tower of field extensions (i.e., K is a subfield of L, and k of K). Then $L \supset k$ is finite if and only if $L \supset K$ and $K \supset k$ are finite, and in this case, $[L : k] = [L : K] \cdot [K : k]$.*

Proof. First assume that $L \supset k$ is finite. Then certainly $K \supset k$ is finite since K is a

k-linear subspace of L. Further, a k-basis of L also generates L as a k-vector space. Hence $L \supset K$ is finite as well. Conversely, suppose that $K \supset k$ is finite and let $\{\alpha_1, \ldots, \alpha_r\}$ a k-basis of K, and suppose that $L \supset K$ is finite and let $\{\beta_1, \ldots, \beta_s\}$ be a K-basis of L. Then $\{\alpha_i\beta_j : i = 1, \ldots, r, j = 1, \ldots, s\}$ is a k-basis of L. This proves our lemma. □

Let $K \supset k$ be a field extension, and $\alpha_1, \ldots, \alpha_r \in K$. Then $k(\alpha_1, \ldots, \alpha_r)$ denotes the smallest subfield of K containing both k and $\alpha_1, \ldots, \alpha_r$. Thus, $k(\alpha_1, \ldots, \alpha_r)$ consists of all entities $f(\alpha_1, \ldots, \alpha_r)/g(\alpha_1, \ldots, \alpha_r)$, where $f, g \in k[X_1, \ldots, X_r]$, and $g(\alpha_1, \ldots, \alpha_r) \neq 0$. An extension of the type $k(\alpha) \supset k$ is called *primitive*.

Let $K \supset k$ be an extension and $\alpha \in K$. We say that α is algebraic over k if there is a non-zero polynomial $g \in k[X]$ with $g(\alpha) = 0$. The necessarily unique, monic polynomial of minimal degree with this property is called the *minimal polynomial of α over k*, notation $f_{\alpha,k}$. The degree of α over k is the degree of $f_{\alpha,k}$. The polynomial $f_{\alpha,k}$ is necessarily irreducible in $k[X]$.

Lemma 3.9. *Suppose α has degree d over k. Then $k(\alpha)$ is a finite extension of k with basis $\{1, \alpha, \ldots, \alpha^{d-1}\}$ over k. Hence $[k(\alpha) : k] = d$.*

Proof. $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is certainly linearly independent over k since any non-trivial k-linear combination of these elements would yield a polynomial expression in α of degree $< d$ which is necessarily non-zero. Let $V := \{g(\alpha) : \ g \in k[X]\}$. This is clearly a k-vector space. Using division with remainder, we can write $g \in k[X]$ as $qf_{\alpha,k} + r$ with $q, r \in k[X]$ and $r = 0$ or $\deg r < d$. Now $g(\alpha) = r(\alpha)$ is a k-linear combination of $1, \alpha, \ldots, \alpha^{d-1}$, so these elements form a k-basis of V. To show that V is a field, it remains to show that it is closed under multiplicative inversion. Let $g(\alpha) \in V$ where $g \in k[X]$ is non-zero and of degree $< d$. Since $f_{\alpha,k}$ is irreducible in $k[X]$ it is coprime with g, implying that there are $a, b \in k[X]$ with $ag + bf_{\alpha,k} = 1$. Hence $a(\alpha)g(\alpha) = 1$. This shows that $V = k(\alpha)$. □

We now specialize to algebraic number fields. Note that by Lemmas 3.8 and 3.9, if $\alpha_1, \ldots, \alpha_r$ are algebraic numbers then $\mathbb{Q}(\alpha_1, \ldots, \alpha_r)$ is an algebraic number field. Conversely, any algebraic number field K can be expressed in this form, for instance by taking a $\mathbb{Q}$-basis of K. The following result, which we state without proof, asserts that a number field can always be generated by a single element.

Theorem 3.10 (Theorem of the primitive element)**.** *Let K be an algebraic number field of degree d. Then there is $\theta \in K$ such that $K = \mathbb{Q}(\theta)$.*

A consequence is that K is a $\mathbb{Q}$-vector space with basis $\{1, \theta, \ldots, \theta^{d-1}\}$.

Example. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.
To verify this, observe first that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Hence $K := \mathbb{Q}(\sqrt{2}, \sqrt{3})$ has degree $[K : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$. For a $\mathbb{Q}$-basis of K one may take $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$. On the other hand, $L := \mathbb{Q}(\sqrt{2} + \sqrt{3})$ is a subfield of K, and it has the four $\mathbb{Q}$-linearly independent elements $1, \sqrt{2}+\sqrt{3}, (\sqrt{2}+\sqrt{3})^2 = 5+2\sqrt{6}, (\sqrt{2}+\sqrt{3})^3 = 11\sqrt{2}+9\sqrt{3}$. Hence $L = K$.

An *embedding* of a number field K in $\mathbb{C}$ is an injective field homomorphism of K into $\mathbb{C}$. An embedding of K in $\mathbb{C}$ necessarily leaves the elements of $\mathbb{Q}$ unchanged. This has the following consequences.

First, let σ be an embedding of K in $\mathbb{C}$, $\alpha_1, \ldots, \alpha_r \in K$, and

$$\beta = f(\alpha_1, \ldots, \alpha_r)/g(\alpha_1, \ldots, \alpha_r) \text{ with } f, g \in \mathbb{Q}[X_1, \ldots, X_r].$$

Then $\sigma(\beta) = f(\sigma(\alpha_1), \ldots, \sigma(\alpha_r))/g(\sigma(\alpha_1), \ldots, \sigma(\alpha_r))$. So if $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_r)$, then σ is uniquely determined by its images on $\alpha_1, \ldots, \alpha_r$.

Second, if $f \in \mathbb{Q}[X]$, and $\alpha \in K$ is a zero of f, then also $\sigma(\alpha)$ is a zero of f. For $f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0$.

Proposition 3.11. *Let K be an algebraic number field of degree d. Then there are precisely d distinct embeddings of K in $\mathbb{C}$.*

These d embeddings can be described explicitly as follows. Suppose that $K = \mathbb{Q}(\theta)$. Let f_θ be the minimal polynomial of θ (over $\mathbb{Q}$) and suppose f_θ has degree d. Then

$$f_\theta = (X - \theta^{(1)}) \cdots (X - \theta^{(d)}) \text{ with } \theta^{(1)}, \ldots, \theta^{(d)} \in \mathbb{C}.$$

As mentioned above, the embeddings of K in $\mathbb{C}$ map θ to the zeros of f_θ, and each embedding is uniquely determined by its image of θ. Hence the d embeddings $\sigma_1, \ldots, \sigma_d$ of K in $\mathbb{C}$ can be given by $\sigma_i(\theta) = \theta^{(i)}$.

An embedding σ of K in $\mathbb{C}$ is called *real* if $\sigma(K) \subset \mathbb{R}$, and *complex* if $\sigma(K) \not\subset \mathbb{R}$. If σ is a complex embedding of K, then so is its composition with complex conjugation, $\overline{\sigma} : x \mapsto \overline{\sigma(x)}$. Thus the complex embeddings of K occur in conjugate

pairs $\sigma, \overline{\sigma}$. Suppose that K has precisely r_1 real embeddings, and r_2 pairs of conjugate complex embeddings. Then $r_1 + 2r_2 = d$. It will often be convenient to order the embeddings $\sigma_1, \ldots, \sigma_d$ in such a way that

- $\sigma_1, \ldots, \sigma_{r_1}$ are the real embeddings;
- $\{\sigma_{r_1+1}, \sigma_{r_1+r_2+1} = \overline{\sigma_{r_1+1}}\}, \ldots, \{\sigma_{r_1+r_2}, \sigma_{r_1+2r_2} = \overline{\sigma_{r_1+r_2}}\}$ are the pairs of conjugate complex embeddings.

Example. Let $K = \mathbb{Q}(\sqrt[4]{2})$. The minimal polynomial of $\sqrt[4]{2}$ is $X^4 - 2$, and the zeros of $X^4 - 2$ are $i^k \sqrt[4]{2}$ $(k = 0, 1, 2, 3)$, where $i^2 = -1$. Thus,

$$K = \left\{ \sum_{j=0}^{3} x_j (\sqrt[4]{2})^j \,:\, x_j \in \mathbb{Q} \right\},$$

the four embeddings of K in $\mathbb{C}$ are given by

$$\sum_{j=0}^{3} x_j (\sqrt[4]{2})^j \mapsto \sum_{j=0}^{3} x_j (i^k \sqrt[4]{2})^j \quad (k = 0, 1, 2, 3),$$

and σ_0, σ_2 are real, σ_1, σ_3 are complex, and $\sigma_3 = \overline{\sigma_1}$. So $r_1 = 2$, $r_2 = 1$.

Let K be an algebraic number field, and L a finite extension of K. Further, let σ, τ be embeddings of respectively K and L in $\mathbb{C}$. Then τ of L is called a *continuation* of σ if $\tau|_K = \sigma$, i.e., $\sigma(x) = \tau(x)$ for $x \in K$. Obviously, each embedding of L in $\mathbb{C}$ is a continuation of some embedding of K in $\mathbb{C}$.

Proposition 3.12. *Each embedding of K in $\mathbb{C}$ can be continued in precisely $[L : K]$ ways to an embedding of L in $\mathbb{C}$.*

Example. Let $K = \mathbb{Q}(\sqrt[4]{2})$, $L = \mathbb{Q}(\sqrt[12]{2})$. Then $L \supset K$ and $[L : K] = 3$. The four embeddings of K in $\mathbb{C}$ are given by $\sigma_k(\sqrt[4]{2}) = i^k \sqrt[4]{2}$ $(k = 0, 1, 2, 3)$. The twelve embeddings of L in $\mathbb{C}$ are given by $\tau_l(\sqrt[12]{2}) = \zeta_{12}^l \sqrt[12]{2}$ $(l = 0, 1, \ldots, 11)$, where $\zeta_{12}^3 = i$. The continuations of σ_k to L are τ_l with $3l \equiv k \pmod 4$, $0 \leqslant l \leqslant 11$.

Corollary 3.13. *Let K be an algebraic number field of degree d, and let $\sigma_1, \ldots, \sigma_d$ be the embeddings of K in $\mathbb{C}$. Further, let $\alpha \in K$. Then each of the conjugates of α occurs precisely $[K : \mathbb{Q}(\alpha)]$ times in the sequence $\sigma_1(\alpha), \ldots, \sigma_d(\alpha)$.*

Proof. Suppose $\mathbb{Q}(\alpha)$ has degree m. Let $f_\alpha = \prod_{i=1}^{m} (X - \alpha^{(i)})$. Then the m embeddings $\tau_1, \ldots, \tau_m$ of $\mathbb{Q}(\alpha)$ in $\mathbb{C}$ are determined by $\tau_i(\alpha) = \alpha^{(i)}$ for $i = 1, \ldots, m$. Since

each τ_i has precisely d/m continuations to K and each embedding of K in $\mathbb{C}$ is a continuation of some τ_i, each of the numbers $\alpha^{(i)}$ occurs precisely $d/m = [K : \mathbb{Q}(\alpha)]$ times among $\sigma_1(\alpha), \ldots, \sigma_m(\alpha)$. □

Corollary 3.14. *Let $\alpha_1, \ldots, \alpha_r \in \overline{\mathbb{Q}}$ and $F \in \mathbb{Q}[X_1, \ldots, X_r]$. For $i = 1, \ldots, r$, let $\alpha_i^{(j)}$ $(j = 1, \ldots, r_i)$ be the conjugates of α_i. Then all conjugates of $F(\alpha_1, \ldots, \alpha_r)$ are contained in the set*

$$F(\alpha_1^{(j_1)}, \ldots, \alpha_r^{(j_r)}) \quad (j_1 = 1, \ldots, d_1; \ldots; j_r = 1, \ldots, d_r).$$

Proof. Let $K := \mathbb{Q}(\alpha_1, \ldots, \alpha_r)$ and $\beta := F(\alpha_1, \ldots, \alpha_r)$. Every conjugate of β is of the shape $\sigma(\beta)$, where σ is an embedding of K in $\mathbb{C}$. On the other hand, $\sigma(\beta) = F(\sigma(\alpha_1), \ldots, \sigma(\alpha_r))$ and $\sigma(\alpha_i)$ is a conjugate of α_i, for $i = 1, \ldots, r$. □

Let K be an algebraic number field of degree d and $\sigma_1, \ldots, \sigma_d$ the embeddings of K in $\mathbb{C}$. The *characteristic polynomial* of $\alpha \in K$ is defined by

$$\chi_{\alpha,K} := \prod_{i=1}^{d} (X - \sigma_i(\alpha)).$$

In case that $K = \mathbb{Q}(\alpha)$, we have $\chi_{\alpha,K} = f_\alpha$ is the minimal polynomial of α. In case that $\mathbb{Q}(\alpha)$ is strictly smaller than α we have the following.

Lemma 3.15. *Let $\alpha \in K$ and let f_α be the minimal polynomial of α. Then $\chi_{\alpha,K} = f_\alpha^{[K:\mathbb{Q}(\alpha)]}$. Hence $\chi_{\alpha,K} \in \mathbb{Q}[X]$.*

Proof. Let $m := [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Then $f_\alpha = (X - \alpha^{(1)}) \cdots (X - \alpha^{(m)})$ where $\alpha^{(1)}, \ldots, \alpha^{(m)}$ are the conjugates of α. Apply Corollary 3.13. □

Definition. Let K be an algebraic number field. The *ring of integers of K* is given by

$$O_K := \{\alpha \in K : \ \alpha \text{ is integral over } \mathbb{Z}\} = K \cap \overline{\mathbb{Z}}.$$

That is, O_K is the integral closure of $\mathbb{Z}$ in K. The group of units (invertible elements) of O_K is denoted by O_K^*. We observe that if $\alpha \in O_K$ and σ is an embedding of K in $\mathbb{C}$, then $\sigma(\alpha)$ is an algebraic integer. For α is a zero of a monic $f \in \mathbb{Z}[X]$ hence so is $\sigma(\alpha)$.

Lemma 3.16. *Let $\alpha \in K$. Then $\alpha \in O_K \iff \chi_{\alpha,K} \in \mathbb{Z}[X]$.*

Proof. $\Longleftarrow$ $\chi_{\alpha,K}$ is a monic polynomial having α as a root.

$\Longrightarrow$ Lemma 3.4 implies $f_\alpha \in \mathbb{Z}[X]$, and then Lemma 3.15 implies $\chi_{\alpha,K} \in \mathbb{Z}[X]$. □

Definition. Let K be an algebraic number field of degree d and $\sigma_1, \ldots, \sigma_d$ the embeddings of K in $\mathbb{C}$. Then the *trace* and *norm* of $\alpha \in K$ over $\mathbb{Q}$ are given by respectively

$$Tr_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^{d} \sigma_i(\alpha), \quad N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{d} \sigma_i(\alpha).$$

These numbers are coefficients of $\chi_{\alpha,K}$. So by Lemma 3.15 these numbers belong to $\mathbb{Q}$; moreover, if $\alpha \in O_K$ then by Lemma 3.16 they belong to $\mathbb{Z}$. Notice that for $\alpha, \beta \in K$ we have

$$Tr_{K/\mathbb{Q}}(\alpha+\beta) = Tr_{K/\mathbb{Q}}(\alpha) + Tr_{K/\mathbb{Q}}(\beta), \quad N_{K/\mathbb{Q}}(\alpha\beta) = N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\beta).$$

Lemma 3.17. *Let $\alpha \in O_K$. Then $\alpha \in O_K^* \Longleftrightarrow N_{K/\mathbb{Q}}(\alpha) = \pm 1$.*

Proof. $\Longrightarrow$ Both α, α^{-1} are in O_K, hence $N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$, $N_{K/\mathbb{Q}}(\alpha^{-1}) \in \mathbb{Z}$. But $N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\alpha^{-1}) = 1$, hence $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.

$\Longleftarrow$ Without loss of generality, $\sigma_1(\alpha) = \alpha$. Then $\alpha^{-1} = \pm\sigma_2(\alpha)\cdots\sigma_d(\alpha)$ is an algebraic integer, hence belongs to O_K. □

Exercise 3.4. *Let K be a quadratic number field, that is an algebraic number field of degree 2.*
(i) Prove that $K = \mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$, where $d \in \mathbb{Z} \setminus \{0, 1\}$ and d is not divisible by the square of an integer $\neq 1$. Also determine the two embeddings of K in $\mathbb{C}$.
(ii) Let $\alpha = a + b\sqrt{d}$ with $a, b \in \mathbb{Q}$. Prove the following:
if $d \equiv 2 \pmod 4$ or $d \equiv 3 \pmod 4$ then $\alpha \in O_K$ if and only if $a, b \in \mathbb{Z}$;
if $d \equiv 1 \pmod 4$ then $\alpha \in O_K$ if and only if $2a, 2b \in \mathbb{Z}$ and $2a \equiv 2b \pmod 2$.
Hint. *Determine the minimal polynomial f_α of α and use that its coefficients are in $\mathbb{Z}$.*

3.3 Galois theory

Let K be an algebraic number field with $K \subset \mathbb{C}$. The field K is called *normal* if $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_r)$ where $\alpha_1, \ldots, \alpha_r$ are such that $(X - \alpha_1) \cdots (X - \alpha_r) \in \mathbb{Q}[X]$.

Let $K \subset \mathbb{C}$ be a normal algebraic number field and $\alpha_1, \ldots, \alpha_r$ as above. Let σ be an embedding of K in $\mathbb{C}$. In general, if $f \in \mathbb{Q}[X]$ and α is a zero of f in K, then $f(\sigma(\alpha)) = 0$. As a consequence, σ permutes $\alpha_1, \ldots, \alpha_r$. Since K consists of rational functions in $\alpha_1, \ldots, \alpha_r$ with coefficients in $\mathbb{Q}$, this implies that σ is an isomorphism mapping K to itself, i.e., an *automorphism* of K.

The automorphisms of K form a group under composition, the *Galois group* of K, notation $\mathrm{Gal}(K/\mathbb{Q})$. We state without proof some properties of the Galois group.

Proposition 3.18. *Let K be a normal algebraic number field, and $\mathrm{Gal}(K/\mathbb{Q})$ its Galois group.*
(i) $\mathrm{Gal}(K/\mathbb{Q})$ is a group of order $[K : \mathbb{Q}]$. We have

$$\{x \in K : \sigma(x) = x \ \forall \sigma \in \mathrm{Gal}(K/\mathbb{Q})\} = \mathbb{Q}.$$

(ii) There is a bijection between the subgroups of $\mathrm{Gal}(K/\mathbb{Q})$ and the subfields of K, given by

$$\begin{array}{rcl} H \leqslant \mathrm{Gal}(K/\mathbb{Q}) & \longrightarrow & K^H := \{x \in K : \sigma(x) = x \, \forall \, \sigma \in H\} \\ \mathrm{Gal}(K/L) := \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) : \sigma|_L = \mathrm{id}\} & \longleftarrow & L \end{array}$$

and the order of H is equal to $[K : K^H]$.

(iii) Let $f \in \mathbb{Q}[X]$ be an irreducible polynomial having at least one root in K. Then all roots of f lie in K, for any two roots α, β of f there is $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(\alpha) = \beta$, and each $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ permutes the roots of f.

Remarks. 1. The bijection in (ii) reverses inclusions: if H_1 is a subgroup of H_2, then K^{H_2} is a subfield of K^{H_1}.

2. Every algebraic number field K can be extended to a normal number field. Let $K = \mathbb{Q}(\theta)$. Then for the minimal polynomial f_θ of θ we have $f_\theta = (X - \theta^{(1)}) \cdots (X - \theta^{(d)})$. Clearly, $N := \mathbb{Q}(\theta^{(1)}, \ldots, \theta^{(d)})$ is normal, and N contains K.

Example. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then $K = \mathbb{Q}(\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3})$ is generated by the four roots of $(X^2 - 2)(X^2 - 3)$ hence it is normal. We have seen before that

$[K:\mathbb{Q}]=4$, and that K has basis $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ over $\mathbb{Q}$. Hence $G:=\mathrm{Gal}(K/\mathbb{Q})$ has order 4. Any $\sigma\in\mathrm{Gal}(K/\mathbb{Q})$ maps $\sqrt{2}$ to a root of X^2-2, hence to $\pm\sqrt{2}$. Likewise, σ maps $\sqrt{3}$ to $\pm\sqrt{3}$. Thus, $G=\{\sigma_{ab}:\ a,b=1,-1\}$, where $\sigma_{ab}(\sqrt{2})=a\sqrt{2}$, $\sigma_{ab}(\sqrt{3})=b\sqrt{3}$. It is easy to check that G is the Klein four group, with σ_{11} the identity. The table below gives the subgroups of G and corresponding subfields of K.

H	$K^H=\{x\in K:\ \sigma(x)=x\ \forall\sigma\in H\}$
$\{\mathrm{id}\}$	$\mathbb{Q}(\sqrt{2},\sqrt{3})$
$\{\mathrm{id},\sigma_{1,-1}\}$	$\mathbb{Q}(\sqrt{2})$
$\{\mathrm{id},\sigma_{-1,1}\}$	$\mathbb{Q}(\sqrt{3})$
$\{\mathrm{id},\sigma_{-1,-1}\}$	$\mathbb{Q}(\sqrt{6})$
G	$\mathbb{Q}$

As an example, we compute the subfield K^H corresponding to the subgroup $H=\{\mathrm{id},\sigma_{-1,-1}\}$ of G. Recall that $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ is a basis of K. Thus, every element of K can be expressed uniquely as $x_0+x_1\sqrt{2}+x_2\sqrt{3}+x_3\sqrt{6}$ with $x_i\in\mathbb{Q}$. Now $\sigma_{-1,-1}$ maps $\beta=x_0+x_1\sqrt{2}+x_2\sqrt{3}+x_3\sqrt{6}$ to $x_0-x_1\sqrt{2}-x_2\sqrt{3}+x_3\sqrt{6}$, and thus $\sigma_{11}(\beta)=\beta$ if and only if $x_1=x_2=0$. This shows that $K^H=\mathbb{Q}(\sqrt{6})$.

Exercise 3.5. *Let $\sqrt[3]{2}$ be the real cube root of 2, and ζ a primitive cube root of unity.*
(i) Prove that the field $K:=\mathbb{Q}(\sqrt[3]{2},\zeta)$ is normal and that $[K:\mathbb{Q}]=6$.
(ii) Determine the subfields of K.

3.4 Appendix: Ring extensions

A ring A is always supposed to have a (necessarily unique) unit element 1 such that $x\cdot 1=1\cdot x=x$ for all $x\in A$. An element $a\in A$ is called a *unit* of A if there is $b\in A$ with $ba=ab=1$; this necessarily unique element b is denoted by a^{-1}. The units of A form a multiplicative group, the unit group of A, which we denote by A^*. In particular, the unit group of a field K is $K^*=K\setminus\{0\}$.

An *integral domain* is a commutative ring without divisors of 0, i.e., it does not contain non-zero elements a, b such that $ab=0$. The quotient field of an integral domain A is denoted by Q_A. The field Q_A consists of all fractions a/b with $a,b\in A$, $b\neq 0$, where two fractions a/b, c/d are identified if $ad=bc$.

Given two rings A, B, when writing $A \subset B$ or $B \supset A$ we always mean that A is a subring of B, i.e., A is a ring with the addition, multiplication and unit element of B. We call $A \subset B$ or $B \supset A$ a ring extension. It is possible to set up a theory for ring extensions similar to that for field extensions. We restrict ourselves to extensions of commutative rings.

A role similar to that of vector spaces in the theory of field extensions is played by *modules* in the theory of ring extensions. In general, if A is a commutative ring, then an A-module is a set M, endowed with an addition $+ : M \times M \to M$ and scalar multiplication $\cdot : A \times M \to M$, which satisfy precisely the same axioms as the addition and scalar multiplication of a vector space, except that the scalars are taken from a ring instead of a field. A $\mathbb{Z}$-module is simply an abelian group.

Let A be a commutative ring, and M an A-module. We call M' an A-submodule of M if it is closed under the addition and scalar multiplication of M. That is, M' is an A-submodule of M if and only if for all $\alpha, \beta \in M'$, $r, s \in A$ we have $r\alpha + s\beta \in M'$.

We say that M is *finitely generated over* A, if there is a finite set of elements $\alpha_1, \ldots, \alpha_r \in M$ such that $M = \{\sum_{i=1}^{r} x_i \alpha_i : x_i \in A\}$. We call $\{\alpha_1, \ldots, \alpha_r\}$ an A-*basis* for M if $\alpha_1, \ldots, \alpha_r$ generate M as an A-module, and if they are A-linearly independent, i.e., there is no $(x_1, \ldots, x_r) \in A^r \setminus \{\mathbf{0}\}$ with $\sum_{i=1}^{r} x_i \alpha_i = 0$.

One notable difference between vector spaces and modules is that finitely generated vector spaces always have a basis, whereas finitely generated modules over a ring need not have a basis. An A-module which does have a basis is called *free*.

Example. View the residue class ring $\mathbb{Z}/n\mathbb{Z}$ (with n a positive integer) as a $\mathbb{Z}$-module. Write the residue class $a \bmod n$ as $\overline{a}$. As a $\mathbb{Z}$-module, $\mathbb{Z}/n\mathbb{Z}$ is generated by $\overline{1}$. But for each $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ we have $n \cdot \overline{a} = \overline{0}$, Hence each element of $\mathbb{Z}/n\mathbb{Z}$ is linearly dependent over $\mathbb{Z}$, and so $\mathbb{Z}/n\mathbb{Z}$ does not have a $\mathbb{Z}$-basis.

Now let $A \subset B$ be an extension of commutative rings. We denote the unit element of A by 1. Clearly, B may be viewed as an A-module. We call $A \subset B$ or $B \supset A$ a *finite ring extension* and say that B is *finite over* A, if B is finitely generated as an A-module.

Given $\alpha_1, \ldots, \alpha_r \in B$, we denote by $A[\alpha_1, \ldots, \alpha_r]$ the smallest subring of B

containing A and $\alpha_1, \ldots, \alpha_r$. Thus,

$$A[\alpha_1, \ldots, \alpha_r] = \{f(\alpha_1, \ldots, \alpha_r) : f \in A[X_1, \ldots, X_r]\}.$$

An element $\alpha \in B$ is said to be *integral* over A if there is a *monic* polynomial $f \in A[X]$ with $f(\alpha) = 0$.

Before proceeding, we recall a version of the division with remainder algorithm for rings.

Lemma 3.19. *Let A be a commutative ring, and $f, g \in A[X]$ polynomials such that the leading coefficient of f is in A^*. Then there are polynomials $q, r \in A[X]$ such that $g = qf + r$, $\deg q \leqslant \deg g - \deg f$ and $\deg r < \deg f$. The polynomials q, r are uniquely determined by f, g.*

Proof. Induction on the degree of g. First assume that $\deg g < \deg f$. If $g = qf + r$ for some $q, r \in A[X]$ with $q \neq 0$ and $\deg r < \deg f$, then since the leading coefficient of f is in A^*, we have $\deg qf \geqslant \deg f$, while on the other hand $\deg qf = \deg(g - r) < \deg f$, which is impossible. Hence $q = 0$, $r = g$.

Suppose that $\deg g = m$ and $\deg f = n$ with $m \geqslant n$. let a, b be the leading coefficients of f, g, respectively. So $a \in A^*$. Then apply the induction hypothesis to $g - ba^{-1}X^{m-n}f$, which is in $A[X]$ and has degree smaller than m. □

Lemma 3.20. *Let $A \subset B$ be an extension of commutative rings, and $\alpha \in B$. Then the following are equivalent:*
(i) α is integral over A;
(ii) $A[\alpha]$ is finite over A;
(iii) there is a non-zero, finitely generated A-submodule M of B such that $1 \in M$ and $\alpha M \subseteq M$, where $\alpha M = \{\alpha x : x \in M\}$.

Proof. (i)$\Longrightarrow$(ii). Let $f \in A[X]$ be a monic polynomial with $f(\alpha) = 0$. Let $\beta \in A[\alpha]$. Then $\beta = g(\alpha)$ with $g \in A[X]$. Since f is monic, using division with remainder we find $q, r \in A[X]$ with $g = qf + r$, and $\deg r < \deg f = n$. We may write $r = c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$ with $c_i \in A$. Thus,

$$\beta = g(\alpha) = q(\alpha)f(\alpha) + r(\alpha) = r(\alpha) = \sum_{i=0}^{n-1} c_i\alpha^i.$$

It follows that $A[\alpha]$ is generated as an A-module by $1, \alpha, \ldots, \alpha^{n-1}$.

(ii)$\Longrightarrow$(iii). Trivial.

(iii)$\Longrightarrow$(i). let $\{\omega_1, \ldots, \omega_r\}$ be a set of A-module generators for M. Since $1 \in M$ we may assume that $\omega_1 = 1$. Further, since $\alpha\omega_i \in M$ we have

$$\alpha\omega_i = c_{i1}\omega_1 + \cdots + c_{ir}\omega_r \quad \text{with } c_{ij} \in A \text{ for } i, j = 1, \ldots, r.$$

This can be rewritten as

$$(\alpha I - C) \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_r \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix},$$

where I is the $r \times r$ unit matrix and $C = (c_{ij})_{i,j=1,\ldots,r}$ is the $r \times r$-matrix with c_{ij} on the i-th row and j-th column. We multiply both sides of this identity on the left with the matrix consisting of the minors of $\alpha I - C$, i.e., with $D = (M_{ij})_{i,j=1,\ldots,r}$, where $M_{ij} = (-1)^{i+j}$ times the determinant of the matrix, obtained by removing the j-th row and i-th column from $\alpha I - C$. Then since

$$D \cdot (\alpha I - C) = \det(\alpha I - C) \cdot I,$$

we obtain $\det(\alpha I - C)\omega_i = 0$ for $i = 1, \ldots, r$, so $\det(\alpha I - C) = 0$. That is, α is a zero of $\det(XI - C)$, which is a monic polynomial from $A[X]$. □

Corollary 3.21. *Let $A \subset B$ be a finite extension of commutative rings. Then every $\alpha \in B$ is integral over A.*

Proof. Apply Lemma 3.20, (iii)$\Longrightarrow$(i) with $M = B$. □

Lemma 3.22. *Let A, B, C be commutative rings such that B is finite over A and C is finite over B. Then C is finite over A.*

Proof. Suppose that B is generated as an A-module by $\alpha_1, \ldots, \alpha_m$, and C is generated as a B-module by $\beta_1, \ldots, \beta_n$. A straightforward computation shows that C is generated an as A-module by $\alpha_i\beta_j$ $(i = 1, \ldots, m,\ j = 1, \ldots, n)$. □

Lemma 3.23. *Let A, B be commutative rings. Then B is finite over A if and only if $B = A[\alpha_1, \ldots, \alpha_r]$ for certain $\alpha_1, \ldots, \alpha_r$ that are integral over A.*

Proof. Suppose that B is finite over A, say B is generated as an A-module by $\alpha_1, \ldots, \alpha_r$. By Corollary 3.21, $\alpha_1, \ldots, \alpha_r$ are integral over A, and clearly, $B = A[\alpha_1, \ldots, \alpha_r]$.

Conversely, suppose that $B = A[\alpha_1, \ldots, \alpha_r]$ where $\alpha_1, \ldots, \alpha_r$ are integral over A. Let $B_0 := A$ and $B_i := A[\alpha_1, \ldots, \alpha_i]$ for $i = 1, \ldots, r$. Thus, $B_i = B_{i-1}[\alpha_i]$ for $i = 1, \ldots, r$. By Lemma 3.20, (i)$\Longrightarrow$(ii), B_i is finite over B_{i-1} for $i = 1, \ldots, r$, and then by Lemma 3.22, $B = B_r$ is finite over A. □

Proposition 3.24. *Let $A \subset B$ be an extension of commutative rings.*
(i) Let $\alpha, \beta \in B$ be integral over A. Then $\alpha \pm \beta$ and $\alpha\beta$ are integral over A.
(ii) Let $\beta_1, \ldots, \beta_n \in B$ be integral over A, and let $\alpha \in B$ be a zero of $X^n + \beta_1 X^{n-1} + \cdots + \beta_n$. Then α is integral over A.

Proof. (i). By Lemma 3.23, the ring $A[\alpha, \beta]$ is finite over A, and then by Corollary 3.21, all elements of $A[\alpha, \beta]$ are integral over A.

(ii). Let $C = A[\beta_1, \ldots, \beta_n]$. By Lemma 3.23, C is finite over A. The number α is integral over C, so by Lemma 3.20, $C[\alpha]$ is finite over C. Again by Lemma 3.23, $C[\alpha]$ is finite over A, and then by Corollary 3.21, α is integral over A. □

Definition. Let $A \subset B$ be an extension of commutative rings. By Proposition 3.24 (i), the set

$$C = \{\alpha \in B : \alpha \text{ is integral over } A\}$$

is a subring of B, called the *integral closure* of A in B. Note that by Proposition 3.24,(ii) every element of B that is integral over C already belongs to C.

We say that A is *integrally closed in* B if $C = A$, i.e., every element of B that is integral over A already belongs to A.

Let A be an integral domain. The integral closure of A is defined as its integral closure in its quotient field. If this integral closure is equal to A itself, we call A integrally closed.

Examples. 1. $\mathbb{Z}$ is integrally closed.

2. Let $A = \mathbb{Z}[2\sqrt{2}]$. The quotient field of A is $\mathbb{Q}(\sqrt{2})$, and its integral closure is $\mathbb{Z}[\sqrt{2}]$.