4. Rings of integral elements

Definition: Let R be an integral domain and A an $n \times n$-matrix with entries in R. Let A^{ij} (with $1 \le i,j \le n$) denote the $(n-1)\times(n-1)$-matrix obtained by removing the i^{th} row and j^{th} column from A. Then $A^{\#} := \left((-1)^{i+j} \det A^{ji}\right)_{1 \le i,j \le n}$ is called the (classical) adjoint matrix of A [dt. klassische adjungierte Matrix von A].

Lemma 41 Let R be an integral domain and A an $n \times n$-matrix with entries in R. Then $A \cdot A^{\#} = A^{\#} \cdot A = (\det A) \cdot I_n$.

Proof: Let $B := A \cdot A^{\#} = (b_{ij})_{1 \le i,j \le n}$, i.e.,

$$b_{ij} = \sum_{k=1}^{n} a_{ik} (-1)^{k+j} \det A^{jk} = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{j-1,1} & a_{j-1,2} & \cdots & a_{j-1,n} \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ a_{j+1,1} & a_{j+1,2} & \cdots & a_{j+1,n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = \begin{cases} \det A & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

(The truth of the second equal sign can be seen by expanding the determinant with respect to the j^{th} row.) The equation $A^{\#} \cdot A = (\det A) \cdot I_n$ can be checked analogously.

Remarks: 1) Lemma 41 is still correct if we assume R to be a commutative ring with identity.

2) If R is a field and $\det A \neq 0$ then A is invertible and $A^{-1} = (\det A)^{-1} \cdot A^{\#}$.

Definition: Let S be a commutative ring with identity and R a subring of S with $1_R = 1_S$. An element $\alpha \in S$ is said to be integral over R [dt. ganz über R] if there exists a monic polynomial $p \in R[X]$ such that $p(\alpha) = 0$. I.e., there is an integer $n \ge 1$ and $a_0, a_1, \dots, a_{n-1} \in R$ such that

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

Remark: We are interested in integral elements in the case $R = \mathbb{Z}$ and $S = \mathbb{C}$ or S is an algebraic number field.

Definition: An $\alpha \in \mathbb{C}$ is called an algebraic integer [dt. ganzalgebraisch] if α is integral over $\mathbb{Z}$ (i.e., there is a monic polynomial $p \in \mathbb{Z}[X]$ such that $p(\alpha) = 0$).

Examples: 1) If R and S are fields then $\alpha \in S$ is integral over R if and only if α is algebraic over R.

2) If $d \in \mathbb{Z}$ then $\sqrt{d}$ is an algebraic integer as $p(\sqrt{d}) = 0$ for $p(x) = x^2 - d$.

3) Every n^{th} root of unity ζ is an algebraic integer as $p(\zeta)=0$ for $p(X)=X^n-1$.
(Note that p will normally not be $m_{\mathbb{Q},\zeta}$ as $p(X)=(X-1)(X^{n-1}+X^{n-2}+\cdots+X+1)$ for $n\geq 2$.)

4) $\frac{1+\sqrt{5}}{2}$ is an algebraic integer as $p\left(\frac{1+\sqrt{5}}{2}\right)=0$ for $p(X)=X^2-X-1$.

5) $\frac{-1+i\sqrt{3}}{2}$ is an algebraic integer as $p\left(\frac{-1+i\sqrt{3}}{2}\right)=0$ for $p(X)=X^2+X+1$.

6) $\frac{1}{\sqrt{2}}$ is algebraic over $\mathbb{Q}$ (as it is a root of $X^2-\frac{1}{2}\in\mathbb{Q}[X]$) but it is not an algebraic integer.
(Suppose $\frac{1}{\sqrt{2}}$ is an algebraic integer. Then $\frac{1}{\sqrt{2}^n}+a_{n-1}\frac{1}{\sqrt{2}^{n-1}}+\cdots+a_1\frac{1}{\sqrt{2}}+a_0=0$ for some $n\geq 1$ and certain $a_0,a_1,\dots,a_{n-1}\in\mathbb{Z}$ $\Rightarrow 1+a_{n-1}\sqrt{2}+\cdots+a_1\sqrt{2}^{n-1}+a_0\sqrt{2}^n=0$

$\Rightarrow (1+2a_{n-2}+4a_{n-4}+\cdots)+\sqrt{2}(a_{n-1}+2a_{n-3}+\cdots)=0$

If $a_{n-1}+2a_{n-3}+\cdots\neq 0$ then $\sqrt{2}=-\frac{1+2a_{n-2}+4a_{n-4}+\cdots}{a_{n-1}+2a_{n-3}+\cdots}\in\mathbb{Q}$.

If $a_{n-1}+2a_{n-3}+\cdots=0$ then $0=1+2a_{n-2}+4a_{n-4}+\cdots\equiv 1\pmod 2$.

Both are contradictions.

Theorem 42 Let S be an integral domain, R a subring (with identity) of S and $\alpha\in S$. Then the following are equivalent:

(i) α is integral over R,

(ii) $R[\alpha]$ is a finitely generated R-module,

(iii) There is a subring T (of S), which is a finitely generated R-module, such that $R[\alpha]\subseteq T\subseteq S$.

Proof: (i) $\Rightarrow$ (ii) As α is integral over R there is a monic $p\in R[X]$ such that $p(\alpha)=0$. Let $n:=\deg p$. We claim that $R[\alpha]=\langle 1,\alpha,\dots,\alpha^{n-1}\rangle_R$. Clearly $R[\alpha]$ is an R-module. We know from algebra that $R[\alpha]=\{f(\alpha)\mid f\in R[X]\}$. As p is a monic polynomial its leading coefficient is $1\in R^\times$ and for any $f\in R[X]$ we can use division with remainder to find $q,r\in R[X]$ such that $f(X)=q(X)p(X)+r(X)$ and $\deg r<\deg p=n$. Therefore,

$$f(\alpha)=q(\alpha)\underbrace{p(\alpha)}_{=0}+r(\alpha)\in R+R\alpha+\cdots+R\alpha^{n-1}=\langle 1,\alpha,\dots,\alpha^{n-1}\rangle_R$$

where we used Theorem 37 in the last step.

(ii) $\Rightarrow$ (iii) Set $T:=R[\alpha]$.

9.11.2022

(iii) $\Rightarrow$ (i) There are $\beta_1,\dots,\beta_n\in T$ which generate T as an R-module, i.e., $T=\langle\beta_1,\dots,\beta_n\rangle_R$. As T is a ring and $\alpha\in T$ we know $\alpha\beta_i\in T$ (for $1\leq i\leq n$). Therefore

$\forall i \in \{1,\dots,n\}\ \exists c_{i1},\dots,c_{in} \in R : \alpha\beta_i = \sum_{j=1}^{n} c_{ij}\beta_j$ and thus $\sum_{j=1}^{n} (\alpha\delta_{ij} - c_{ij})\beta_j = 0 \quad (1 \le i \le n) \quad (*)$.

Let A denote the matrix $A := (\alpha\delta_{ij} - c_{ij})_{1 \le i,j \le n}$ (with entries in $R[\alpha]$). We rewrite $(*)$ as

$$A \cdot \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \Rightarrow \det A \cdot \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = \det A \cdot I_n \cdot \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} \overset{\text{Lemma 41}}{=} A^{\#} A \cdot \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = A^{\#} \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

which yields $\det A \cdot \beta_i = 0$ for $1 \le i \le n$. As $\langle \beta_1,\dots,\beta_n \rangle_R = T$ there are $b_1,\dots,b_n \in R$ such that $1 = \sum_{i=1}^{n} b_i\beta_i$ and therefore $\det A = \sum_{i=1}^{n} b_i \underbrace{(\det A \cdot \beta_i)}_{=0} = 0$. This says that

$$\begin{vmatrix} \alpha - c_{11} & -c_{12} & \cdots & -c_{1n} \\ -c_{21} & \alpha - c_{22} & & -c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -c_{n1} & -c_{n2} & \cdots & \alpha - c_{nn} \end{vmatrix} = 0$$ which gives a monic polynomial in $R[x]$ which has α as a root.

Remark: The proof of the implication (iii) $\Rightarrow$ (i) could be simplified. However, the above proof has the advantage of working even if R and S are only commutative rings with identity.

Corollary 43 Let $\alpha \in \mathbb{C}$. Then the following are equivalent:

(i) α is an algebraic integer,

(ii) $\mathbb{Z}[\alpha]$ is a finitely generated abelian group,

(iii) There is a subring T of $\mathbb{C}$ such that $\mathbb{Z}[\alpha] \subseteq T$ and T is a finitely generated abelian group.

Proof: Set $R = \mathbb{Z}$ and $S = \mathbb{C}$ in Theorem 42.

Lemma 44 Let S be a commutative ring with identity and R a subring of S with $1_R = 1_S$. If M is a finitely generated S-module and S is a finitely generated R-module then M is a finitely generated R-module.

Proof: Clearly, M is also an R-module. There are $m_1,\dots,m_n \in M$ and $s_1,\dots,s_k \in S$ such that $M = \langle m_1,\dots,m_n \rangle_S$ and $S = \langle s_1,\dots,s_k \rangle_R$. We claim that

$M = \langle s_1m_1,\dots,s_km_1,\dots,s_1m_n,\dots,s_km_n \rangle_R$. Let $m \in M$. Then there are $c_1,\dots,c_n \in S$ such that $m = \sum_{i=1}^{n} c_im_i$. Furthermore, $\forall i \in \{1,\dots,n\}\ \exists d_{i1},\dots,d_{ik} \in R : c_i = \sum_{j=1}^{k} d_{ij}s_j$

$$\Rightarrow m = \sum_{i=1}^{n} c_im_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{k} d_{ij}s_j \right) m_i = \sum_{i=1}^{n} \sum_{j=1}^{k} d_{ij}(s_jm_i).$$

Corollary 45 Let S be an integral domain, R a subring (with identity) of S and $\alpha_1,\dots,\alpha_n \in S$. Then the following are equivalent:

(i) $\alpha_1,\dots,\alpha_n$ are all integral over R;

(ii) $R[\alpha_1,\dots,\alpha_n]$ is a finitely generated R-module

Proof: (i) $\Rightarrow$ (ii) We use induction on n. The case $n=1$ was proved as implication (i)$\Rightarrow$(iii) in Theorem 42. Now let $n>1$. We know from algebra that $R[\alpha_1,\dots,\alpha_n] = R[\alpha_1,\dots,\alpha_{n-1}][\alpha_n]$. As α_n is integral over R, it is also integral over $R[\alpha_1,\dots,\alpha_{n-1}]$. Theorem 42 implies that $R[\alpha_1,\dots,\alpha_n]$ is a finitely generated $R[\alpha_1,\dots,\alpha_{n-1}]$-module. The induction hypothesis is that $R[\alpha_1,\dots,\alpha_{n-1}]$ is a finitely generated R-module. Lemma 44 implies that $R[\alpha_1,\dots,\alpha_n]$ is a finitely generated R-module.

(ii) $\Rightarrow$ (i) For $1\le i\le n$ we have $R[\alpha_i] \subseteq R[\alpha_1,\dots,\alpha_n] \subseteq S$ and α_i is integral over R by implication (iii)$\Rightarrow$(i) of Theorem 42.

Corollary 46 Let $\alpha_1,\dots,\alpha_n \in \mathbb{C}$. Then the following are equivalent:

(i) $\alpha_1,\dots,\alpha_n$ are algebraic integers,

(ii) $\mathbb{Z}[\alpha_1,\dots,\alpha_n]$ is a finitely generated abelian group.

Proof: Set $R=\mathbb{Z}$ and $S=\mathbb{C}$ in Corollary 45.

Lemma 47 Let S be an integral domain and R a subring (with identity) of S.

(i) If $\alpha_1,\dots,\alpha_n \in S$ are integral over R then each $\beta \in R[\alpha_1,\dots,\alpha_n]$ is integral over R,

(ii) If $\alpha_1,\alpha_2 \in S$ are integral over R then $\alpha_1+\alpha_2$, $\alpha_1-\alpha_2$ and $\alpha_1\alpha_2$ are integral over R.

Proof: (i) We have $R \subseteq R[\beta] \subseteq R[\alpha_1,\dots,\alpha_n] \subseteq S$, where $R[\alpha_1,\dots,\alpha_n]$ is a finitely generated R-module by Corollary 45. Theorem 42 implies that β is integral over R.

(ii) If $\beta \in \{\alpha_1+\alpha_2, \alpha_1-\alpha_2, \alpha_1\alpha_2\}$ then $\beta \in R[\alpha_1,\alpha_2]$ and β is integral over R by (i).

Definition: Let S be an integral domain and R a subring (with identity) of S. Then $\overline{R}^S := \{\alpha \in S \mid \alpha \text{ is integral over } R\}$ is called the integral closure of R in S [dt. der ganze Abschluss von R in S].

Theorem 48 Let S be an integral domain and R a subring (with identity) of S. Then $\overline{R}^S$ is an integral domain.

Proof: Lemma 47 (ii) shows that $\overline{R}^S$ is a subring of S. Therefore $\overline{R}^S$ is a commutative ring with identy and even an integral domain as S is an integral domain.

Definition: 1) Let $\mathcal{O} := \overline{\mathbb{Z}}^{\mathbb{C}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ is an algebraic integer}\}$.

2) If K is an algebraic number field let $\mathcal{O}_K := \overline{\mathbb{Z}}^{K} = \{\alpha \in K \mid \alpha \text{ is an algebraic integer}\}$.

Remark: $\mathcal{O}$ and $\mathcal{O}_K$ are integral domains by Theorem 48.

Definition: Let S be a commutative ring with identity and R a subring of S with $1_R = 1_S$. Then S is said to be integral over R [dt ganz über R] if every $\alpha \in S$ is integral over R.

Theorem 49 Let T be an integral domain, S a subring (with identity) of T and R a subring (with identity) of S (i.e., $R \subseteq S \subseteq T$).

(i) If S is integral over R and $\beta \in T$ is integral over S, then β is integral over R.

(ii) If S is integral over R and T is integral over S, then T is integral over R.

Proof: (i) As β is integral over S there is a polynomial $p(X) = X^n + \alpha_{n-1}X^{n-1} + \cdots + \alpha_1 X + \alpha_0 \in S[X]$ such that $p(\beta) = 0$. As S is integral over R its coefficients $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in S$ are all integral over R. By Corollary 45 $R[\alpha_0, \alpha_1, \ldots, \alpha_{n-1}]$ is a finitely generated R-module. Clearly β is also integral over $R[\alpha_0, \alpha_1, \ldots, \alpha_{n-1}]$ and Theorem 42 implies that $R[\alpha_0, \alpha_1, \ldots, \alpha_{n-1}][\beta]$ is a finitely generated $R[\alpha_0, \alpha_1, \ldots, \alpha_{n-1}]$-module. Lemma 44 implies that $R[\alpha_0, \alpha_1, \ldots, \alpha_{n-1}][\beta]$ is a finitely generated R-module. Because of Corollary 45 β is integral over R.

(ii) Follows from (i).

Corollary 50 Let K be an algebraic number field and $\beta \in K$. If β is integral over $\mathcal{O}_K$, then β is an algebraic integer. (I.e., if there is a polynomial $p(X) = X^n + \alpha_{n-1}X^{n-1} + \cdots + \alpha_1 X + \alpha_0 \in \mathcal{O}_K[X]$ such that $p(\beta) = 0$ then $\beta \in \mathcal{O}_K$.)

Proof: Use Theorem 49 (i) with $R = \mathbb{Z}$, $S = \mathcal{O}_K$ and $T = K$.

Definition: 1) Let S be a commutative ring with identity and R a subring of S with $1_R = 1_S$. Then R is said to be integrally closed in S [dt R ist ganzabgeschlossen in S] if $\overline{R}^S = R$.

2) Let R be an integral domain and K its quotient field. Then R is called integrally closed [dt ganzabgeschlossen] if R is integrally closed in K (i.e., $\overline{R}^K = R$).

Corollary 51 Let S be an integral domain and R a subring (with identity) of S. Then $\overline{R}^S$ is integrally closed in S.

Proof: We have to show $\overline{(\overline{R}^S)}^S = \overline{R}^S$. We first check $\overline{R}^S \subseteq \overline{(\overline{R}^S)}^S$. Let $\alpha \in \overline{R}^S$. Then there is a monic polynomial $p \in R[X]$ such that $p(\alpha) = 0$. As $p \in R[X] \subseteq \overline{R}^S[X]$ we get $\alpha \in \overline{(\overline{R}^S)}^S$.

It remains to check $(\overline{R}^S)^S \subseteq \overline{R}^S$. If $\alpha \in (\overline{R}^S)^S$ then α is integral over $\overline{R}^S$. As $\overline{R}^S$ is integral over R, Theorem 49(i) implies that α is integral over R, i.e., $\alpha \in \overline{R}^S$.

Theorem 52 Let R be a unique factorization domain. Then R is integrally closed.

Proof: Let $\alpha, \beta \in R$, $\beta \neq 0$ and $\frac{\alpha}{\beta}$ integral over R. W.l.o.g. we can assume that α and β are relatively prime. There are $c_1, \dots, c_n \in R$ such that $\left(\frac{\alpha}{\beta}\right)^n + c_1\left(\frac{\alpha}{\beta}\right)^{n-1} + \dots + c_{n-1}\frac{\alpha}{\beta} + c_n = 0$ and therefore $\alpha^n + c_1\alpha^{n-1}\beta + \dots + c_{n-1}\alpha\beta^{n-1} + c_n\beta^n = 0$. If a prime element $\pi \in R$ would have the property $\pi \mid \beta$ then necessarily $\pi \mid \alpha$. As α and β are assumed to be relatively prime such a π does not exist. Therefore $\beta \in R^*$ and $\frac{\alpha}{\beta} = \alpha\beta^{-1} \in R$.

Example: $\mathbb{Z}$ is integrally closed (as it is a unique factorization domain). 14.11.2022

Lemma 53 Let K be an algebraic number field and $\alpha \in K$. Then $\exists m \in \mathbb{Z}\setminus\{0\} : m\alpha \in \mathcal{O}_K$.

Proof: As α is algebraic (over $\mathbb{Q}$) there are $n \geq 1$ and $a_n (\neq 0), a_{n-1}, \dots, a_1, a_0 \in \mathbb{Z}$ such that $a_n\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0$. This implies

$$(a_n\alpha)^n + a_{n-1}(a_n\alpha)^{n-1} + a_{n-2}a_n(a_n\alpha)^{n-2} + \dots + a_1a_n^{n-2}(a_n\alpha) + a_0a_n^{n-1} = 0.$$

This shows $a_n\alpha \in \mathcal{O}_K$, i.e., one can choose $m := a_n$.

Corollary 54 Let K be an algebraic number field. Then there is an $\alpha \in \mathcal{O}_K$ such that $K = \mathbb{Q}(\alpha)$.

Proof: The primitive element theorem (Theorem 15) implies that there is a $\beta \in K$ such that $K = \mathbb{Q}(\beta)$. By Lemma 53 there is an $m \in \mathbb{Z}\setminus\{0\}$ such that $m\beta \in \mathcal{O}_K$. Let $\alpha := m\beta$. Then $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = K$.

Corollary 55 Let K be an algebraic number field. Then the quotient field of $\mathcal{O}_K$ is (isomorphic to) K.

Proof: Let Q denote the quotient field of $\mathcal{O}_K$. Consider the map $\varphi : Q \to K$, $\varphi\left(\frac{\alpha}{\beta}\right) = \alpha\beta^{-1}$. Then φ is a ring homomorphism as

$$\varphi\left(\frac{\alpha}{\beta}\cdot\frac{\gamma}{\delta}\right) = \varphi\left(\frac{\alpha\gamma}{\beta\delta}\right) = \alpha\gamma(\beta\delta)^{-1} = (\alpha\beta^{-1})(\gamma\delta^{-1}) = \varphi\left(\frac{\alpha}{\beta}\right)\varphi\left(\frac{\gamma}{\delta}\right) \quad \text{and}$$

$$\varphi\left(\frac{\alpha}{\beta}+\frac{\gamma}{\delta}\right) = \varphi\left(\frac{\alpha\delta+\beta\gamma}{\beta\delta}\right) = (\alpha\delta+\beta\gamma)(\beta\delta)^{-1} = \alpha\delta\beta^{-1}\delta^{-1} + \beta\gamma\beta^{-1}\delta^{-1} = \alpha\beta^{-1} + \gamma\delta^{-1} = \varphi\left(\frac{\alpha}{\beta}\right) + \varphi\left(\frac{\gamma}{\delta}\right)$$

for all $\alpha, \beta, \gamma, \delta \in \mathcal{O}_K$ with $\beta \neq 0, \delta \neq 0$. Clearly $\varphi\left(\frac{1}{1}\right) = 1$ (i.e., $\varphi(1_Q) = 1_K$) and $\varphi\left(\frac{\alpha}{\beta}\right) = 1 \Rightarrow \alpha\beta^{-1} = 1 \Rightarrow \alpha = \beta (\neq 0) \Rightarrow \frac{\alpha}{\beta} = \frac{1}{1}$ shows that φ injective. If $x \in K$ then there is a $\beta \in \mathbb{Z}\setminus\{0\} \subseteq \mathcal{O}_K\setminus\{0\}$: $\alpha := \beta x \in \mathcal{O}_K$. Therefore $\varphi\left(\frac{\alpha}{\beta}\right) = \alpha\beta^{-1} = x$ which shows that φ is also surjective.

Corollary 56 Let K be an algebraic number field. Then $\mathcal{O}_K$ is integrally closed.

Proof: Because of Corollary 55 it suffices that if $\beta \in K$ is integral over $\mathcal{O}_K$ then β is an algebraic integer. This was already proved in Corollary 50.

Corollary 57 (i) $\mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$,

(ii) If K is an algebraic number field then $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$.

Proof: (i) Clearly $\mathbb{Z} \subseteq \mathcal{O} \cap \mathbb{Q}$. If $\alpha \in \mathcal{O} \cap \mathbb{Q}$ then $\alpha \in \mathbb{Q}$ and there is a monic $p \in \mathbb{Z}[x]$ such that $p(\alpha) = 0$. As $\mathbb{Z}$ is a unique factorization domain it is integrally closed by Theorem 52 and therefore $\alpha \in \mathbb{Z}$.

(ii) $\mathcal{O}_K \cap \mathbb{Q} = (\mathcal{O} \cap K) \cap \mathbb{Q} = K \cap (\mathcal{O} \cap \mathbb{Q}) \overset{(i)}{=} K \cap \mathbb{Z} = \mathbb{Z}$.

Corollary 58 Let $\alpha \in \mathbb{C}$ be algebraic over $\mathbb{Q}$. Then the following are equivalent:

(i) α is an algebraic integer,

(ii) $m_{\mathbb{Q},\alpha} \in \mathbb{Z}[x]$.

Proof: (i) $\Rightarrow$ (ii) There is a monic polynomial $p \in \mathbb{Z}[x]$ such that $p(\alpha) = 0$. This implies $m_{\mathbb{Q},\alpha} \mid p$ (in $\mathbb{Q}[x]$). If $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_d \in \mathbb{C}$ are the different roots of $m_{\mathbb{Q},\alpha}$ then $\alpha_1, \dots, \alpha_d$ are roots of p and therefore $\alpha_1, \dots, \alpha_d$ are algebraic integers. If $m_{\mathbb{Q},\alpha}(x) = x^d + c_{d-1}x^{d-1} + \dots + c_1 x + c_0 \in \mathbb{Q}[x]$ then $m_{\mathbb{Q},\alpha}(x) = \prod_{i=1}^{d} (x - \alpha_i)$ and by Vieta's root theorem $c_0, c_1, \dots, c_{d-1}$ are algebraic integers, i.e., $c_0, c_1, \dots, c_{d-1} \in \mathbb{Q} \cap \mathcal{O} \overset{\text{Cor 57}}{=} \mathbb{Z}$ and therefore $m_{\mathbb{Q},\alpha} \in \mathbb{Z}[x]$.

(ii) $\Rightarrow$ (i) Trivial.

Theorem 59 Let K be an algebraic number field.

(i) If $\alpha \in \mathcal{O}_K$ then $N_{K/\mathbb{Q}}(\alpha), \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$,

(ii) If $\alpha \in \mathcal{O}_K$ then $\alpha \in \mathcal{O}_K^* \iff N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}^* = \{1, -1\}$,

(iii) If $\alpha, \beta \in \mathcal{O}_K$ are associates (i.e., $\exists \varepsilon \in \mathcal{O}_K^* : \beta = \varepsilon\alpha$) then $|N_{K/\mathbb{Q}}(\alpha)| = |N_{K/\mathbb{Q}}(\beta)|$,

(iv) If $\alpha \in \mathcal{O}_K$ and $|N_{K/\mathbb{Q}}(\alpha)|$ is a prime (in $\mathbb{Z}$) then α is irreducible in $\mathcal{O}_K$.

Proof: (i) If $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_d \in \mathbb{C}$ are the different roots of $m_{\mathbb{Q},\alpha}$ then $\alpha_1, \alpha_2, \dots, \alpha_d$ are algebraic integers because of Corollary 58. Corollary 24 implies

$$N_{K/\mathbb{Q}}(\alpha) = \left(\prod_{i=1}^{d} \alpha_i\right)^{[K:\mathbb{Q}(\alpha)]} \in \mathbb{Q} \cap \mathcal{O} = \mathbb{Z} \quad \text{and}$$

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = [K:\mathbb{Q}(\alpha)] \sum_{i=1}^{d} \alpha_i \in \mathbb{Q} \cap \mathcal{O} = \mathbb{Z}.$$

(ii) ($\Rightarrow$) If $\alpha \in \mathcal{O}_K^*$ then $\exists \beta \in \mathcal{O}_K : \alpha\beta = 1$ and therefore

$N_{K/\mathbb{Q}}(\alpha)\cdot N_{K/\mathbb{Q}}(\beta) \overset{\text{Lemma 22}}{=} N_{K/\mathbb{Q}}(\alpha\beta) = N_{K/\mathbb{Q}}(1) = 1$. As $N_{K/\mathbb{Q}}(\alpha), N_{K/\mathbb{Q}}(\beta) \in \mathbb{Z}$ (by (i)) we get $N_{K/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(\beta) \in \mathbb{Z}^* = \{1,-1\}$.

($\Leftarrow$) Let $\sigma_1,\dots,\sigma_n : K \hookrightarrow \mathbb{C}$ denote the different homomorphisms with $\sigma_i|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$ for $1 \le i \le n = [K:\mathbb{Q}]$, where we assume $\sigma_1 = \mathrm{id}_K$. Then

$$\varepsilon := \alpha \prod_{i=2}^{n} \sigma_i(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \overset{\text{Th 23 (ii)}}{=} N_{K/\mathbb{Q}}(\alpha) \in \{1,-1\}.$$ Let $\beta := \varepsilon \prod_{i=2}^{n} \sigma_i(\alpha)$. Then

$\alpha\beta = \varepsilon\alpha \prod_{i=2}^{n} \sigma_i(\alpha) = \varepsilon^2 = 1$, i.e., $\beta = \alpha^{-1} \in K$. As $\alpha \in \mathcal{O}$ clearly $\sigma_i(\alpha) \in \mathcal{O}$ for $2 \le i \le n$.

This implies $\sigma_2(\alpha)\cdots\sigma_n(\alpha) \in \mathcal{O}$ and thus $\beta \in \mathcal{O} \cap K = \mathcal{O}_K$.

(iii) $N_{K/\mathbb{Q}}(\beta) = N_{K/\mathbb{Q}}(\varepsilon\alpha) = \underbrace{N_{K/\mathbb{Q}}(\varepsilon)}_{\in\{1,-1\}} N_{K/\mathbb{Q}}(\alpha) \in \{N_{K/\mathbb{Q}}(\alpha), -N_{K/\mathbb{Q}}(\alpha)\}$ and therefore

$|N_{K/\mathbb{Q}}(\beta)| = |N_{K/\mathbb{Q}}(\alpha)|$.

(iv) Let $p := |N_{K/\mathbb{Q}}(\alpha)|$ and assume $\alpha = \beta\gamma$ for some $\beta,\gamma \in \mathcal{O}_K$. Then

$N_{K/\mathbb{Q}}(\beta)N_{K/\mathbb{Q}}(\gamma) = N_{K/\mathbb{Q}}(\beta\gamma) = N_{K/\mathbb{Q}}(\alpha) \in \{p,-p\}$. As $N_{K/\mathbb{Q}}(\beta), N_{K/\mathbb{Q}}(\gamma) \in \mathbb{Z}$ we see $N_{K/\mathbb{Q}}(\beta) \in \{1,-1\}$ or $N_{K/\mathbb{Q}}(\gamma) \in \{1,-1\}$ and (ii) implies $\beta \in \mathcal{O}_K^*$ or $\gamma \in \mathcal{O}_K^*$.

Remark: The reverses of (iii) and (iv) are not true. (Examples will follow shortly.)

Definition: Let K be an algebraic number field. Then $\{\omega_1,\dots,\omega_n\} \subseteq \mathcal{O}_K$ is called an integral basis [dt. Ganzheitsbasis] if $\forall \alpha \in \mathcal{O}_K\ \exists!\, c_1,\dots,c_n \in \mathbb{Z} : \alpha = c_1\omega_1 + \cdots + c_n\omega_n$.

Remarks: 1) If there is an integral basis with n elements then $(\mathcal{O}_K, +)$ is a free abelian group of rank n, i.e., an integral basis is a $\mathbb{Z}$-basis. By Theorem 3 the number of elements of an integral basis is uniquely determined, i.e., if $\{\omega_1,\dots,\omega_n\}$ and $\{\gamma_1,\dots,\gamma_m\}$ are both integral bases for K then $n = m$.

2) So far, we have not established the existence of an integral basis for any algebraic number field. (However, we will prove shortly that they exist for every algebraic number field.)

3) If $\{\omega_1,\dots,\omega_n\}$ is an integral basis for K then it is also a basis of K as a $\mathbb{Q}$-vector space (which contains only elements of $\mathcal{O}_K$). Let $\alpha \in K$. Then $\exists\, c_0 \in \mathbb{Z}\setminus\{0\} : c_0\alpha \in \mathcal{O}_K$ and therefore $\exists c_1,\dots,c_n \in \mathbb{Z} : c_0\alpha = \sum_{i=1}^{n} c_i\omega_i$ which implies $\alpha = \sum_{i=1}^{n} \frac{c_i}{c_0}\omega_i$. Furthermore, $\omega_1,\dots,\omega_n$ are linearly independent over $\mathbb{Q}$. Suppose

$\sum_{i=1}^{n} q_i\omega_i = 0$ (with $q_1,\dots,q_n \in \mathbb{Q}$). Then $\exists c \in \mathbb{Z}\setminus\{0\}: cq_1,\dots,cq_n \in \mathbb{Z}$ and therefore $\sum_{i=1}^{n} (cq_i)\omega_i = 0$. By assumption $cq_i = 0$ (for $1 \le i \le n$) and thus $q_1 = \dots = q_n = 0$.

4) Remark 3) implies immediately: if $\{\omega_1,\dots,\omega_n\}$ is an integral basis for K, then $n = [K:\mathbb{Q}]$.

5) Every algebraic number field K has a basis (as a $\mathbb{Q}$-vector space) that contains only elements of $\mathcal{O}_K$. By Corollary 54 $\exists \alpha \in \mathcal{O}_K: K = \mathbb{Q}(\alpha)$ and $\{1,\alpha,\dots,\alpha^{n-1}\}$ (with $n = [K:\mathbb{Q}]$) is a basis of K (as a $\mathbb{Q}$-vector space) containing only elements of $\mathcal{O}_K$. However, not every basis of K (as a $\mathbb{Q}$-vector space) containing only elements of $\mathcal{O}_K$ is an integral basis. Let, e.g., $K = \mathbb{Q}(\sqrt{5})$. Then $\{1,\sqrt{5}\}$ is a basis of K (as a $\mathbb{Q}$-vector space) containing only elements of $\mathcal{O}_K$ but $\mathbb{Z}+\mathbb{Z}\sqrt{5} \subsetneq \mathcal{O}_K$ as $\frac{1+\sqrt{5}}{2} \in \mathcal{O}_K$ and $\frac{1+\sqrt{5}}{2} \notin \mathbb{Z}+\mathbb{Z}\sqrt{5}$.

16.11.2022

<u>Lemma 60</u> Let K be an algebraic number field with $[K:\mathbb{Q}] = n$. Let $\{\alpha_1,\dots,\alpha_n\}$ be a basis of K (as a $\mathbb{Q}$-vector space) which contains only elements of $\mathcal{O}_K$. Let

$$d := \Delta_{K/\mathbb{Q}}(\alpha_1,\dots,\alpha_n)$$

(i) $d \in \mathbb{Z}\setminus\{0\}$,

(ii) $d \cdot \mathcal{O}_K \subseteq \mathbb{Z}\alpha_1 + \dots + \mathbb{Z}\alpha_n$.

<u>Proof</u>: Let $\alpha \in \mathcal{O}_K$. Then $\exists a_1,\dots,a_n \in \mathbb{Q}: \alpha = \sum_{j=1}^{n} a_j\alpha_j$ which implies $\alpha_i\alpha = \sum_{j=1}^{n} a_j(\alpha_i\alpha_j)$ and therefore $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha) \overset{\text{Lemma 22}}{=} \sum_{j=1}^{n} a_j \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)$ for $1 \le i \le n$. This shows that $(a_1,\dots,a_n) \in \mathbb{Q}^n$ is a solution of the following system of linear equations:

$$\sum_{j=1}^{n} \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)\cdot x_j = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha) \quad \text{for } 1 \le i \le n.$$

It follows from $\alpha \in \mathcal{O}_K$ and $\alpha_i \in \mathcal{O}_K$ (for $1 \le i \le n$) that $\alpha_i\alpha \in \mathcal{O}_K$ (for $1 \le i \le n$) and $\alpha_i\alpha_j \in \mathcal{O}_K$ (for $1 \le i,j \le n$). By Theorem 59 (i) $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha) \in \mathbb{Z}$ (for $1 \le i \le n$) and $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j) \in \mathbb{Z}$ (for $1 \le i,j \le n$). This implies

$$0 \overset{\text{Th 33}}{\neq} d = \Delta_{K/\mathbb{Q}}(\alpha_1,\dots,\alpha_n) \overset{\text{Th 29}}{=} \det\Big(\underbrace{(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j))_{1\le i,j\le n}}_{\in \mathbb{Z}}\Big) \in \mathbb{Z},$$

which shows (i).

Cramer's rule yields

$$a_i := \frac{1}{d} \underbrace{\begin{vmatrix} \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_1^2) & \cdots & \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_1\alpha_{i-1}) & \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_1\alpha) & \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_1\alpha_{i+1}) & \cdots & \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_1\alpha_n) \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_n\alpha_1) & \cdots & \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_n\alpha_{i-1}) & \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_n\alpha) & \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_n\alpha_{i+1}) & \cdots & \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_n^2) \end{vmatrix}}_{\in\mathbb{Z}} \quad \text{for } 1\le i\le n$$

Therefore $da_i \in \mathbb{Z}$ (for $1\le i\le n$) and thus $d\alpha = \sum_{j=1}^{n} (da_j)\alpha_j \in \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$.

Theorem 61 (DEDEKIND) Every algebraic number field K has an integral basis, i.e., $(\mathcal{O}_K, +)$ is a free abelian group of rank $[K:\mathbb{Q}]$.

1st proof: According to Corollary 54 there is an $\alpha\in\mathcal{O}_K$ such that $K=\mathbb{Q}(\alpha)$. Therefore $\{1,\alpha,\dots,\alpha^{n-1}\}$ (with $n=[K:\mathbb{Q}]$) is a basis of K (as a $\mathbb{Q}$-vector space) containing only elements of $\mathcal{O}_K$. Let $d := \Delta_{K/\mathbb{Q}}(1,\alpha,\dots,\alpha^{n-1})$. By Lemma 60 $d\in\mathbb{Z}\setminus\{0\}$ and $d\cdot\mathcal{O}_K \subseteq \mathbb{Z}+\mathbb{Z}\alpha+\cdots+\mathbb{Z}\alpha^{n-1}$. This implies

$$\mathbb{Z}+\mathbb{Z}\alpha+\cdots+\mathbb{Z}\alpha^{n-1} \subseteq \mathcal{O}_K \subseteq \mathbb{Z}\tfrac{1}{d}+\mathbb{Z}\tfrac{\alpha}{d}+\cdots+\mathbb{Z}\tfrac{\alpha^{n-1}}{d}$$

Obviously $\left(\mathbb{Z}\frac{1}{d}+\mathbb{Z}\frac{\alpha}{d}+\cdots+\mathbb{Z}\frac{\alpha^{n-1}}{d}, +\right)$ is a free abelian group of rank n. (The set $\{\frac{1}{d}, \frac{\alpha}{d}, \dots, \frac{\alpha^{n-1}}{d}\}$ is linearly independent over $\mathbb{Z}$ as $\{1,\alpha,\dots,\alpha^{n-1}\}$ is linearly independent over $\mathbb{Q}$.) By Theorem 5 $(\mathcal{O}_K,+)$ is a free abelian group of rank $r\le n$. Furthermore, $(\mathcal{O}_K,+)$ has the free abelian group $(\mathbb{Z}+\mathbb{Z}\alpha+\cdots+\mathbb{Z}\alpha^{n-1},+)$ of rank n as a subgroup. Therefore $n\le r$ (again by Theorem 5) and thus $r=n$, i.e., $(\mathcal{O}_K,+)$ is a free abelian group of rank n.

2nd proof: Let $n:=[K:\mathbb{Q}]$ (as in the first proof) and

$$S := \left\{ |\Delta_{K/\mathbb{Q}}(\alpha_1,\dots,\alpha_n)| \,\middle|\, \{\alpha_1,\dots,\alpha_n\} \text{ is a basis of } K \text{ (as a } \mathbb{Q}\text{-vector space) with } \{\alpha_1,\dots,\alpha_n\}\subseteq\mathcal{O}_K \right\}$$

We know $S\neq\emptyset$ and as $\Delta_{K/\mathbb{Q}}(\alpha_1,\dots,\alpha_n)\in\mathbb{Z}\setminus\{0\}$ for such $\{\alpha_1,\dots,\alpha_n\}$ (by Lemma 60) we see $S\subseteq\mathbb{N}$. Let $\{\omega_1,\dots,\omega_n\}$ $(\subseteq\mathcal{O}_K)$ be a basis of K (as a $\mathbb{Q}$-vector space) such that $|\Delta_{K/\mathbb{Q}}(\alpha_1,\dots,\alpha_n)| = \min S$. We claim that $\{\omega_1,\dots,\omega_n\}$ is an integral basis. Suppose that $\{\omega_1,\dots,\omega_n\}$ is not an integral basis. As every $\alpha\in K$ has a unique representation $\alpha=\sum_{j=1}^{n} c_j\omega_j$ (with $c_1,\dots,c_n\in\mathbb{Q}$) there has to exist an $\alpha\in\mathcal{O}_K$ with the property that at least one $c_j\in\mathbb{Q}\setminus\mathbb{Z}$. W.l.o.g. let $c_1 = c+r$ where $c=[c_1]$

and $x \in (0,1) \cap \mathbb{Q}$. Let $\eta_1 := \alpha - c\omega_1 = x\omega_1 + c_2\omega_2 + \cdots + c_n\omega_n$ and $\eta_i := \omega_i$ for $2 \le i \le n$. Then $\{\eta_1, \dots, \eta_n\}$ is a basis of K (as a $\mathbb{Q}$-vector space) by results from linear algebra and contains only elements of $\mathcal{O}_K$. The determinant of the matrix representation for the change of basis is

$$\begin{vmatrix} x & c_2 & c_3 & \cdots & c_n \\ & 1 & & 0 & \\ & & 1 & & \\ & 0 & & \ddots & \\ & & & & 1 \end{vmatrix} = x$$

and therefore $\Delta_{K|\mathbb{Q}}(\eta_1, \dots, \eta_n) \overset{\text{Lemma 31}}{=} x^2 \Delta_{K|\mathbb{Q}}(\omega_1, \dots, \omega_n)$ which implies

$|\Delta_{K|\mathbb{Q}}(\omega_1, \dots, \omega_n)| > x^2 |\Delta_{K|\mathbb{Q}}(\omega_1, \dots, \omega_n)| = |\Delta_{K|\mathbb{Q}}(\eta_1, \dots, \eta_n)|$, a contradiction.

Theorem 62 Let K be an algebraic number field with $[K:\mathbb{Q}] = n$ and $\{\alpha_1, \dots, \alpha_n\}$ a basis of K (as a $\mathbb{Q}$-vector space) containing only elements of $\mathcal{O}_K$. If $\Delta_{K|\mathbb{Q}}(\alpha_1, \dots, \alpha_n)$ is squarefree then $\{\alpha_1, \dots, \alpha_n\}$ is an integral basis.

Proof: Let $\{\omega_1, \dots, \omega_n\}$ be an integral basis of K. Then there are $c_{ij} \in \mathbb{Z}$ (with $1 \le i,j \le n$) such that $\alpha_i = \sum_{j=1}^{n} c_{ij}\omega_j$ $(1 \le i \le n)$. Let $C := (c_{ij})_{1 \le i,j \le n}$. Then

$\Delta_{K|\mathbb{Q}}(\alpha_1, \dots, \alpha_n) \overset{\text{Lemma 31}}{=} (\det C)^2 \cdot \Delta_{K|\mathbb{Q}}(\omega_1, \dots, \omega_n)$. As $\Delta_{K|\mathbb{Q}}(\alpha_1, \dots, \alpha_n)$ is squarefree we get $\det C \in \{1, -1\}$, i.e., C is unimodular and $\{\alpha_1, \dots, \alpha_n\}$ is an integral basis by Lemma 4.

Remarks: 1) The converse of Theorem 62 is not correct, i.e., there are integral bases $\{\omega_1, \dots, \omega_n\}$ such that $\Delta_{K|\mathbb{Q}}(\omega_1, \dots, \omega_n)$ is not squarefree: (Examples will follow shortly)

2) The proof of Theorem 62 shows the following: if $\{\alpha_1, \dots, \alpha_n\}$ is a basis of K (as a $\mathbb{Q}$-vector space) containing only elements of $\mathcal{O}_K$ and $\{\omega_1, \dots, \omega_n\}$ is an integral basis for K, then $\Delta_{K|\mathbb{Q}}(\omega_1, \dots, \omega_n) \mid \Delta_{K|\mathbb{Q}}(\alpha_1, \dots, \alpha_n)$ and $\Delta_{K|\mathbb{Q}}(\alpha_1, \dots, \alpha_n) / \Delta_{K|\mathbb{Q}}(\omega_1, \dots, \omega_n)$ is a square (in $\mathbb{Z}$).

Definition: Let K be an algebraic number field and $\{\omega_1, \dots, \omega_n\}$ an integral basis for K. Then $d_K := \Delta_{K|\mathbb{Q}}(\omega_1, \dots, \omega_n)$ is called the discriminant of K [dt. Diskriminante von K]

Remark: If $\{\omega_1, \dots, \omega_n\}$ and $\{\eta_1, \dots, \eta_n\}$ are two integral bases for K, there are $c_{ij} \in \mathbb{Z}$ (with $1 \le i,j \le n$) such that $\eta_i = \sum_{j=1}^{n} c_{ij}\omega_j$. If $C := (c_{ij})_{1 \le i,j \le n}$ then C is unimodular by Lemma 4 (i.e., $\det C \in \{1, -1\}$) and Lemma 31 implies $\Delta_{K|\mathbb{Q}}(\eta_1, \dots, \eta_n) = (\det C)^2 \Delta_{K|\mathbb{Q}}(\omega_1, \dots, \omega_n) = \Delta_{K|\mathbb{Q}}(\omega_1, \dots, \omega_n)$. This shows that d_K is well defined and $d_K \in \mathbb{Z} \setminus \{0\}$ (because of Lemma 60).

Corollary 63 Let K be an algebraic number field with $[K:\mathbb{Q}]=n$ and $\alpha \in \mathcal{O}_K$ such that $K=\mathbb{Q}(\alpha)$. If $\Delta_{K|\mathbb{Q}}(1,\alpha,\dots,\alpha^{n-1})$ is squarefree, then $\{1,\alpha,\dots,\alpha^{n-1}\}$ is an integral basis for K, $\mathcal{O}_K=\mathbb{Z}[\alpha]$ and $d_K=\Delta_{K|\mathbb{Q}}(1,\alpha,\dots,\alpha^{n-1})$.

Proof: As $K=\mathbb{Q}(\alpha)$, clearly $\{1,\alpha,\dots,\alpha^{n-1}\}$ is a basis of K (as a $\mathbb{Q}$-vector space) containing only elements of $\mathcal{O}_K$. As $\Delta_{K|\mathbb{Q}}(1,\alpha,\dots,\alpha^{n-1})$ is squarefree, $\{1,\alpha,\dots,\alpha^{n-1}\}$ is an integral basis for K (by Theorem 62). This implies $\mathcal{O}_K=\mathbb{Z}[\alpha]$ and $d_K=\Delta_{K|\mathbb{Q}}(1,\alpha,\dots,\alpha^{n-1})$.

Corollary 64 Let K be an algebraic number field with $[K:\mathbb{Q}]=n$ and $\alpha \in \mathcal{O}_K$ such that $K=\mathbb{Q}(\alpha)$. If $\{1,\alpha,\dots,\alpha^{n-1}\}$ is an integral basis for K then

$$d_K=(-1)^{\frac{n(n-1)}{2}} N_{K|\mathbb{Q}}(m'_{\alpha,\alpha}(\alpha)).$$

Proof: $d_K=\Delta_{K|\mathbb{Q}}(1,\alpha,\dots,\alpha^{n-1}) \overset{\text{Theorem 34}}{=} (-1)^{\frac{n(n-1)}{2}} N_{K|\mathbb{Q}}(m'_{\alpha,\alpha}(\alpha))$.

Remark: There are (infinitely many, pairwise not isomorphic) algebraic number fields K such that $\mathcal{O}_K=\mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$. (Examples will follow shortly.) However, it is not possible to find such an α for every algebraic number field K.

Theorem 65 Let K be an algebraic number field with $[K:\mathbb{Q}]=n$ and $\alpha_1,\dots,\alpha_n \in \mathcal{O}_K$. Then $\Delta_{K|\mathbb{Q}}(\alpha_1,\dots,\alpha_n) \equiv 0 \pmod 4$ or $\Delta_{K|\mathbb{Q}}(\alpha_1,\dots,\alpha_n) \equiv 1 \pmod 4$.

21.11.2022

Proof: The Leibniz formula for the determinant yields

$$\det\left((\sigma_i(\alpha_j))_{1\le i,j\le n}\right) = \sum_{\substack{\pi\in S_n \\ \operatorname{sgn}\pi=1}} \prod_{i=1}^{n} \sigma_i(\alpha_{\pi(i)}) - \sum_{\substack{\pi\in S_n \\ \operatorname{sgn}\pi=-1}} \prod_{i=1}^{n} \sigma_i(\alpha_{\pi(i)})$$

where $\sigma_1,\dots,\sigma_n$ are the different homomorphisms $\sigma_i: K \hookrightarrow \mathbb{C}$ (with $\sigma_i|_{\mathbb{Q}}=\mathrm{id}_{\mathbb{Q}}$) for $1\le i\le n$ and S_n denotes the symmetric group. Clearly

$$A:=\sum_{\substack{\pi\in S_n \\ \operatorname{sgn}\pi=1}} \prod_{i=1}^{n} \sigma_i(\alpha_{\pi(i)}) \in \mathcal{O} \quad \text{and} \quad B:=\sum_{\substack{\pi\in S_n \\ \operatorname{sgn}\pi=-1}} \prod_{i=1}^{n} \sigma_i(\alpha_{\pi(i)}) \in \mathcal{O}.$$

Let N be a field containing K such that $N/\mathbb{Q}$ is a normal field extension. (If $K=\mathbb{Q}(\beta)$ then let N be, e.g., the splitting field of $m_{\mathbb{Q},\beta}$. Theorem 26 implies that $N/\mathbb{Q}$ is a normal field extension.) By Theorem 20 σ_i can be extended to a homomorphism $\sigma_i: N \hookrightarrow \mathbb{C}$ (with $1\le i\le n$). Because of Theorem 25 these maps

can be considered as isomorphisms $\sigma_i : N \to N$. (We will always keep the notation σ_i although, strictly speaking, these are different maps. However, this will not lead to any problems.)

If $\varphi : N \to N$ is an isomorphism, then so is $\varphi \circ \sigma_i$ (for $1 \le i \le n$) and $\varphi\circ\sigma_1, \dots, \varphi\circ\sigma_n$ are pairwise different (as $\sigma_1, \dots, \sigma_n$ are pairwise different). As $\varphi \circ \sigma_i|_K : K \hookrightarrow \mathbb{C}$ is a homomorphism (and $\varphi \circ \sigma_i|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$) there has to exist a $\tau \in S_n$ such that $\varphi \circ \sigma_i = \sigma_{\tau(i)}$ (for $1 \le i \le n$). This implies

$$\varphi\Big(\prod_{i=1}^{n} \sigma_i(\alpha_{\pi(i)})\Big) = \prod_{i=1}^{n} (\varphi\circ\sigma_i)(\alpha_{\pi(i)}) = \prod_{i=1}^{n} \sigma_{\tau(i)}(\alpha_{\pi(i)}) = \prod_{i=1}^{n} \sigma_i(\alpha_{\pi\circ\tau^{-1}(i)})$$

and therefore

$$\varphi(A) = \sum_{\substack{\pi\in S_n \\ \mathrm{sgn}\,\pi = 1}} \varphi\Big(\prod_{i=1}^{n} \sigma_i(\alpha_{\pi(i)})\Big) = \sum_{\substack{\pi\in S_n \\ \mathrm{sgn}\,\pi = -1}} \prod_{i=1}^{n} \sigma_i(\alpha_{\pi\circ\tau^{-1}(i)}) = \begin{cases} \displaystyle\sum_{\substack{\pi\in S_n \\ \mathrm{sgn}\,\pi = 1}} \prod_{i=1}^{n} \sigma_i(\alpha_{\pi(i)}) = A & \text{if } \mathrm{sgn}\,\tau = 1 \\ \displaystyle\sum_{\substack{\pi\in S_n \\ \mathrm{sgn}\,\pi = -1}} \prod_{i=1}^{n} \sigma_i(\alpha_{\pi(i)}) = B & \text{if } \mathrm{sgn}\,\tau = -1 \end{cases}$$

and completely analogously $\varphi(B) = \begin{cases} B & \text{if } \mathrm{sgn}\,\tau = 1, \\ A & \text{if } \mathrm{sgn}\,\tau = -1. \end{cases}$ In both cases we have

$\varphi(A+B) = A+B$ and $\varphi(AB) = AB$. As $\varphi : N \to N$ was an arbitrary isomorphism we get $A+B, AB \in \mathbb{Q}$. (Otherwise we could use Theorems 17 and 20 to find an isomorphism $\varphi : N \to N$ with $\varphi(A+B) \neq A+B$ or $\varphi(AB) \neq AB$.) This implies $A+B, AB \in \mathbb{Q} \cap \mathcal{O} \overset{\text{Cor. 57}}{=} \mathbb{Z}$ and therefore

$$\Delta_{K|\mathbb{Q}}(\alpha_1, \dots, \alpha_n) = (A-B)^2 = (A+B)^2 - 4AB \equiv (A+B)^2 \pmod 4.$$

This implies our assertion as $(A+B)^2 \equiv 0 \pmod 4$ if $A+B$ is even and $(A+B)^2 \equiv 1 \pmod 4$ if $A+B$ is odd.

Corollary 66 (STICKELBERGER) Let K be an algebraic number field. Then $d_K \equiv 0 \pmod 4$ or $d_K \equiv 1 \pmod 4$.

Proof: Use Theorem 65 with $\{\alpha_1, \dots, \alpha_n\}$ an integral basis for K.

Definition: Let K be an algebraic number field. If $\sigma: K \hookrightarrow \mathbb{C}$ is a homomorphism then so is $\overline{\sigma}: K \hookrightarrow \mathbb{C}, \alpha \mapsto \overline{\sigma(\alpha)}$ (where $\overline{z}$ denotes the complex conjugate of $z \in \mathbb{C}$). If $\sigma(K) \subseteq \mathbb{R}$ then $\overline{\sigma} = \sigma$, but if $\sigma(K) \not\subseteq \mathbb{R}$ then $\overline{\sigma} \neq \sigma$. Let

$$r = r(K) = \left|\{\sigma: K \hookrightarrow \mathbb{C} \mid \sigma \text{ is a homomorphism}, \sigma(K) \subseteq \mathbb{R}\}\right|$$

and

$$s = s(K) = \tfrac{1}{2}\left|\{\sigma: K \hookrightarrow \mathbb{C} \mid \sigma \text{ is a homomorphism}, \sigma(K) \not\subseteq \mathbb{R}\}\right|.$$

If $[K:\mathbb{Q}] = n$ then $n = r + 2s$. The algebraic number field K is called *totally imaginary* [dt. *total imaginär*] if $r(K) = 0$ (i.e., K cannot be embedded in $\mathbb{R}$) and K is called *totally real* [dt. *total reell*] if $s(K) = 0$ (i.e., $\sigma(K) \subseteq \mathbb{R}$ for each embedding $\sigma: K \hookrightarrow \mathbb{C}$).

Remark: If $K/\mathbb{Q}$ is a normal field extension, K has to be either totally imaginary or totally real as $\sigma(K) = K$ for each embedding $\sigma: K \hookrightarrow \mathbb{C}$.

Examples: 1) If $K = \mathbb{Q}(\sqrt{2})$ then $r = 2$ and $s = 0$, i.e., $\mathbb{Q}(\sqrt{2})$ is totally real.

2) If $K = \mathbb{Q}(i)$ then $r = 0$ and $s = 1$, i.e., $\mathbb{Q}(i)$ is totally imaginary.

3) If $K = \mathbb{Q}(\sqrt[3]{2})$ then $r = 1$ and $s = 1$.

Theorem 67 (BRILL) Let K be an algebraic number field. Then $\operatorname{sgn} d_K = (-1)^s = (-1)^{s(K)}$.

Proof: Let $\sigma_1, \dots, \sigma_r: K \hookrightarrow \mathbb{C}$ be the homomorphisms with $\sigma_i(K) \subseteq \mathbb{R}$ (for $1 \le i \le r$) and $\sigma_{r+1}, \overline{\sigma_{r+1}}, \dots, \sigma_{r+s}, \overline{\sigma_{r+s}}: K \hookrightarrow \mathbb{C}$ the homomorphisms with $\sigma_i(K) \not\subseteq \mathbb{R}$ (for $r < i \le r+s$). Let $n = [K:\mathbb{Q}]$ and let $\{\omega_1, \dots, \omega_n\}$ be an integral basis for K. Set

$$d_1 + i d_2 := \begin{vmatrix} \sigma_1(\omega_1) & \cdots & \sigma_r(\omega_1) & \sigma_{r+1}(\omega_1) & \overline{\sigma_{r+1}}(\omega_1) & \cdots & \sigma_{r+s}(\omega_1) & \overline{\sigma_{r+s}}(\omega_1) \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \sigma_1(\omega_n) & \cdots & \sigma_r(\omega_n) & \sigma_{r+1}(\omega_n) & \overline{\sigma_{r+1}}(\omega_n) & \cdots & \sigma_{r+s}(\omega_n) & \overline{\sigma_{r+s}}(\omega_n) \end{vmatrix} \quad (\text{with } d_1, d_2 \in \mathbb{R})$$

Complex conjugation yields

$$d_1 - i d_2 = \begin{vmatrix} \sigma_1(\omega_1) & \cdots & \sigma_r(\omega_1) & \overline{\sigma_{r+1}(\omega_1)} & \sigma_{r+1}(\omega_1) & \cdots & \overline{\sigma_{r+s}(\omega_1)} & \sigma_{r+s}(\omega_1) \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \sigma_1(\omega_n) & \cdots & \sigma_r(\omega_n) & \overline{\sigma_{r+1}(\omega_n)} & \sigma_{r+1}(\omega_n) & \cdots & \overline{\sigma_{r+s}(\omega_n)} & \sigma_{r+s}(\omega_n) \end{vmatrix} = (-1)^s (d_1 + i d_2).$$

If $2 \mid s$ then $d_2 = 0$ and $d_K = d_1^2 > 0$. If $2 \nmid s$ then $d_1 = 0$ and $d_K = (i d_2)^2 = -d_2^2 < 0$.

In both cases $\operatorname{sgn} d_K = (-1)^s$.