2. Algebraic number fields

Definition: A subfield K of $\mathbb{C}$ with the property $[K:\mathbb{Q}] < \infty$ is called an algebraic number field [dt. Algebraischer Zahlkörper].

Definition: Let K be a field. An irreducible polynomial $p \in K[X]$ is called separable [dt. separabel] if it has only simple roots (in a splitting field of p over K).

Remark: We know (from algebra) that an irreducible polynomial p has only simple roots if and only if $p' \neq 0$ (where p' denotes the formal derivative of p).

Lemma 11 Let K be a field and let $p \in K[X]$ be irreducible. Then p is separable if and only if $p' \neq 0$.

Proof: This follows immediately from the remark above.

Corollary 12 Let K be a field with $\operatorname{char} K = 0$ and let $p \in K[X]$ be irreducible. Then p is separable.

Proof: As $\operatorname{char} K = 0$ we get $\deg p' = \deg p - 1 \geq 1 - 1 = 0$ and therefore $p' \neq 0$

Definition: Let L/K be a field extension and let $\alpha \in L$ be algebraic over K. Then α is called separable (over K) if its minimal polynomial $m_{K,\alpha} \in K[X]$ is separable.

Definition: An algebraic field extension L/K is called separable if all $\alpha \in L$ are separable (over K).

Corollary 13 Let L/K be an algebraic field extension with $\operatorname{char} K = \operatorname{char} L = 0$. Then L/K is a separable extension.

Proof: This follows immediately from Corollary 12.

Corollary 14 Let L/K be a field extension of algebraic number fields. Then L/K is a separable extension.

Proof: As $[L:K] = \frac{[L:\mathbb{Q}]}{[K:\mathbb{Q}]} < \infty$ we know that L/K is a finite extension and therefore an algebraic extension. The assertion follows from Corollary 13.

Theorem 15 (primitive element theorem [dt. Satz vom primitiven Element])
Let K be an infinite field and L/K a finite separable field extension. Then L/K is a simple extension, i.e., there is a (primitive element) $\alpha \in L$ such that $L = K(\alpha)$.

Proof: As a first step we show that $\forall \beta,\gamma \in L \; \exists \alpha \in L : K(\beta,\gamma) = K(\alpha)$

Let $m_{K,\beta}(X) = \prod_{i=1}^{n} (X-\beta_i)$ and $m_{K,\gamma}(X) = \prod_{j=1}^{m} (X-\gamma_j)$ be the factorizations of the minimal polynomials of β and γ (in a splitting field $\tilde{K}$ of $m_{K,\beta} \cdot m_{K,\gamma}$), where we assume $\beta_1 = \beta$ and $\gamma_1 = \gamma$. As L/K is seperable we know $\beta \neq \beta_i$ (for $2 \leq i \leq n$) and $\gamma \neq \gamma_j$ (for $2 \leq j \leq m$). As K is infinite there is a $\lambda \in K \setminus \{0\}$ such that $\lambda \notin \left\{ \frac{\beta-\beta_i}{\gamma_j-\gamma} \;\middle|\; 2 \leq i \leq n, 2 \leq j \leq m \right\}$. Let $\alpha := \beta + \lambda\gamma$. We claim $K(\alpha) = K(\beta,\gamma)$

Clearly $K(\alpha)$ is an intermediate field of the extension $K(\beta,\gamma)/K$. In order to prove $K(\alpha) = K(\beta,\gamma)$ it suffices to prove $\gamma \in K(\alpha)$ as $\beta = \alpha - \lambda\gamma \in K(\alpha)$ follows.

Consider the polynomial $p(X) = m_{K,\beta}(\alpha - \lambda X) \in K(\alpha)[X]$. As

$$p(\gamma) = m_{K,\beta}(\alpha - \lambda\gamma) = m_{K,\beta}(\beta + \lambda\gamma - \lambda\gamma) = m_{K,\beta}(\beta) = 0$$

we see that p and $m_{K,\gamma}$ have γ as a common root. We claim that it is the only one. For if $\xi \in \tilde{K}$ with $\xi \neq \gamma$ has the property $p(\xi) = m_{K,\gamma}(\xi) = 0$ then $\exists i \in \{1,\dots,n\} : \alpha - \lambda\xi = \beta_i$ and $\exists j \in \{1,\dots,m\} : \xi = \gamma_j$. As $\xi \neq \gamma$ we see $j \neq 1$ and $\alpha - \lambda\xi = \beta + \lambda\gamma - \lambda\gamma_j = \beta_i$ implies $\beta - \beta_i = \lambda(\gamma_j - \gamma) \neq 0$ and therefore $i \neq 1$. Thus $\lambda = \frac{\beta-\beta_i}{\gamma_j-\gamma}$ for some $i \in \{2,\dots,n\}, j \in \{2,\dots,m\}$ which contradicts our choice of λ. We know $m_{K(\alpha),\gamma} \mid p$ and $m_{K(\alpha),\gamma} \mid m_{K,\gamma}$ in the polynomial ring $K(\alpha)[X]$. As p and $m_{K,\gamma}$ have only one common root and γ is a simple root of $m_{K,\gamma}$ we see $\deg m_{K(\alpha),\gamma} = 1$. As $m_{K(\alpha),\gamma}(\gamma) = 0$ we arrive at $m_{K(\alpha),\gamma}(X) = X - \gamma \in K(\alpha)[X]$ which shows $\gamma \in K(\alpha)$.

In the second step we show that $\forall \beta_1,\dots,\beta_n \in L \; \exists \alpha \in L : K(\beta_1,\dots,\beta_n) = K(\alpha)$ by induction on n. This is trivial for $n=1$ and has just been proved for $n=2$.

If our claim has already been proved for some $n \geq 2$ we know that there is a $\tilde{\alpha} \in L : K(\beta_1,\dots,\beta_n) = K(\tilde{\alpha})$ and therefore

$$K(\beta_1,\dots,\beta_n,\beta_{n+1}) = K(\beta_1,\dots,\beta_n)(\beta_{n+1}) = K(\tilde{\alpha})(\beta_{n+1}) = K(\tilde{\alpha},\beta_{n+1}) = K(\alpha)$$

for some $\alpha \in L$ by the case $n=2$

As L/K is a finite extension there are $\beta_1,\dots,\beta_n \in L$ which are a basis of L as a K-vector space. As $K(\beta_1,\dots,\beta_n) \subseteq L = K\beta_1 + \dots + K\beta_n \subseteq K(\beta_1,\dots,\beta_n)$ we get $L = K(\beta_1,\dots,\beta_n)$ and the theorem follows from the second step.

Remark: The following result is often presented as part of the primitive element theorem. We probably will not need it but present it for the sake of completeness.

Theorem 16 Let K be finite field and L/K a finite field extension. Then there is an $\alpha \in L$: $L = K(\alpha)$

Proof: As $L \cong K^{[L:K]}$ (isomorphism of vector spaces) L is also finite field and by a theorem from algebra $(L^*, \cdot)$ is a cyclic group. Let $\alpha \in L^*$ be a generator, i.e., $L^* = \langle \alpha \rangle = \{1, \alpha, \alpha^2, \dots, \alpha^{|L|-1}\}$. Then $L = K(\alpha)$.

Remarks: 1) The primitive element in Theorem 15 is not uniquely determined as there are infinitely many possible choices for λ and $K(\alpha) = K(\alpha+1) = K(\alpha+2) = \dots$

2) Most important for us is the following case: Let L/K be an extension of algebraic number fields. Then $\exists \alpha \in L: L = K(\alpha)$. Note that this includes the following: If K is an algebraic number field then $\exists \alpha \in K: K = \mathbb{Q}(\alpha)$.

3) The proof of Theorem 15 can be used to find primitive elements. Let, e.g., $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Here $\beta = \beta_1 = \sqrt{2}$ and $\gamma = \gamma_1 = \sqrt{3}$ $\Rightarrow \beta_2 = -\sqrt{2}$, $\gamma_2 = -\sqrt{3}$ and $\frac{\beta - \beta_2}{\gamma^2 - \gamma} = -\frac{2\sqrt{2}}{2\sqrt{3}} = -\frac{\sqrt{2}}{\sqrt{3}} = -\frac{\sqrt{6}}{3}$. I.e., any $\lambda \in \mathbb{Q} \setminus \{0, -\frac{\sqrt{2}}{\sqrt{3}}\}$ has the property $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \lambda\sqrt{3})$. E.g., with $\lambda = 1$ we get $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

4) Let $L = K(\alpha)$ be a simple extension where α is algebraic over K. Then $K(\alpha) = K[\alpha]$, $[L:K] = \deg m_{K,\alpha}$ and $\{1, \alpha, \alpha^2, \dots, \alpha^{d-1}\}$ (with $d = \deg m_{K,\alpha}$) is a basis of L as a K-vector space. I.e., for all $x \in L$ there are uniquely determined $a_0, a_1, \dots, a_{d-1} \in K$ such that $x = a_0 + a_1\alpha + \dots + a_{d-1}\alpha^{d-1}$ (see algebra).

Theorem 17 Let L/K be a field extension, $\alpha \in L$ algebraic over K and n (where $n \le d := \deg m_{K,\alpha} = [K(\alpha):K]$) the number of different roots of $m_{K,\alpha}$ (in an algebraic closure $\overline{K}$ of K). Then there are exactly n homomorphisms $\varphi: K(\alpha) \hookrightarrow \overline{K}$ with $\varphi|_K = \mathrm{id}_K$. If $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n \in \overline{K}$ are the different roots of $m_{K,\alpha}$ then these homomorphisms have shape $\varphi_j\left(\sum_{i=0}^{d-1} a_i \alpha^i\right) = \sum_{i=0}^{d-1} a_i \alpha_j^i$ (for $1 \le j \le n$) where $a_0, a_1, \dots, a_{d-1} \in K$.

Proof: Let $m_{K,\alpha}(x) = \sum_{i=0}^{d} b_i x^i \in K[x]$. If $\varphi: K(\alpha) \hookrightarrow \overline{K}$ is a homomorphism with $\varphi|_K = \mathrm{id}_K$ then

$$0 = \varphi(0) = \varphi\left(m_{K,\alpha}(\alpha)\right) = \varphi\left(\sum_{i=0}^{d} b_i \alpha^i\right) = \sum_{i=0}^{d} b_i \varphi(\alpha)^i = m_{K,\alpha}(\varphi(\alpha)),$$

i.e., $\varphi(\alpha)$ is a root of $m_{K,\alpha}$ and $\exists j \in \{1,\dots,n\} : \varphi(\alpha) = \alpha_j$.

Therefore $\varphi\left(\sum_{i=0}^{d-1} a_i \alpha^i\right) = \sum_{i=0}^{d-1} a_i \alpha_j^i$ and $\varphi = \varphi_j$. Note, that if $p(x) = \sum_{i=0}^{d-1} a_i x^i \in K[x]$ then $\varphi_j(p(\alpha)) = p(\varphi_j(\alpha)) = p(\alpha_j)$.

12.10.2022

The maps $\varphi_1,\dots,\varphi_n$ are all different as $\varphi_1(\alpha) = \alpha_1 = \alpha$, $\varphi_2(\alpha) = \alpha_2, \dots, \varphi_n(\alpha) = \alpha_n$ are all different. It remains to check that $\varphi_1,\dots,\varphi_n$ are homomorphisms. Let $1 \le j \le n$ and $p_1, p_2 \in K[x]$ with $\deg p_1, \deg p_2 < d$. Then, using the properties of the substitution homomorphism, we get

$$\varphi_j(p_1(\alpha) + p_2(\alpha)) = \varphi_j((p_1+p_2)(\alpha)) = (p_1+p_2)(\alpha_j) = p_1(\alpha_j) + p_2(\alpha_j) = \varphi_j(p_1(\alpha)) + \varphi_j(p_2(\alpha))$$

and

$$\varphi_j(p_1(\alpha)\cdot p_2(\alpha)) = \varphi_j((p_1\cdot p_2)(\alpha)) = (p_1 p_2)(\alpha_j) = p_1(\alpha_j)\cdot p_2(\alpha_j) = \varphi_j(p_1(\alpha))\cdot\varphi_j(p_2(\alpha))$$

Remark: Clearly in the above proof $m_{K,\alpha_j} = m_{K,\alpha}$ (for $1 \le j \le n$) and $\varphi_j : K(\alpha) \to K(\alpha_j)$ is an isomorphism.

Corollary 18 Let L/K be a finite separable field extension. Then there are exactly $[L:K]$ homomorphisms $\sigma : L \to \bar{K}$ with $\sigma|_K = \mathrm{id}_K$.

Proof: By the primitive element theorem (Theorems 15 and 16) there is an $\alpha \in L$: $L = K(\alpha)$. Theorem 17 implies that there are exactly $\deg m_{K,\alpha} = [K(\alpha):K] = [L:K]$ homomorphisms $\sigma : L \hookrightarrow \bar{K}$ with $\sigma|_K = \mathrm{id}_K$.

Remarks: If L/K is an extension of algebraic number fields then Corollary 18 implies that there are exactly $[L:K]$ homomorphisms $\sigma : L \hookrightarrow \mathbb{C}$ with $\sigma|_K = \mathrm{id}_K$. Especially important is the following special case: if K is an algebraic number field then there are exactly $[K:\mathbb{Q}]$ homomorphisms $\sigma : K \hookrightarrow \mathbb{C}$.

Examples: 1) If $K = \mathbb{Q}(i)$ then $m_{\mathbb{Q},i}(X) = X^2+1 = (X-i)(X+i)$ and $\sigma_1 = \mathrm{id}_{\mathbb{Q}(i)}$ (i.e., $\sigma_1(a+bi) = a+bi$) and $\sigma_2 = \overline{\sigma_1}$ (where the bar denotes complex conjugation, i.e., $\sigma_2(a+bi) = a-bi$).

2) If $K = \mathbb{Q}(\sqrt{2})$ then $m_{\mathbb{Q},\sqrt{2}}(X) = X^2-2 = (X-\sqrt{2})(X+\sqrt{2})$ and $\sigma_1 = \mathrm{id}_{\mathbb{Q}(\sqrt{2})}$ (i.e., $\sigma_1(a+b\sqrt{2}) = a+b\sqrt{2}$) and $\sigma_2(a+b\sqrt{2}) = a-b\sqrt{2}$.

3) More generally, let $d \in \mathbb{Z} \setminus \{0,1\}$ be squarefree and $K = \mathbb{Q}(\sqrt{d}) = \{a+b\sqrt{d} \mid a,b \in \mathbb{Q}\}$. Then $\sigma_1(a+b\sqrt{d}) = a+b\sqrt{d}$ and $\sigma_2(a+b\sqrt{d}) = a-b\sqrt{d}$. (This contains the first two examples as the special cases $d=-1$ and $d=2$.) If $d<0$ then $\sigma_2(\alpha) = \bar{\alpha}$.

4) If $K = \mathbb{Q}(\sqrt[3]{2})$ then $m_{\mathbb{Q},\sqrt[3]{2}}(x) = x^3 - 2$ which has roots $\sqrt[3]{2}, \sqrt[3]{2}e^{2\pi i/3}, \sqrt[3]{2}e^{4\pi i/3} \in \mathbb{C}$. Then $\sigma_1 : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2})$, $\sigma_1(a+b\sqrt[3]{2}+c\sqrt[3]{4}) = a+b\sqrt[3]{2}+c\sqrt[3]{4}$ (with $a,b,c \in \mathbb{Q}$), $\sigma_2 : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2}e^{2\pi i/3})$, $\sigma_2(a+b\sqrt[3]{2}+c\sqrt[3]{4}) = a+b\sqrt[3]{2}e^{2\pi i/3}+c\sqrt[3]{4}e^{4\pi i/3}$ and $\sigma_3 : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2}e^{4\pi i/3})$, $\sigma_3(a+b\sqrt[3]{2}+c\sqrt[3]{4}) = a+b\sqrt[3]{2}e^{4\pi i/3}+c\sqrt[3]{4}e^{2\pi i/3}$ (where we used $(e^{4\pi i/3})^2 = e^{8\pi i/3} = e^{2\pi i/3 + 2\pi i} = e^{2\pi i/3}$).
Note that $\mathbb{Q}(\sqrt[3]{2}e^{2\pi i/3}) \neq \mathbb{Q}(\sqrt[3]{2})$ as $e^{2\pi i/3} \in \mathbb{C}\setminus\mathbb{R}$ whereas $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$.

5) If $K = \mathbb{Q}(\sqrt[4]{2})$ then $m_{\mathbb{Q},\sqrt[4]{2}}(x) = x^4 - 2$ has roots $\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}i$ (as $x^4-2 = (x^2-\sqrt{2})(x^2+\sqrt{2}) = (x-\sqrt[4]{2})(x+\sqrt[4]{2})(x-\sqrt[4]{2}i)(x+\sqrt[4]{2}i)$) and the maps $\sigma_1,\sigma_2,\sigma_3,\sigma_4 : \mathbb{Q}(\sqrt[4]{2}) \hookrightarrow \mathbb{C}$ are determined by $\sigma_1(\sqrt[4]{2}) = \sqrt[4]{2}$, $\sigma_2(\sqrt[4]{2}) = -\sqrt[4]{2}$, $\sigma_3(\sqrt[4]{2}) = \sqrt[4]{2}i$ and $\sigma_4(\sqrt[4]{2}) = -\sqrt[4]{2}i$.

Lemma 19 Let L/K be a finite separable field extension and M an intermediate field. Then both L/M and M/K are finite separable field extensions.

Proof: It follows from $[L:K] = [L:M]\cdot[M:K]$ that both L/M and M/K are finite extensions. If $\alpha \in L$ then $m_{M,\alpha} \mid m_{K,\alpha}$ (in $M[x]$) and as $m_{K,\alpha}$ has only simple roots, $m_{M,\alpha}$ has only simple roots. As $M \subseteq L$ it is obvious that M/K is a separable extension.

Remark: Let R,S be commutative rings with identity and $\varphi : R \to S$ a ring homomorphism with $\varphi(1_R) = 1_S$. Then the map $R[x] \to S[x]$, $p \mapsto p^\varphi$ which maps $p(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ to $p^\varphi(x) = \sum_{i=0}^{n} \varphi(a_i) x^i \in S[x]$ is a ring homomorphism, i.e., $(p_1+p_2)^\varphi = p_1^\varphi + p_2^\varphi$ and $(p_1\cdot p_2)^\varphi = p_1^\varphi \cdot p_2^\varphi$ $\forall p_1,p_2 \in R[x]$ (see algebra). If $\varphi : R \to S$ is an isomorphism then $R[x] \to S[x]$, $p \mapsto p^\varphi$ is also an isomorphism.

Theorem 20 Let L/K be a finite separable field extension, $\alpha \in L$ and $\varphi : K(\alpha) \hookrightarrow \bar{K}$ a homomorphism. Then there are exactly $[L:K(\alpha)]$ homomorphisms $\psi : L \hookrightarrow \bar{K}$ with the property $\psi|_{K(\alpha)} = \varphi$.

Proof: Lemma 19 implies that $L/K(\alpha)$ is finite separable extension and by the primitive element theorem (Theorem 15) there is a $\beta \in L$ such that $L = K(\alpha)(\beta)$. Let $m_{K(\alpha),\beta}(x) = \sum_{i=0}^{d} c_i x^i \in K(\alpha)[x]$ with $d = \deg m_{K(\alpha),\beta} = [L:K(\alpha)]$.

If $\psi: L \hookrightarrow \overline{K}$ is a homomorphism with $\psi|_{K(\alpha)} = \varphi$ then

$$0 = \psi(0) = \psi\left(m_{K(\alpha),\beta}(\beta)\right) = \psi\left(\sum_{i=0}^{d} c_i \beta^i\right) = \sum_{i=0}^{d} \varphi(c_i)\, \psi(\beta)^i,$$

i.e., $\psi(\beta)$ is a root of $m^{\varphi}_{K(\alpha),\beta}$ which is also an irreducible and separable polynomial of degree d. Let $\beta_1, \dots, \beta_d$ be the different roots of $m^{\varphi}_{K(\alpha),\beta}$. Then $\exists j \in \{1,\dots,d\}: \psi(\beta) = \beta_j$ and $\psi\left(\sum_{i=0}^{d-1} a_i \beta^i\right) = \sum_{i=0}^{d-1} \varphi(a_i) \beta_j^i$ (where $a_0, \dots, a_{d-1} \in K(\alpha)$).

As $\beta_1, \dots, \beta_d$ are all different the maps $\psi_1, \dots, \psi_d$ with $\psi_j\left(\sum_{i=0}^{d-1} a_i \beta^i\right) = \sum_{i=0}^{d-1} \varphi(a_i) \beta_j^i$ (with $1 \le j \le d$) are all different. If $p \in K(\alpha)[x]$ with $\deg p < d$ we can write them as $\psi_j(p(\beta)) = p^{\varphi}(\beta_j)$. They are homomorphisms as

$$\begin{aligned}\psi_j(p_1(\beta) + p_2(\beta)) &= \psi_j((p_1+p_2)(\beta)) = (p_1+p_2)^{\varphi}(\beta_j) = (p_1^{\varphi} + p_2^{\varphi})(\beta_j) \\ &= p_1^{\varphi}(\beta_j) + p_2^{\varphi}(\beta_j) = \psi_j(p_1(\beta)) + \psi_j(p_2(\beta))\end{aligned}$$

and

$$\begin{aligned}\psi_j(p_1(\beta)\cdot p_2(\beta)) &= \psi_j((p_1 \cdot p_2)(\beta)) = (p_1 \cdot p_2)^{\varphi}(\beta_j) = (p_1^{\varphi} \cdot p_2^{\varphi})(\beta_j) \\ &= p_1^{\varphi}(\beta_j) \cdot p_2^{\varphi}(\beta_j) = \psi_j(p_1(\beta)) \cdot \psi_j(p_2(\beta)).\end{aligned}$$

Lemma 21 Let L/K be a field extension. For $\alpha \in L$ let φ_α denote the map $\varphi_\alpha: L \to L$, $\varphi_\alpha(x) = \alpha x$.

(i) φ_α is a K-linear map (of the K-vector space L) $\forall \alpha \in L$,

(ii) $\varphi_\alpha \circ \varphi_\beta = \varphi_{\alpha\beta}$ $\forall \alpha, \beta \in L$,

(iii) $\varphi_\alpha + \varphi_\beta = \varphi_{\alpha+\beta}$ $\forall \alpha, \beta \in L$.

Proof: (i) $\varphi_\alpha(x+y) = \alpha(x+y) = \alpha x + \alpha y = \varphi_\alpha(x) + \varphi_\alpha(y)$ $\forall x, y \in L$ and $\varphi_\alpha(xy) = \alpha(xy) = x(\alpha y) = x\varphi_\alpha(y)$ $\forall x, y \in L$.

(ii) $(\varphi_\alpha \circ \varphi_\beta)(x) = \varphi_\alpha(\varphi_\beta(x)) = \alpha(\beta x) = (\alpha\beta)x = \varphi_{\alpha\beta}(x)$ $\forall x \in L$.

(iii) $(\varphi_\alpha + \varphi_\beta)(x) = \varphi_\alpha(x) + \varphi_\beta(x) = \alpha x + \beta x = (\alpha+\beta)x = \varphi_{\alpha+\beta}(x)$ $\forall x \in L$.

Definition: If L/K is a finite field extension and $\alpha \in L$ we define the norm [dt Norm] $N_{L/K}(\alpha)$ of α as $N_{L/K}(\alpha) = \det \varphi_\alpha$ and the trace [dt Spur] $\mathrm{Tr}_{L/K}(\alpha)$ of α as $\mathrm{Tr}_{L/K}(\alpha) = \mathrm{tr}\,\varphi_\alpha$ (where $\det \varphi_\alpha$ and $\mathrm{tr}\,\varphi_\alpha$ denote the determinant and the trace of the linear map φ_α which was introduced in Lemma 21).

Remark: Note that by definition $N_{L/K}(\alpha), \mathrm{Tr}_{L/K}(\alpha) \in K$ $\forall \alpha \in L$.

Lemma 22 Let L/K be a finite field extension

(i) $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)\cdot N_{L/K}(\beta) \quad \forall \alpha,\beta \in L$,

(ii) $\mathrm{Tr}_{L/K}(\alpha+\beta) = \mathrm{Tr}_{L/K}(\alpha) + \mathrm{Tr}_{L/K}(\beta) \quad \forall \alpha,\beta \in L$,

(iii) $N_{L/K}(\alpha) = \alpha^{[L:K]} \quad \forall \alpha \in K$,

(iv) $\mathrm{Tr}_{L/K}(\alpha) = [L:K]\alpha \quad \forall \alpha \in K$,

(v) $N_{L/K}(\alpha\beta) = \alpha^{[L:K]} N_{L/K}(\beta) \quad \forall \alpha \in K \ \forall \beta \in L$,

(vi) $\mathrm{Tr}_{L/K}(\alpha\beta) = \alpha \mathrm{Tr}_{L/K}(\beta) \quad \forall \alpha \in K \ \forall \beta \in L$,

(vii) $N_{L/K} : (L^*, \cdot) \to (K^*, \cdot)$ is a group homomorphism,

(viii) $\mathrm{Tr}_{L/K} : (L, +) \to (K, +)$ is a group homomorphism,

(ix) $\mathrm{Tr}_{L/K} : L \to K$ is a K-linear map (of K-vector spaces)

(x) If $p_\alpha(x) = \det(X\,\mathrm{id}_L - \varphi_\alpha) = X^n - a_{n-1}X^{n-1} + - \cdots + (-1)^n a_0$ (with $n = [L:K]$) is the characteristic polynomial of φ_α then $a_{n-1} = \mathrm{Tr}_{L/K}(\alpha)$ and $a_0 = N_{L/K}(\alpha)$.

17.10.2022

Proof: (i) $N_{L/K}(\alpha\beta) = \det \varphi_{\alpha\beta} \overset{\text{Lemma 21(ii)}}{=} \det(\varphi_\alpha \circ \varphi_\beta) = (\det\varphi_\alpha)(\det\varphi_\beta) = N_{L/K}(\alpha) N_{L/K}(\beta)$,

(ii) $\mathrm{Tr}_{L/K}(\alpha+\beta) = \mathrm{tr}\,\varphi_{\alpha+\beta} \overset{\text{Lemma 21(iii)}}{=} \mathrm{tr}(\varphi_\alpha + \varphi_\beta) = \mathrm{tr}\,\varphi_\alpha + \mathrm{tr}\,\varphi_\beta = \mathrm{Tr}_{L/K}(\alpha) + \mathrm{Tr}_{L/K}(\beta)$,

(iii) $N_{L/K}(\alpha) = \det \varphi_\alpha = \begin{vmatrix} \alpha & & 0 \\ & \ddots & \\ 0 & & \alpha \end{vmatrix} = \alpha^{[L:K]}$,

(iv) $\mathrm{Tr}_{L/K}(\alpha) = \mathrm{tr}\,\varphi_\alpha = \mathrm{tr}\begin{pmatrix} \alpha & & 0 \\ & \ddots & \\ 0 & & \alpha \end{pmatrix} = [L:K]\alpha$,

(v) Follows from (i) and (iii)

(vi) Choose any basis of L as a K-vector space and let B be the $[L:K]\times[L:K]$-matrix with entries in K which is the matrix representing φ_β with regard to this basis. Then $\mathrm{Tr}_{L/K}(\beta) = \mathrm{tr}\,\varphi_\beta = \mathrm{tr}\,B$. Then the matrix αB represents $\varphi_{\alpha\beta}$ with regard to this basis and

$$\mathrm{Tr}_{L/K}(\alpha\beta) = \mathrm{tr}\,\varphi_{\alpha\beta} = \mathrm{tr}(\alpha B) = \alpha\,\mathrm{tr}\,B = \alpha\,\mathrm{Tr}_{L/K}(\beta).$$

(vii) Clearly $N_{L/K}(0) = 0$. If $\alpha \in L^*$ then $\varphi_\alpha \circ \varphi_{\alpha^{-1}} = \varphi_{\alpha^{-1}} \circ \varphi_\alpha = \mathrm{id}_L$ and therefore $N_{L/K}(\alpha) = \det\varphi_\alpha \neq 0$. The assertion follows from (i).

(viii) Follows from (ii).

(ix) Follows from (ii) and (vi)

(x) Follows from a result in linear algebra which says that $a_{n-1} = \mathrm{tr}\,\varphi_\alpha$ and $a_0 = \det\varphi_\alpha$.

Theorem 23 Let L/K be a finite separable field extension and let $\sigma_i : L \hookrightarrow \overline{K}$ (with $1 \le i \le [L:K]$) be the different embeddings of L in an algebraic closure $\overline{K}$ of K with $\sigma_i|_K = \mathrm{id}_K$.

(i) $p_\alpha(X) = \det(X \cdot \mathrm{id}_L - \varphi_\alpha) = \prod_{i=1}^{[L:K]} (X - \sigma_i(\alpha))$ is the characteristic polynomial of φ_α $\forall \alpha \in L$,

(ii) $N_{L|K}(\alpha) = \prod_{i=1}^{[L:K]} \sigma_i(\alpha)$ $\forall \alpha \in L$,

(iii) $\mathrm{Tr}_{L|K}(\alpha) = \sum_{i=1}^{[L:K]} \sigma_i(\alpha)$ $\forall \alpha \in L$.

Proof: (i) Let $m_{K,\alpha}(X) = X^d + c_1 X^{d-1} + \cdots + c_{d-1} X + c_d \in K[X]$ (where $d = [K(\alpha):K]$). Then $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is a basis of $K(\alpha)$ as a K-vector space. If $\{\beta_1, \ldots, \beta_{[L:K(\alpha)]}\}$ is a basis of L as a $K(\alpha)$-vector space then (by a theorem from algebra)
$B := \{\beta_i \alpha^j \mid 1 \le i \le [L:K(\alpha)],\ 0 \le j < [K(\alpha):K]\}$ is a basis of L as a K-vector space.
For $1 \le i \le [L:K(\alpha)]$ we have

$$\varphi_\alpha(\beta_i \alpha^j) = \begin{cases} \beta_i \alpha^{j+1} & \text{if } 0 \le j \le d-2, \\ \beta_i \alpha^d = \beta_i(-c_d - c_{d-1}\alpha - \cdots - c_1 \alpha^{d-1}) = -c_d \beta_i - c_{d-1}\beta_i \alpha - \cdots - c_1 \beta_1 \alpha^{d-1} & \text{if } j = d-1. \end{cases}$$

This can be stated as

$$\alpha \begin{pmatrix} \beta_i \\ \beta_i \alpha \\ \vdots \\ \beta_i \alpha^{d-2} \\ \beta_i \alpha^{d-1} \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -c_d & -c_{d-1} & -c_{d-2} & \cdots & -c_1 \end{pmatrix}}_{=:M} \cdot \begin{pmatrix} \beta_i \\ \beta_i \alpha \\ \vdots \\ \beta_i \alpha^{d-2} \\ \beta_i \alpha^{d-1} \end{pmatrix}$$

for $1 \le i \le [L:K(\alpha)]$ (i.e., the matrix M does not depend on i). This shows that the K-linear map $\varphi_\alpha : L \to L$ has matrix representation

$$\begin{pmatrix} M & & 0 \\ & M & \\ 0 & & M \end{pmatrix}$$

with respect to a (suitably ordered) basis B, in which M appears $[L:K(\alpha)]$ times. Using some facts from linear algebra we get

$$\det(X \cdot I_d - M) = \begin{vmatrix} X & -1 & 0 & \cdots & 0 & 0 \\ 0 & X & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & X & -1 \\ c_d & c_{d-1} & c_{d-2} & \cdots & c_2 & X + c_1 \end{vmatrix} = X^d + c_1 X^{d-1} + \cdots + c_{d-1} X + c_d = m_{K,\alpha}(X)$$

and therefore $\det(X\,id_L - \varphi_\alpha) = \left(\det(X\cdot I_d - M)\right)^{[L:K(\alpha)]} = \left(m_{K,\alpha}(X)\right)^{[L:K(\alpha)]}$. If $\alpha = \alpha_1, \alpha_2, \dots, \alpha_d$ are the roots of $m_{K,\alpha}$ then $m_{K,\alpha}(X) = \prod_{i=1}^{d}(X-\alpha_i)$. There are exactly d homomorphisms $\tau_i : K(\alpha) \hookrightarrow \bar{K}$ with $\tau_i|_K = id_K$ which are determined by $\tau_i(\alpha) = \alpha_i$ (for $1 \le i \le d = [K(\alpha):K]$) by Theorem 17. (In other words $m_{K,\alpha}(X) = \prod_{i=1}^{d}(X - \tau_i(\alpha))$.)

For each $i \in \{1, \dots, [K(\alpha):K]\}$ there are exactly $[L:K(\alpha)]$ homomorphisms $\sigma_{ij} : L \hookrightarrow \bar{K}$ with $\sigma_{ij}|_{K(\alpha)} = \tau_i$ (and therefore $\sigma_{ij}(\alpha) = \alpha_i$) for $1 \le j \le [L:K(\alpha)]$ by Theorem 20. This implies

$$\det(X\,id_L - \varphi_\alpha) = \left(m_{K,\alpha}(X)\right)^{[L:K(\alpha)]} = \prod_{i=1}^{d}(X-\tau_i(\alpha))^{[L:K(\alpha)]} = \prod_{i=1}^{[K:K(\alpha)]}\ \prod_{j=1}^{[L:K(\alpha)]}(X-\sigma_{ij}(\alpha))$$

which shows (i) as $\{\sigma_{ij} \mid 1 \le i \le [K(\alpha):K],\ 1 \le j \le [L:K(\alpha)]\}$ are exactly the homomorphisms $\sigma : L \hookrightarrow \bar{K}$ with $\sigma|_K = id_K$.

(ii) and (iii) Follow from (i) and Lemma 22 (x).

Corollary 24 Let L/K be a finite separable field extension and $\alpha \in L$. Let $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_d$ be the different roots of $m_{K,\alpha}$.

(i) $N_{L/K}(\alpha) = \left(\prod_{i=1}^{d}\alpha_i\right)^{[L:K(\alpha)]}$,

(ii) $Tr_{L/K}(\alpha) = [L:K(\alpha)]\sum_{i=1}^{d}\alpha_i$.

Proof: Keeping the notation from the proof of Theorem 23 we see

$$N_{L/K}(\alpha) = \left(\prod_{i=1}^{d}\tau_i(\alpha)\right)^{[L:K(\alpha)]} = \left(\prod_{i=1}^{d}\alpha_i\right)^{[L:K(\alpha)]} \quad \text{and}$$

$$Tr_{L/K}(\alpha) = [L:K(\alpha)]\sum_{i=1}^{d}\tau_i(\alpha) = [L:K(\alpha)]\sum_{i=1}^{d}\alpha_i.$$

Examples: 1) If $\alpha \in \mathbb{Q}(i)$ we have $N_{\mathbb{Q}(i)/\mathbb{Q}}(\alpha) = \alpha\bar{\alpha} = |\alpha|^2$ and $Tr_{\mathbb{Q}(i)/\mathbb{Q}}(\alpha) = \alpha + \bar{\alpha} = 2\,\mathrm{Re}(\alpha)$ $\left(\text{i.e., } N_{\mathbb{Q}(i)/\mathbb{Q}}(a+bi) = a^2+b^2 \text{ and } Tr_{\mathbb{Q}(i)/\mathbb{Q}}(a+bi) = 2a\right)$.

2) More generally, if $d \in \mathbb{Z}\setminus\{0,1\}$ is squarefree and $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ then

$N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(a+b\sqrt{d}) = (a+b\sqrt{d})(a-b\sqrt{d}) = a^2 - b^2 d$ and

$Tr_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(a+b\sqrt{d}) = (a+b\sqrt{d}) + (a-b\sqrt{d}) = 2a$.

(If $d < 0$ then $N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(\alpha) = |\alpha|^2$ and $Tr_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(\alpha) = 2\,\mathrm{Re}\,\alpha \quad \forall \alpha \in \mathbb{Q}(\sqrt{d})$.)

3) We have $N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(\sqrt{2}) = \sqrt{2}\cdot(-\sqrt{2}^1) = -2$ and $\mathrm{Tr}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(\sqrt{2}) = \sqrt{2} - \sqrt{2} = 0$.

However, if we consider $\sqrt{2}$ as an element of $\mathbb{Q}(\sqrt[4]{2})$ then $\sqrt{2} = (\sqrt[4]{2})^2$ and therefore

$\sigma_1(\sqrt{2}) = (\sqrt[4]{2})^2 = \sqrt{2}$, $\sigma_2(\sqrt{2}) = (-\sqrt[4]{2})^2 = \sqrt{2}$, $\sigma_3(\sqrt{2}) = (i\sqrt[4]{2})^2 = -\sqrt{2}$, $\sigma_4(\sqrt{2}) = (-i\sqrt[4]{2})^2 = -\sqrt{2}$

$\Rightarrow N_{\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}}(\sqrt{2}) = \sigma_1(\sqrt{2})\sigma_2(\sqrt{2})\sigma_3(\sqrt{2})\sigma_4(\sqrt{2}) = \sqrt{2}^2(-\sqrt{2})^2 = 4$ and

$\mathrm{Tr}_{\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}}(\sqrt{2}) = \sigma_1(\sqrt{2}) + \sigma_2(\sqrt{2}) + \sigma_3(\sqrt{2}) + \sigma_4(\sqrt{2}) = 2\sqrt{2} - 2\sqrt{2} = 0$

4) If L/K is an extension of algebraic number fields and $\alpha \in K$ then $N_{L/K}(\alpha) = \alpha^{[L:K]}$ and $\mathrm{Tr}_{L/K}(\alpha) = [L:K]\alpha$

Remarks: 1) Examples 3) and 4) show that $N_{L/K}(\alpha)$ and $\mathrm{Tr}_{L/K}(\alpha)$ do not only depend on α but also on L and K.

2) Despite its name the norm $N_{L/K}$ need not be positive definite (as one might expect erroneously). Compare, e.g., Example 3).

19.10.2022

Theorem 25 Let L/K be an algebraic field extension. Then the following are equivalent:

(i) Each irreducible polynomial $p \in K[X]$ which has a root in L splits in L. (I.e., p can be written as a product of linear factors.)

(ii) If $\overline{K}$ is an algebraic closure of K with the property $L \subseteq \overline{K}$ and $\varphi: L \hookrightarrow \overline{K}$ a homomorphism satisfying $\varphi|_K = \mathrm{id}_K$ then $\varphi(L) = L$ (i.e., φ is an automorphism of L).

Proof: (i) $\Rightarrow$ (ii) Let $\alpha \in L$. Then α is algebraic over K. By assumption $m_{K,\alpha} \in K[X]$ splits over L, i.e., $m_{K,\alpha}(X) = \prod_{i=1}^{n}(X - \alpha_i)$ with $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n \in L$. As $\varphi|_K = \mathrm{id}_K$ we see that $m_{K,\alpha}(X) = m^{\varphi}_{K,\alpha}(X) = \prod_{i=1}^{n}(X - \varphi(\alpha_i))$. As $L[X]$ is a unique factorization domain $\varphi(\alpha_1) = \varphi(\alpha), \varphi(\alpha_2), \dots, \varphi(\alpha_n)$ has to be a permutation of $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$. Therefore, there are $i, j \in \{1, \dots, n\}$: $\varphi(\alpha) = \varphi(\alpha_1) = \alpha_i$ and $\varphi(\alpha_j) = \alpha_1 = \alpha$, i.e., $\varphi(\alpha) \in L$ and $\alpha \in \varphi(L)$. As α was arbitrary this shows $\varphi(L) \subseteq L$ and $L \subseteq \varphi(L)$.

(ii) $\Rightarrow$ (i) Let $p \in K[X]$ be irreducible with root $\alpha \in L$. If $\beta \in \overline{K}$ is any root of p then there is an isomorphism $\varphi: K(\alpha) \to K(\beta)$ with the properties $\varphi|_K = \mathrm{id}_K$ and $\varphi(\alpha) = \beta$. We compose φ with an embedding $K(\beta) \hookrightarrow \overline{K}$ (i.e., $K(\alpha) \xrightarrow{\varphi} K(\beta) \hookrightarrow \overline{K}$) and extend this to an embedding $\tilde{\varphi}: L \hookrightarrow \overline{K}$. Then the assumption implies $\tilde{\varphi}(L) = L$ and therefore $\beta = \tilde{\varphi}(\alpha) = \varphi(\alpha) \in L$. As β was an arbitrary root of p we get that L contains all the roots of p and p splits over L.

Definition: An algebraic field extension L/K which satisfies one (and therefore both) of the conditions of Theorem 25 is called a normal field extension.

Theorem 26 Let L/K be a finite field extension. Then the following are equivalent:

(i) L/K is a normal field extension,

(ii) L is the splitting field of a polynomial $p \in K[X]$.

Proof: (i) $\Rightarrow$ (ii) There are $\alpha_1, \dots, \alpha_n \in L$, which are algebraic over K such that $L = K(\alpha_1, \dots, \alpha_n)$. (Let, e.g., $\{\alpha_1, \dots, \alpha_n\}$ be a basis of L as a K-vector space.) Then $m_{K,\alpha_i} \in K[X]$ has a root in L (namely α_i) and is irreducible over K (for $1 \le i \le n$). By assumption m_{K,α_i} splits over L (for $1 \le i \le n$). Therefore $p = m_{K,\alpha_1} \cdot \dots \cdot m_{K,\alpha_n}$ splits over L and is splitting field of p.

(ii) $\Rightarrow$ (i) Let $\alpha_1, \dots, \alpha_n \in L$ be the roots of $p \in K[X]$, i.e., $p(X) = c \prod_{i=1}^{n} (X - \alpha_i)$ with $c \in K$. Then $L = K(\alpha_1, \dots, \alpha_n)$. Let $\overline{K}$ be an algebraic closure of K with $L \subseteq \overline{K}$ and $\varphi : L \hookrightarrow \overline{K}$ a homomorphism satisfying $\varphi|_K = \mathrm{id}_K$. Then $p(X) = p^{\varphi}(X) = c \prod_{i=1}^{n} (X - \varphi(\alpha_i))$.

As $\overline{K}[X]$ is a unique factorization domain, $\varphi(\alpha_1), \dots, \varphi(\alpha_n)$ have to be a permutation of $\alpha_1, \dots, \alpha_n$ and $\varphi(\alpha_i) \in L$ for $1 \le i \le n$. This implies

$$\varphi(L) = \varphi(K(\alpha_1, \dots, \alpha_n)) = K(\varphi(\alpha_1), \dots, \varphi(\alpha_n)) = K(\alpha_1, \dots, \alpha_n) = L.$$

Examples: 1) $\mathbb{Q}(i)/\mathbb{Q}$ is a normal field extension as $\mathbb{Q}(i)$ is the splitting field of $X^2 + 1 \in \mathbb{Q}[X]$.

2) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is a normal field extension as $\mathbb{Q}(\sqrt{2})$ is the splitting field of $X^2 - 2 \in \mathbb{Q}[X]$.

3) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not a normal field extension. The polynomial $X^3 - 2 \in \mathbb{Q}[X]$ is irreducible and has the root $\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2})$ but does not split over $\mathbb{Q}(\sqrt[3]{2})$ (as its roots $\sqrt[3]{2}e^{2\pi i/3}, \sqrt[3]{2}e^{4\pi i/3} \in \mathbb{C} \setminus \mathbb{R}$ and $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$).

Theorem 27 Let L/K be a normal field extension and M an intermediate field. Then L/M is also a normal extension.

Proof: Let $\overline{K}$ be an algebraic closure of K with $L \subseteq \overline{K}$. Then $\overline{K}$ is also an algebraic closure of M. If $\varphi : L \hookrightarrow \overline{K}$ is a homomorphism with $\varphi|_M = \mathrm{id}_M$ then $\varphi|_K = \mathrm{id}_K$ and thus $\varphi(L) = L$.

Theorem 28 Let L/K be a finite separable field extension and M an intermediate field.

(i) $N_{L/K} = N_{M/K} \circ N_{L/M}$,

(ii) $\mathrm{Tr}_{L/K} = \mathrm{Tr}_{M/K} \circ \mathrm{Tr}_{L/M}$

Proof: There is a $\gamma \in L$ such that $L = K(\gamma)$. Let N be a splitting field of $m_{K,\gamma}$. By Theorem 26 N/K is a (finite) normal field extension. Let $\overline{K}$ be an algebraic closure of K with $N \subseteq \overline{K}$. Let $\sigma_i : M \hookrightarrow \overline{K}$ (with $1 \le i \le [M:K]$) be the different

homomorphisms with $\sigma_i|_K = id_K$ and let $\tau_j : L \hookrightarrow \overline{K}$ (with $1 \le j \le [L:M]$) be the different homomorphisms with $\tau_j|_M = id_M$. We extend all σ_i and τ_j to homomorphisms $N \hookrightarrow \overline{K}$ and use the same notations for these extensions. (This should not lead to any confusion.) As N/K is a normal extension the σ_i and the τ_j are all automorphisms of N (by Theorem 25). Then $\sigma_i \circ \tau_j : N \to N$ is also an automorphism and $\sigma_i \circ \tau_j : L \hookrightarrow \overline{K}$ is a homomorphism with the property $\sigma_i \circ \tau_j|_K = id_K$ (for $1 \le i \le [M:K]$, $1 \le j \le [L:M]$). These are pairwise different, i.e., $\sigma_i \circ \tau_j|_L \neq \sigma_k \circ \tau_\ell|_L$ if $(i,j) \neq (k,\ell)$. (If $\sigma_i \circ \tau_j|_L = \sigma_k \circ \tau_\ell|_L$ $\Rightarrow \sigma_i \circ \tau_j|_M = \sigma_k \circ \tau_\ell|_M \Rightarrow \sigma_i|_M = \sigma_k|_M \Rightarrow i = k \Rightarrow \sigma_i \circ \tau_j = \sigma_i \circ \tau_k$ $\Rightarrow \tau_j = \tau_\ell \Rightarrow \tau_j|_L = \tau_\ell|_L \Rightarrow j = \ell$.) I.e., we have found all $[L:M] \cdot [M:K] = [L:K]$ pairwise different homomorphisms $\sigma_i \circ \tau_j : L \hookrightarrow \overline{K}$ with the property $\sigma_i \circ \tau_j|_K = id_K$.

If $\alpha \in L$ then

$$N_{L|K}(\alpha) = \prod_{i=1}^{[M:K]} \prod_{j=1}^{[L:M]} (\sigma_i \circ \tau_j)(\alpha) = \prod_{i=1}^{[M:K]} \sigma_i \left(\prod_{j=1}^{[L:M]} \tau_j(\alpha) \right) = \prod_{i=1}^{[M:K]} \sigma_i \left(N_{L|M}(\alpha) \right) = N_{M|K}\left(N_{L|M}(\alpha) \right)$$

and

$$Tr_{L|K}(\alpha) = \sum_{i=1}^{[M:K]} \sum_{j=1}^{[L:M]} (\sigma_i \circ \tau_j)(\alpha) = \sum_{i=1}^{[M:K]} \sigma_i \left(\sum_{j=1}^{[L:M]} \tau_j(\alpha) \right) = \sum_{i=1}^{[M:K]} \sigma_i \left(Tr_{L|M}(\alpha) \right) = Tr_{M|K}\left(Tr_{L|M}(\alpha) \right)$$

Definition: Let L/K be a finite separable field extension, $[L:K] = n$ and $\sigma_i : L \hookrightarrow \overline{K}$ be the different homomorphisms with $\sigma_i|_K = id_K$ (for $1 \le i \le n$). If $\alpha_1, \dots, \alpha_n \in L$ the discriminant $\Delta_{L|K}(\alpha_1, \dots, \alpha_n)$ of $\alpha_1, \dots, \alpha_n$ is defined as

$$\Delta_{L|K}(\alpha_1, \dots, \alpha_n) := \left(\det \left((\sigma_i(\alpha_j))_{1 \le i,j \le n} \right) \right)^2 = \begin{vmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{vmatrix}^2.$$

Remark: The square in the definition ensures that the discriminant does not depend on the ordering of $\sigma_1, \dots, \sigma_n$ or $\alpha_1, \dots, \alpha_n$.

Theorem 29 Let L/K be a finite separable field extension, $[L:K] = n$ and $\alpha_1, \dots, \alpha_n \in L$. Then

$$\Delta_{L|K}(\alpha_1, \dots, \alpha_n) = \det \left(\left(Tr_{L|K}(\alpha_i \alpha_j) \right)_{1 \le i,j \le n} \right).$$

Proof:

$$\Delta_{L|K}(\alpha_1,\dots,\alpha_n) = \begin{vmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{vmatrix}^2$$

$$= \begin{vmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \cdots & \sigma_n(\alpha_2) \\ \vdots & \vdots & & \vdots \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{vmatrix} \cdot \begin{vmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & & \sigma_2(\alpha_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{vmatrix}$$

$$= \det\left(\begin{pmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \cdots & \sigma_n(\alpha_2) \\ \vdots & \vdots & & \vdots \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{pmatrix} \cdot \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{pmatrix} \right)$$

$$= \begin{vmatrix} \mathrm{Tr}_{L|K}(\alpha_1^2) & \mathrm{Tr}_{L|K}(\alpha_1\alpha_2) & \cdots & \mathrm{Tr}_{L|K}(\alpha_1\alpha_n) \\ \mathrm{Tr}_{L|K}(\alpha_1\alpha_2) & \mathrm{Tr}_{L|K}(\alpha_2^2) & \cdots & \mathrm{Tr}_{L|K}(\alpha_2\alpha_n) \\ \vdots & \vdots & & \vdots \\ \mathrm{Tr}_{L|K}(\alpha_1\alpha_n) & \mathrm{Tr}_{L|K}(\alpha_2\alpha_n) & \cdots & \mathrm{Tr}_{L|K}(\alpha_n^2) \end{vmatrix}$$

24.10.2022

Corollary 30 Let $L|K$ be a finite separable field extension and $[L:K]=n$.
Then $\Delta_{L|K}(\alpha_1,\dots,\alpha_n) \in K$ for all $\alpha_1,\dots,\alpha_n \in L$.

Proof: Follows from Theorem 29 and $\mathrm{Tr}_{L|K}(\alpha_i\alpha_j) \in K$ for $1 \le i,j \le n$.

Lemma 31 Let $L|K$ be a finite separable field extension, $[L:K]=n$ and $\alpha_1,\dots,\alpha_n \in L$.
Furthermore, let $\lambda_{jk} \in K$ (for $1 \le j,k \le n$) and $\beta_k = \sum_{j=1}^{n} \lambda_{jk}\alpha_j$ (for $1 \le k \le n$).
If A denotes the matrix $(\lambda_{jk})_{1 \le j,k \le n}$ then $\Delta_{L|K}(\beta_1,\dots,\beta_n) = (\det A)^2 \Delta_{L|K}(\alpha_1,\dots,\alpha_n)$.

Proof: Let $\sigma_i : L \hookrightarrow \overline{K}$ denote the different homomorphisms with $\sigma_i|_K = \mathrm{id}_K$ $(1 \le i \le n)$.
Then $\sigma_i(\beta_k) = \sum_{j=1}^{n} \lambda_{jk}\sigma_i(\alpha_j) = \sum_{j=1}^{n} \sigma_i(\alpha_j)\lambda_{jk}$ (with $1 \le i,k \le n$). Rewriting this as a matrix gives

$$\begin{pmatrix} \sigma_1(\beta_1) & \sigma_1(\beta_2) & \cdots & \sigma_1(\beta_n) \\ \sigma_2(\beta_1) & \sigma_2(\beta_2) & \cdots & \sigma_2(\beta_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\beta_1) & \sigma_n(\beta_2) & \cdots & \sigma_n(\beta_n) \end{pmatrix} = \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{pmatrix} \cdot \begin{pmatrix} \lambda_{11} & \lambda_{12} & \cdots & \lambda_{1n} \\ \lambda_{21} & \lambda_{22} & \cdots & \lambda_{2n} \\ \vdots & \vdots & & \vdots \\ \lambda_{n1} & \lambda_{n2} & \cdots & \lambda_{nn} \end{pmatrix}$$

and therefore

$$\Delta_{L|K}(\beta_1,\dots,\beta_n) = \begin{vmatrix} \sigma_1(\beta_1) & \sigma_1(\beta_2) & \dots & \sigma_1(\beta_n) \\ \sigma_2(\beta_1) & \sigma_2(\beta_2) & \dots & \sigma_2(\beta_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\beta_1) & \sigma_n(\beta_2) & \dots & \sigma_n(\beta_n) \end{vmatrix}^2 = \begin{vmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \dots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \dots & \sigma_2(\alpha_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \dots & \sigma_n(\alpha_n) \end{vmatrix}^2 \cdot \begin{vmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2n} \\ \vdots & \vdots & & \vdots \\ x_{n1} & x_{n2} & \dots & x_{nn} \end{vmatrix}^2$$

$$= \Delta_{L|K}(\alpha_1,\dots,\alpha_n)\cdot(\det A)^2$$

Theorem 32 Let $L|K$ be a finite separable field extension with $L=K(\alpha)$, $[L:K]=n$ and $\alpha_1=\alpha,\alpha_2,\dots,\alpha_n$ the different roots of $m_{K,\alpha}$. Then $\Delta_{L|K}(1,\alpha,\dots,\alpha^{n-1}) = \prod_{1\le i<j\le n}(\alpha_i-\alpha_j)^2$.

Proof: If $\sigma_i: L\hookrightarrow\bar{K}$ are the different homomorphisms with $\sigma_i|_K = id_K$ (for $1\le i\le n$) then we can assume w.l.o.g. $\sigma_i(\alpha)=\alpha_i$ (for $1\le i\le n$). Using Vandermonde's determinant we get

$$\Delta_{L|K}(1,\alpha,\dots,\alpha^{n-1}) = \begin{vmatrix} \sigma_1(1) & \sigma_1(\alpha) & \dots & \sigma_1(\alpha^{n-1}) \\ \sigma_2(1) & \sigma_2(\alpha) & \dots & \sigma_2(\alpha^{n-1}) \\ \vdots & \vdots & & \vdots \\ \sigma_n(1) & \sigma_n(\alpha) & \dots & \sigma_n(\alpha^{n-1}) \end{vmatrix}^2 = \begin{vmatrix} 1 & \alpha_1 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \dots & \alpha_2^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \dots & \alpha_n^{n-1} \end{vmatrix}^2 = \prod_{1\le i<j\le n}(\alpha_i-\alpha_j)^2$$

Theorem 33 Let $L|K$ be a finite separable field extension, $[L:K]=n$ and $\alpha_1,\dots,\alpha_n\in L$. Then the following are equivalent:

(i) $\alpha_1,\dots,\alpha_n$ are linearly dependent over K,

(ii) $\Delta_{L|K}(\alpha_1,\dots,\alpha_n)=0$.

Proof: (i) $\Rightarrow$ (ii) Let $\sigma_i: L\hookrightarrow\bar{K}$ be the different homomorphisms with $\sigma_i|_K=id_K$ (for $1\le i\le n$). By assumption there are $\lambda_1,\dots,\lambda_n\in K$ (not all $=0$) such that $\sum_{j=1}^n\lambda_j\alpha_j=0$. Therefore

$$0=\sigma_i\Big(\sum_{j=1}^n\lambda_j\alpha_j\Big)=\sum_{j=1}^n\lambda_j\sigma_i(\alpha_j) \quad\text{and thus}\quad \sum_{j=1}^n\lambda_j(\sigma_1(\alpha_j),\dots,\sigma_n(\alpha_j))=(0,\dots,0).$$

I.e., the columns of the matrix $(\sigma_i(\alpha_j))_{1\le i,j\le n}$ are linearly dependent. This implies $\Delta_{L|K}(\alpha_1,\dots,\alpha_n)=0$ by definition of $\Delta_{L|K}$.

(ii) $\Rightarrow$ (i) Let $\alpha_1,\dots,\alpha_n\in L$ be linearly independent over K. By the primitive element theorem there is a $\gamma\in L$ such that $L=K(\gamma)$ and $\{1,\gamma,\dots,\gamma^{n-1}\}$ is a K-basis of L. Therefore, there are $\lambda_{jk}\in K$ (with $1\le j,k\le n$) such that $\alpha_k=\sum_{j=1}^n\lambda_{jk}\gamma^{j-1}$ for $1\le k\le n$. Let A denote the matrix $A=(\lambda_{jk})_{1\le j,k\le n}$. As $\{\alpha_1,\dots,\alpha_n\}$ and $\{1,\gamma,\dots,\gamma^{n-1}\}$ are both K-bases of L, the matrix A is invertible and $\det A\neq 0$. If $\gamma_1=\gamma,\gamma_2,\dots,\gamma_n$ denote the different roots of $m_{K,\gamma}$ then

$$\Delta_{L|K}(\alpha_1,\dots,\alpha_n) \overset{\text{Lemma 31}}{=} (\det A)^2\cdot\Delta_{L|K}(1,\gamma,\dots,\gamma^{n-1}) \overset{\text{Theorem 32}}{=} \underbrace{(\det A)^2}_{\neq 0}\cdot\prod_{1\le i<j\le n}\underbrace{(\gamma_i-\gamma_j)^2}_{\neq 0}\neq 0$$

Remark: In fact we have shown the following: If L/K is a finite separable field extension with $[L:K]=n$ and $\alpha_1,\dots,\alpha_n \in L$, the following are equivalent:

(i) $\alpha_1,\dots,\alpha_n$ is a K-basis of L,

(ii) $\alpha_1,\dots,\alpha_n$ are linearly independent over K,

(iii) $\Delta_{L/K}(\alpha_1,\dots,\alpha_n) \in K\setminus\{0\}$.

Theorem 34 Let L/K be a finite separable field extension with $L=K(\alpha)$ and $[L:K]=n$. Then $\Delta_{L/K}(1,\alpha,\dots,\alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{L/K}\left(m'_{K,\alpha}(\alpha)\right)$.

Proof: Let $\alpha_1=\alpha,\alpha_2,\dots,\alpha_n$ be the different roots of $m_{K,\alpha}$ and $\sigma_i: L \hookrightarrow \bar{K}$ the different homomorphisms with $\sigma_i|_K = \mathrm{id}_K$, where we assume $\sigma_i(\alpha)=\alpha_i$ (for $1\le i\le n$). Then

$$m_{K,\alpha}(X)=\prod_{i=1}^{n}(X-\alpha_i) \Rightarrow m'_{K,\alpha}(X)=\sum_{k=1}^{n}\prod_{\substack{1\le i\le n\\ i\neq k}}(X-\alpha_i) \Rightarrow m'_{K,\alpha}(\alpha_j)=\prod_{\substack{1\le i\le n\\ i\neq j}}(\alpha_j-\alpha_i)$$

$$\Rightarrow N_{L/K}\left(m'_{K,\alpha}(\alpha)\right)=\prod_{j=1}^{n}\sigma_j\left(m'_{K,\alpha}(\alpha)\right)=\prod_{j=1}^{n}m'_{K,\alpha}(\sigma_j(\alpha))=\prod_{j=1}^{n}m'_{K,\alpha}(\alpha_j)$$

$$=\prod_{j=1}^{n}\prod_{\substack{1\le i\le n\\ i\neq j}}(\alpha_j-\alpha_i)=\prod_{\substack{1\le i,j\le n\\ i\neq j}}(\alpha_j-\alpha_i)=\prod_{1\le i<j\le n}(\alpha_j-\alpha_i)(\alpha_i-\alpha_j)$$

$$=(-1)^{\binom{n}{2}}\prod_{1\le i<j\le n}(\alpha_i-\alpha_j)^2=(-1)^{\frac{n(n-1)}{2}}\prod_{1\le i<j\le n}(\alpha_i-\alpha_j)^2$$

$$\overset{\text{Theorem 32}}{=}(-1)^{\frac{n(n-1)}{2}}\Delta_{L/K}(1,\alpha_1,\dots,\alpha^{n-1})$$

Corollary 35 Let $K=\mathbb{Q}(\alpha)$ be an algebraic number field with $[K:\mathbb{Q}]=n$ and the property that the roots of $m_{\mathbb{Q},\alpha}$ are all in $\mathbb{R}$. Then $\Delta_{K/\mathbb{Q}}(\beta_1,\dots,\beta_n)>0$ for all $\mathbb{Q}$-bases $\beta_1,\dots,\beta_n$ of K.

Proof: Let $\alpha_1=\alpha,\alpha_2,\dots,\alpha_n \in \mathbb{R}$ be the roots of $m_{\mathbb{Q},\alpha}$. We know that $1,\alpha_1,\dots,\alpha^{n-1}$ is a $\mathbb{Q}$-basis of K and by Theorem 32 $\Delta_{K/\mathbb{Q}}(1,\alpha_1,\dots,\alpha^{n-1})=\prod_{1\le i<j\le n}(\alpha_i-\alpha_j)^2>0$.

If $\beta_1,\dots,\beta_n$ is a $\mathbb{Q}$-basis of K there are $\lambda_{jk}\in\mathbb{Q}$ (where $1\le j,k\le n$) such that $\beta_k=\sum_{j=1}^{n}\lambda_{jk}\alpha^{j-1}$ for $1\le k\le n$. Let $A=(\lambda_{jk})_{1\le j,k\le n}$. Then $\det A\in\mathbb{Q}\setminus\{0\}$ and Lemma 31 implies $\Delta_{K/\mathbb{Q}}(\beta_1,\dots,\beta_n)=\underbrace{(\det A)^2}_{>0}\cdot\underbrace{\Delta_{K/\mathbb{Q}}(1,\alpha_1,\dots,\alpha^{n-1})}_{>0}>0$.

Examples: 1) Let $K = \mathbb{Q}(i)$. Then $\{1, i\}$ is a $\mathbb{Q}$-basis of K and

$\Delta_{K/\mathbb{Q}}(1,i) = \begin{vmatrix} 1 & i \\ 1 & -i \end{vmatrix}^2 = (-2i)^2 = -4$. We can also employ Theorem 34 to calculate

$\Delta_{K/\mathbb{Q}}(1,i)$: $m_{\mathbb{Q},i}(X) = X^2+1 \Rightarrow m'_{\mathbb{Q},i}(X) = 2X \Rightarrow m'_{\mathbb{Q},i}(i) = 2i$

$\Rightarrow \Delta_{K/\mathbb{Q}}(1,i) = (-1)\, N_{K/\mathbb{Q}}(2i) = -(2i)(-2i) = -4.$

2) Let $K = \mathbb{Q}(i)$. Then $\{2, 1+i\}$ is also a $\mathbb{Q}$-basis of K and

$\Delta_{K/\mathbb{Q}}(2,1+i) = \begin{vmatrix} 2 & 1+i \\ 2 & 1-i \end{vmatrix}^2 = (-4i)^2 = -16$. We have $\begin{pmatrix} 2 \\ 1+i \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ i \end{pmatrix}$ and

using Lemma 31 we get $\Delta_{K/\mathbb{Q}}(2,1+i) = \begin{vmatrix} 2 & 0 \\ 1 & 1 \end{vmatrix}^2 \cdot \Delta_{K/\mathbb{Q}}(1,i) = 4\cdot(-4) = -16$

3) More generally, let $K = \mathbb{Q}(\sqrt{d})$ (with $d \in \mathbb{Z}\setminus\{0,1\}$ squarefree). Then $\{1, \sqrt{d}\}$ is a

$\mathbb{Q}$-basis of K and $\Delta_{K/\mathbb{Q}}(1,\sqrt{d}) = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = (-2\sqrt{d})^2 = 4d$. On using Theorem 34

$m_{\mathbb{Q},\sqrt{d}}(X) = X^2 - d \Rightarrow m'_{\mathbb{Q},\sqrt{d}}(X) = 2X \Rightarrow m'_{\mathbb{Q},\sqrt{d}}(\sqrt{d}) = 2\sqrt{d}$

$\Rightarrow \Delta_{K/\mathbb{Q}}(1,\sqrt{d}) = -N_{K/\mathbb{Q}}(2\sqrt{d}) = -(2\sqrt{d})(-2\sqrt{d}) = 4d$

4) Let $K = \mathbb{Q}(\sqrt[3]{2})$. Then $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ is a $\mathbb{Q}$-basis of K and (setting

$\zeta = e^{2\pi i/3} = \frac{1}{2}(-1+i\sqrt{3})$) we have

$$\Delta_{K/\mathbb{Q}}(1, \sqrt[3]{2}, \sqrt[3]{4}) = \begin{vmatrix} 1 & \sqrt[3]{2} & \sqrt[3]{4} \\ 1 & \sqrt[3]{2}\,\zeta & \sqrt[3]{4}\,\zeta^2 \\ 1 & \sqrt[3]{2}\,\zeta^2 & \sqrt[3]{4}\,\zeta \end{vmatrix}^2 = (2\zeta^2 + 2\zeta^2 + 2\zeta^2 - 2\zeta - 2\zeta - 2\zeta)^2 = (6\zeta^2 - 6\zeta)^2$$

$$= 36(\zeta^2-\zeta)^2 = 36\cdot\frac{1}{4}\left(-1-\sqrt{3}i-(-1+\sqrt{3}i)\right)^2 = 36(-\sqrt{3}i)^2 = -3\cdot 36 = -108$$

Again, we could also use Theorem 34:

$m_{\mathbb{Q},\sqrt[3]{2}}(X) = X^3 - 2 \Rightarrow m'_{\mathbb{Q},\sqrt[3]{2}}(X) = 3X^2 \Rightarrow m'_{\mathbb{Q},\sqrt[3]{2}}(\sqrt[3]{2}) = 3\sqrt[3]{4}$

$\Rightarrow \Delta_{K/\mathbb{Q}}(1, \sqrt[3]{2}, \sqrt[3]{4}) = (-1)^3 N_{K/\mathbb{Q}}(3\cdot\sqrt[3]{4}) = -(3\sqrt[3]{4})(3\cdot\sqrt[3]{4}\,\zeta^2)(3\cdot\sqrt[3]{4}\,\zeta)$

$$= -3^3\cdot 4 = -108$$

Remark: As can be seen from the third example it is often faster and easier to calculate a discriminant with the aid of Theorem 34.

31.10.2022