# Algebra I

## Musterlösung 24

### Radikalerweiterungen

**142.** Zeige: Die Nullstellen des Polynoms $X^5 - 6X + 3 \in \mathbb{Q}[X]$ sind nicht durch Radikale ausdrückbar.

*Lösung:* Das Polynom ist irreduzibel nach dem Kriterium von Eisenstein-Schönemann mit der Primzahl $3$. Ausserdem können wir mit Methoden der Analysis feststellen, dass es genau zwei nicht-reelle Nullstellen hat. Nach einem Satz aus der Vorlesung ist seine Galoisgruppe somit isomorph zu $S_5$. Da $S_5$ nach Aufgabe 134 nicht auflösbar ist, folgt mit einem weiteren Satz der Vorlesung, dass keine Nullstelle des Polynoms durch Radikale auflösbar ist.

Sei $d$ eine positive natürliche Zahl. Sei $\mu_d$ die Menge der primitiven $d$-ten Einheitswurzeln in $\mathbb{C}$. Definiere das $d$-te Kreisteilungspolynom als

$$\Phi_d := \prod_{\xi \in \mu_d} (X - \xi).$$

**143.** *(Irreduzibilität des Kreisteilungspolynoms)* Sei $n$ eine positive ganze Zahl und sei $f \in \mathbb{Z}[X]$ ein normierter irreduzibler Faktor von $X^n - 1$ mit Nullstelle $\xi \in \mathbb{C}$.

(a) Zeige: Für jede natürliche Zahl $k$ existiert ein eindeutiges Polynom $g_k \in \mathbb{Z}[X]$ mit $\deg(g_k) < \deg(f)$ und $f(\xi^k) = g_k(\xi)$.
Zeige ausserdem, dass die Menge $\{g_k : k \in \mathbb{Z}_{\geq 0}\}$ endlich ist.

(b) Sei $a := \sup\{|u| : u \text{ ist Koeffizient eines } g_k\}$. Zeige: Ist $k = p$ prim, so teilt $p$ alle Koeffizienten von $g_p$. Schliesse daraus, dass für alle $p > a$ das Polynom $g_p$ gleich Null ist. [*Hinweis:* $f(\xi^p) = f(\xi^p) - f(\xi)^p$]

(c) Folgere: Wenn alle Primfaktoren einer ganzen Zahl $m$ grösser als $a$ sind, dann gilt $f(\xi^m) = 0$.

(d) Zeige: Für jede zu $n$ teilerfremde ganze Zahl $r$ gilt $f(\xi^r) = 0$. [*Hinweis:* Betrachte $m := r + n \prod_{p \leq a, p \nmid r} p$]

(e) Sei $\Phi_n$ das $n$-te Kreispolynom, das heisst das normierte Polynom, das genau die primitiven $n$-ten Einheitswurzeln als einfache Nullstellen hat.
Zeige:

$$\prod_{0 < d,\, d \mid n} \Phi_d(X) = X^n - 1$$

und folgere, dass für alle $n$ das Polynom $\Phi_n$ ganzzahlige Koeffizienten hat.

(f) Zeige, dass das $n$-te Kreisteilungspolynom $\Phi_n$ irreduzibel ist.

*Lösung:* Note that any factor of $X^n - 1$ in $\mathbb{Z}[X]$ is monic up to sign, and by Gauss' Lemma it is irreducible in $\mathbb{Z}[X]$ if and only if it is irreducible in $\mathbb{Q}[X]$.

(a) Since $f$ is monic and irreducible, it is the minimal polynomial of $\xi$ over $\mathbb{Q}$. Consequently $\mathbb{Q}(\xi) \cong \mathbb{Q}[X]/(f(X))$ is an algebraic extension of $\mathbb{Q}$ of degree $\deg(f)$ with the

basis $1, \xi, \ldots, \xi^{\deg(f)-1}$ over $\mathbb{Q}$. Thus $f(\xi^k) \in \mathbb{Q}(\xi)$ can be expressed in at most one way as $f(\xi^k) = g_k(\xi)$ with $g_k \in \mathbb{Z}[X]$ of degree $< \deg(f)$, and we only have to check existence. Let $g_k$ be the remainder of $f(X^k)$ divided by $f$, then $g_k$ satisfies the desired properties.

Since the set $\{\xi^k : k \in \mathbb{Z}_{\geq 0}\}$ is finite, by uniqueness, so is the set of the $g_k$'s.

(b) Since exponentiation by $p$ is a ring homomorphism modulo $p$ (the Frobenius of degree $p$), we have $f(X^p) \equiv f(X)^p$ modulo $p\mathbb{Z}[X]$. In other words there exists a polynomial $h(X) \in \mathbb{Z}[X]$ with $f(X^p) = f(X)^p + ph(X)$. By the same argument as in (a) there exists a unique polynomial $g_h \in \mathbb{Z}[X]$ of degree less than $\deg(f)$ with $h(\xi) = g_h(\xi)$. Since $f(\xi) = 0$, it follows that

$$g_k(\xi) = f(\xi^p) = ph(\xi) = pg_h(\xi).$$

By the uniqueness of $g_p$ we conclude that $g_p = pg_h \in p\mathbb{Z}[X]$.

If $p > a$, all coefficients of $g_p$ have absolute value less than $p$ and are divisible by $p$; hence they are zero; thus $g_p = 0$.

(c) For every prime $p > a$ we have $f(\xi^p) = g_p(\xi) = 0$ by (b). Thus $\xi^p$ is another root of $f$. As $f$ is irreducible, we therefore have $\xi^p = \gamma(\xi)$ for some $\gamma \in \mathrm{Gal}(\mathbb{Q}(\mu_n) : \mathbb{Q})$. For every $k$ it follows that

$$f(\xi^{pk}) = f(\gamma(\xi)^k) = \gamma(f(\xi^k)) = \gamma(g_k(\xi)) = g_k(\gamma(\xi)) = g_k(\xi^k).$$

Thus the assertions of (a) and (b) are equally true for $\xi^p$ in place of $\xi$.

Now we can prove (c) in general by induction on the number of prime factors of $m$. If this number is $\leq 1$, we are already done. Otherwise write $m = pm'$ with a prime $p$. Then by the above we have $f(\xi^p) = 0$, and applying the induction hypothesis with $(m', \xi^p)$ in place of $(m, \xi)$ we deduce that $f(\xi^{pm'}) = 0$, as desired.

(d) Set $m := r + n\ell$ with $\ell := \prod_{p \leq a, p \nmid r} p$. Then any prime $p \leq a$ not dividing $r$ divides $\ell$; hence it does not divide $m$. Any prime $p \leq a$ dividing $r$ does not divide $n$ by assumption; so it also does not divide $n\ell$; hence it does not divide $m$. Together this shows that all prime divisors of $m$ are greater than $a$. Since $\xi^n = 1$, from (c) we therefore deduce that $f(\xi^r) = f(\xi^m) = 0$.

(e) Let $\gamma_n = \prod_{0<d|n} \Phi_d$. Since a complex number belongs to $\mu_k$ if and only if it has multiplicative order $k$, all the $\mu_k$'s are disjoint. Then $\gamma_n$ has distinct roots, and its set of roots is $\cup_{0<d|n} \mu_d$. On the other hand, the roots of $X^n - 1$ are also all distinct: they are indeed the $n$ distinct complex numbers $\exp(2\pi ik/n)$ for $a = 0, \ldots, n-1$. It is then easy to see that the two polynomials have indeed the same roots, since a $n$-th root of unity has order $d$ dividing $n$, and primitive $d$-th roots of unity are $n$-th roots of unity for $d|n$. As both $\gamma_n$ and $\Phi_n$ are monic, unique factorization in $\mathbb{Q}[X]$ gives $\gamma_n = \Phi_n$ as desired.

We then prove that the coefficients of the $\Phi_n$ are integer by induction on $n$. For $n = 1$ we have $\Phi_n = X - 1 \in \mathbb{Z}[X]$. For $n > 1$, suppose that $\Phi_k \in \mathbb{Z}[X]$ for all $k < n$. Then

$$\Phi_n = \frac{X^n - 1}{\prod_{\substack{0<d|n \\ d \neq n}} \Phi_d(X)},$$

and since the denominator lies in $\mathbb{Z}[X]$ by inductive hypothesis, we can conclude that $\Phi_n \in \mathbb{Z}[X]$. Indeed, $\Phi_n$ needs necessarily to lie in $\mathbb{Q}[X]$ (else, for $l$ the minimal degree of a coefficient of $\Phi_n$ not lying in $\mathbb{Q}$ and $m$ the minimal degree of a non-zero coefficients of the denominator, one would get that the coefficient of degree $l + m$ in $X^n - 1$ would not lie in $\mathbb{Q}$, contradiction). We can then write the monic polynomial $\Phi_n$ as $\frac{1}{\mu}\Theta_n$ for some primitive polynomial $\Theta_n \in \mathbb{Z}[X]$, but then Gauss's Lemma tells us that $X^n - 1$ equals $\frac{1}{d}$ times a primitive polynomial, and the only possibility is $d = \pm 1$, which implies that $\Phi_n \in \mathbb{Z}[X]$.

(f) Let $\xi \in \mathbb{C}$ be a root of unity of precise order $n$. Then the numbers $\xi^r$ for $r \in (\mathbb{Z}/n\mathbb{Z})^*$ are all distinct. Let $f(X) \in \mathbb{Z}[X]$ be the monic irreducible factor of $X^n - 1$ with $f(\xi) = 0$. Then (d) implies that

$$\Phi_n(X) := \prod_{r \in (\mathbb{Z}/n\mathbb{Z})^*} (X - \xi^r)$$

divides $f(X)$. We already know that $\Phi_n$ lies in $\mathbb{Q}[X]$. Since $f$ is irreducible in $\mathbb{Q}[X]$ and both polynomials are monic, it follows that $\Phi_n = f$. Thus $\Phi_n$ is irreducible.

**144.** Ziel dieser Aufgabe ist zu zeigen, dass für primitive $n$-te Einheitswurzeln $\xi$ gilt

$$\mathrm{Gal}(\mathbb{Q}(\xi) : \mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*.$$

Insbesondere erhalten wir $|\mathrm{Gal}(\mathbb{Q}(\xi) : \mathbb{Q})| = \varphi(n)$. Im Folgenden sei $n \geq 2$ eine natürliche Zahl und $\xi \in \mathbb{C}$ eine primitive $n$-te Einheitswurzel. Sei $G$ die Galoisgruppe von $X^n - 1$ über $\mathbb{Q}$.

(a) Zeige: $G \leq (\mathbb{Z}/n\mathbb{Z})^*$. Insbesondere ist $G$ abelsch.

(b) Bestimme $\Phi_d$ für $d = 1, 2, 3, 4, 8$.

(c) Zeige: $G \cong (\mathbb{Z}/n\mathbb{Z})^*$.

*Lösung:* (a) Wie in der Lösung der Aufgabe 132 ist $G \to \mathrm{Aut}(\langle\xi\rangle), \sigma \mapsto \sigma|_{\langle\xi\rangle}$ ein wohldefinierter, injektiver Gruppenhomomorphismus. Mit $\langle\xi\rangle \cong C_n$ folgt $\mathrm{Aut}(\langle\xi\rangle) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

(b) Klarerweise gilt $\Phi_1 = X - 1$.

Die einzige primitive zweite Einheitswurzel ist $-1$, also ist $\Phi_2 = X + 1$.

Die primitiven vierten Einheitswurzeln sind $i$ und $-i$, also ist $\Phi_4 = X^2 + 1$.

Wir wissen mit Aufgabe 142, dass $\Phi_8$ ein irreduzibler Teiler von $X^8 - 1$ sein muss. Es gilt $X^8 - 1 = (X^4 - 1)(X^4 + 1)$. Nur das zweite Polynom in dieser Zerlegung ist irreduzibel und hat Grad $\varphi(8)$. Nach Teil (c) ist $\deg(\Phi_8) = |G| = \varphi(8) = 4$, es folgt $\Phi_8 = X^4 + 1$.

(c) Die Gruppe $\mu_n$ hat nach der Aufgabe 95 genau $\varphi(n)$ Erzeuger. Sie alle haben nach Aufgabe 143 dasselbe Minimalpolynom $\Phi_n$ über $\mathbb{Z}$. Nach Aufgabe 112 existiert für jede Nullstelle von $\Phi_n$ ein $\sigma \in G$, das $\xi$ auf diese Nullstelle abbildet. Somit hat $G$ mindestens $\varphi(n)$ Elemente und ist daher isomorph zu $G \cong (\mathbb{Z}/n\mathbb{Z})^*$.

**145.** Sei $n$ eine positive ganze Zahl und sei $\xi \in \mu_n$.

(a) Zeige: Für jeden Zwischenkörper $K$ der Erweiterung $\mathbb{Q}(\xi) : \mathbb{Q}$ ist die Erweiterung $K : \mathbb{Q}$ normal und hat abelsche Galoisgruppe.

(b) Folgere: Falls $\varphi(n)$ eine Zweierpotenz ist, so ist das regelmässige $n$-Eck konstruierbar (dies vervollständigt den Beweis von Satz 21.6 der Vorlesung).

*Lösung:* (a) Nach der vorigen Aufgabe ist $\mathrm{Gal}(\mathbb{Q}(\xi) : \mathbb{Q})$ abelsch. Also ist jede ihrer Untergruppen ein Normalteiler. Mit einem Korollar des Hauptsatzes der Galoistheorie folgt die Aussage.

(b) Sei $\alpha = \frac{2\pi}{n}$. Wir wissen, dass das regelmässige $n$-Eck genau dann konstruierbar ist, wenn $\cos(\alpha)$ eine konstruierbare Zahl ist. Wegen $\cos(\alpha) = \frac{e^{i\alpha} + \frac{1}{e^{i\alpha}}}{2}$ ist $\cos(\alpha) \in \mathbb{Q}(e^{i\alpha})$. Wegen der vorigen Aufgabe ist die Gruppe $\mathrm{Gal}(\mathbb{Q}(e^{i\alpha}) : \mathbb{Q})$ abelsch und ihr Grad eine Zweierpotenz. Nach Teil (a) ist $\mathbb{Q}(\cos(\alpha)) : \mathbb{Q}$ eine normale Erweiterung, und mit der Multiplikativität des Körpergrades ist auch ihr Grad eine Zweierpotenz. Nach einem Satz der Vorlesung ist $\mathbb{Q}(\cos(\alpha))$ somit ein konstruierbarer Körper.