WS 05/06
Priv.-Doz. Dr. S. Wewers
Andreas Martin

Algebra I

11. Übungsblatt

Die Punkte dieses Übungsblattes sind Bonuspunkte!

Aufgabe 1: (1+1+1=3 P) Sei wie üblich $\zeta_n := \exp(2\pi i/n) \in \mathbb{C}$. Zeigen Sie:

(a) Sind n, m teilerfremd, so gilt

$$\mathbb{Q}[\zeta_{nm}] = \mathbb{Q}[\zeta_n, \zeta_m]$$

(als Unterkörper von $\mathbb{C}$).

(b) Sind n, m teilerfremd, und sind sowohl das reguläre n- als auch das reguläre m-Eck konstruierbar, so ist auch das reguläre nm-Eck konstruierbar. (Geometrische Argumente sind genauso erlaubt wie körpertheoretische.)

(c) Die Aussagen in (a) und (b) sind i.A. falsch ohne die Annahme, dass n und m teilerfremd sind.

Lösung:

(a) Wegen $\zeta_{nm}^n = \zeta_m$ und $\zeta_{nm}^m = \zeta_n$ folgt unmittelbar

$$\mathbb{Q}[\zeta_{nm}] \supseteq \mathbb{Q}[\zeta_n, \zeta_m] .$$

Andererseits sind n und m teilerfremd, also gibt es $a, b \in \mathbb{Z}$ so, daß

$$an + bm = 1 .$$

Dann folgt

$$\zeta_{nm} = \zeta_{nm}^{an+bm} = \zeta_{nm}^{an}\zeta_{nm}^{bm} = \zeta_m^a \zeta_n^b$$

und somit

$$\mathbb{Q}[\zeta_{nm}] \subseteq \mathbb{Q}[\zeta_n, \zeta_m] .$$

(b) Nach Voraussetzung sind

$$\alpha_n := \cos(2\pi/n) , \quad \alpha_m := \cos(2\pi/m)$$

konstruierbar. Es sei F der Körper aller konstruierbaren reellen Zahlen. Nach Vorlesung sind dann auch

$$\beta_n := \sin(2\pi/n) = \sqrt{1-\alpha_n^2} , \quad \beta_m := \sin(2\pi/m) = \sqrt{1-\alpha_m^2}$$

konstruierbar. Also gilt

$$\zeta_n = \alpha_n + i\beta_n \in F[i] , \quad \zeta_m = \alpha_m + i\beta_m \in F[i] .$$

Daraus folgt nach (a)

$$\zeta_{nm} \;\in\; \mathbb{Q}[\zeta_n, \zeta_m] \;\subseteq\; F[i] \;,$$

und daher

$$\cos\left(\frac{2\pi}{nm}\right) \;=\; \frac{1}{2}\left(\zeta_{nm} + \zeta_{nm}^{-1}\right) \;\in\; F[i] \cap \mathbb{R} \;=\; F \;,$$

d.h. der Winkel $\frac{2\pi}{nm}$ ist konstruierbar. Daher ist auch das regelmäßige nm-Eck konstruierbar.

Bemerkung: Geometrisch geht das wie folgt. Es gibt $a, b \in \mathbb{Z}$ mit $an + bm = 1$. Also trägt man b-mal den Winkel $2\pi/n$ ab, und anschließend a-mal den Winkel $2\pi/m$. Insgesamt hat man den Winkel

$$b\,\frac{2\pi}{n} + a\,\frac{2\pi}{m} \;=\; \frac{2\pi(bm + ab)}{nm} \;=\; \frac{2\pi}{nm} \;.$$

(c) Im Falle $n = m = 2$ ist $\mathbb{Q}[\zeta_m, \zeta_m] = \mathbb{Q}[-1] = \mathbb{Q}$, aber $\mathbb{Q}[\zeta_{nm}] = \mathbb{Q}[i] \neq \mathbb{Q}$. Also braucht (a) nicht zu gelten, falls n und m nicht teilerfremd sind.

Das regelmäßige 9-Eck ist nach Vorlesung nicht konstruierbar, das regelmäßige 3-Eck ist es jedoch. Also hat man mit $n = m = 3$ einen Widerspruch zu (b), sofern n und m nicht teilerfremd sind.

Aufgabe 2: (1+1+1+1=4 P)

(a) Bestimme das Minimalpolynom von $\alpha := \zeta_5 + \zeta_5^{-1}$ über $\mathbb{Q}$.

(b) Bestimme das Minimalpolynom von ζ_5 über dem Körper $K := \mathbb{Q}[\alpha]$.

(c) Zeige:

$$\mathbb{Q}[\zeta_8] = \mathbb{Q}[i, \sqrt{2}].$$

(d) Schließe aus (a)-(c): die Kreisteilungspolynome ϕ_5 und ϕ_8 sind irreduzibel über $\mathbb{Q}$.

Lösung:

(a) Es gilt

$$0 \;=\; \Phi_5(\zeta_5) \;=\; \zeta_5^4+\zeta_5^3+\zeta_5^2+\zeta_5+1 \;=\; \zeta_5^{-1}+\zeta_5+\zeta_5^{-2}+\zeta_5^2+1 \;=\; \alpha+\zeta_5^2+\zeta_5^{-2}+1 \;.$$

Daher wird

$$\alpha^2 \;=\; \left(\zeta_5 + \zeta_5^{-1}\right)^2 \;=\; \zeta_5^2 + 2 + \zeta_5^{-2} \;=\; -\alpha + 1 \;.$$

Damit ist α Nullstelle des Polynoms $g := X^2 + X - 1$. Dieses Polynom ist normiert, und seine Reduktion modulo 2 lautet $X^2 + X + 1$ und ist irreduzibel in $\mathbb{F}_2[X]$, da sie vom Grade 2 oder 3 ist und keine Nullstellen in $\mathbb{F}_2$ hat. Daher ist g auch irreduzibel in $\mathbb{Z}[X]$ und $\mathbb{Q}[X]$. Also gilt

$$\mathrm{minpol}_{\mathbb{Q}}(\alpha) \;=\; g \;=\; X^2 + X - 1 \;.$$

(b) Wegen

$$\zeta_5^2 - \alpha\zeta_5 + 1 \;=\; 0$$

ist ζ_5 Nullstelle des Polynoms $X^2 - \alpha X + 1 \in K[X]$. Wegen $K_5 := \mathbb{Q}[\zeta_5] = K[\zeta_5]$ ist

$$[K_5 : K] \;=\; \deg \operatorname{minpol}_K(\zeta_5) \;\leq\; 2\;.$$

Andererseits ist $K \subseteq \mathbb{R}$ wegen $\alpha \in \mathbb{R}$, währenddessen $\zeta_5 \in \mathbb{C} \setminus \mathbb{R}$ ist. Also gilt $K_5 \neq K$ und daher $[K_5 : K] = 2$. (Das war auch schon auf Blatt 10 gezeigt worden). Daraus folgt

$$\operatorname{minpol}_K(\zeta_5) \;=\; X^2 - \alpha X + 1\;.$$

(c) Es gilt

$$i \;=\; \zeta_4 \;=\; \zeta_8^2\;,\;\; \sqrt{2} \;=\; 2\cos(\pi/4) \;=\; (\zeta_8 + \zeta_8^{-1})\;.$$

Daraus folgt

$$\mathbb{Q}[\zeta_8] \;\supseteq\; \mathbb{Q}[i, \sqrt{2}]\;.$$

Andererseits ist

$$\zeta_8 \;=\; \cos(\pi/4) + i\sin(\pi/4) \;=\; \frac{1}{\sqrt{2}}\,(1+i)\;,$$

und daraus folgt

$$\mathbb{Q}[\zeta_8] \;\subseteq\; \mathbb{Q}[i, \sqrt{2}]\;.$$

(d) Nach (a) und (b) ist mit dem Gradsatz

$$[\mathbb{Q}[\zeta_5] : \mathbb{Q}] \;=\; [K_5 : K]\cdot[K : \mathbb{Q}] \;=\; 2\cdot 2 \;=\; 4\;.$$

Ferner ist Φ_5 ein normiertes Polynom vom Grade $\phi(5) = 4$, welches ζ_5 als Nullstelle hat. Daher muß $\operatorname{minpol}_{\mathbb{Q}}(\zeta_5) = \Phi_5$ gelten. Insbesondere ist Φ_5 irreduzibel.

Wir wollen noch die Dimension $[K_8 : \mathbb{Q}]$ bestimmen, ohne die Irreduzibilität von Φ_8 zu verwenden. Es gilt

$$\begin{aligned}
X^2 + 1 &= \operatorname{minpol}_{\mathbb{Q}[\sqrt{2}]}(i) &\Longrightarrow\quad [\mathbb{Q}[i,\sqrt{2}] : \mathbb{Q}[\sqrt{2}]] &= 2\,,\\
X^2 - 2 &= \operatorname{minpol}_{\mathbb{Q}}(\sqrt{2}) &\Longrightarrow\quad [\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] &= 2\,.
\end{aligned}$$

Daraus folgt nach dem Gradsatz

$$[K_8 : \mathbb{Q}] \;=\; [\mathbb{Q}[i, \sqrt{2}] : \mathbb{Q}] \;=\; 2\cdot 2 \;=\; 4\;.$$

Ferner ist Φ_8 ein normiertes Polynom vom Grade $\Phi(8) = 4$, welches ζ_5 als Nullstelle hat. Daher muß $\operatorname{minpol}_{\mathbb{Q}}(\zeta_8) = \Phi_8$ gelten. Insbesondere ist Φ_8 irreduzibel.

Aufgabe 3: (1+1+1+2=5 P) Sei

$$f := X^3 + 2X + 2 \in \mathbb{F}_3[X],$$

$K/\mathbb{F}_3$ ein Zerfällungskörper von f und $\alpha \in K$ eine Nullstelle, $f(\alpha) = 0$. Zeigen Sie:

(a) Das Polynom f ist irreduzibel über $\mathbb{F}_3$. Daher ist K ein (der) Körper mit 27 Elementen.

(b) Es gilt $\alpha^{13} = 1$. (Hinweis: benutze $13 = 8 + 4 + 1$.)

(c) In $K[X]$ hat man folgende Zerlegungen:

$$\bar{\phi}_{13} := \frac{X^{13} - 1}{X - 1} = \prod_{i=1}^{12} (X - \alpha^i)$$

und

$$f = (X - \alpha)(X - \alpha^3)(X - \alpha^9).$$

(Hinweis: die Abbildung $\beta \mapsto \beta^3$ ist ein Automorphismus der Erweiterung $K/\mathbb{F}_3$.)

(d) Bestimme einen von f verschiedenen irreduziblen Faktor $g \in \mathbb{F}_3[X]$ von $\bar{\phi}_{13}$ (es reicht nicht, die Zerlegung von g in $K[X]$ anzugeben!).

Lösung:

Lemma *Es sei $f \in \mathbb{F}_p[X]$ irreduzibel vom Grade n, und es sei $q := p^n$. Dann ist der Zerfällungskörper von f über $\mathbb{F}_p$ gleich $\mathbb{F}_q$.*

Beweis: Es sei L der Zerfällungskörper von f über $\mathbb{F}_p$. Es sei α eine Nullstelle von f in L. Dann gilt $[\mathbb{F}_p[\alpha] : \mathbb{F}_p] = \deg f = n$, und folglich ist $\mathbb{F}_p[\alpha]$ ein Körper mit q Elementen, d.h. es gilt $\mathbb{F}_p[\alpha] = \mathbb{F}_q$. Nun ist $\mathbb{F}_q$ Zerfällungskörper von $X^q - X$ über $\mathbb{F}_p$, d.h. α ist Nullstelle von $X^q - X$. Folglich ist f ein Teiler von $X^q - X$ in $\mathbb{F}_p[X]$, und da $X^q - X$ in $\mathbb{F}_q[X]$ zerfällt, gilt dies auch für f. Dann ist aber $L = \mathbb{F}_q$. □

(a) Das Polynom f hat keine Nullstelle im $\mathbb{F}_3$ und ist vom Grade 2 oder 3. Daher ist es irreduzibel in $\mathbb{F}_3[X]$. Nach obigem Lemma mit $p := 3$ und $n := 3$ folgt $K = \mathbb{F}_{27}$.

(b) Es gilt

$$0 \;=\; f(\alpha) \;=\; \alpha^3 + 2\alpha + 2\,,$$

d.h.

$$\begin{aligned}
\alpha^3 & & &= \alpha + 1 \\
\alpha^4 &= \alpha(\alpha+1) & &= \alpha^2 + \alpha \\
\alpha^8 &= (\alpha^2+\alpha)^2 \;=\; \alpha^4 + 2\alpha^3 + \alpha^2 & & \\
&= \alpha^2 + \alpha + 2\alpha + 2 + \alpha^2 & &= 2\alpha^2 + 2\,.
\end{aligned}$$

Es folgt

$$\begin{aligned}
\alpha^{13} &= \alpha^8\alpha^4\alpha \;=\; (2\alpha^2+2)(\alpha^2+\alpha)\alpha \;=\; (2\alpha^4 + 2\alpha^3 + 2\alpha^2 + 2\alpha)\alpha \\
&= (\alpha^2+2)\alpha \;=\; \alpha^3 + 2\alpha \;=\; 1\,.
\end{aligned}$$

(c) Die Abbildung

$$\sigma : K \to K\,,\quad \beta \mapsto \beta^3$$

ist ein Homomorphismus, welcher auf $\mathbb{F}_3$ die Identität ist. Da K ein endlicher Körper ist, ist σ ein Automorphismus. Also bildet σ Nullstellen von f auf Nullstellen von f ab. Folglich sind mit α auch

$$\sigma(\alpha) \;=\; \alpha^3\,,\quad \sigma(\sigma(\alpha)) \;=\; \alpha^9$$

Nullstellen von f. Wegen $\alpha^{13} = 1$ hat α die Ordnung 13 in der multiplikativen Gruppe $K^\times$. Deshalb sind die Elemente

$$1,\ \alpha,\ \alpha^2,\ \ldots,\ \alpha^{12}$$

paarweise verschieden. Somit sind α, α^3 und α^9 drei verschiedene Nullstellen des normierten Polynoms f, und es ist $\deg f = 3$. Daraus folgt

$$f \ = \ (X-\alpha)(X-\alpha^3)(X-\alpha^9)\ .$$

Wegen $\alpha^{13} = 1$ hat das Polynom

$$\overline{\Phi_{13}} \ := \ \frac{X^{13}-1}{X-1}$$

die paarweise verschiedenen Nullstellen $\alpha, \alpha^2, \ldots, \alpha^{12}$, ist normiert und vom Grade 12. Daraus folgt

$$\overline{\Phi_{13}} \ = \ (X-\alpha)(X-\alpha^2)\cdot\ldots\cdot(X-\alpha^{12})\ .$$

(d) Es sei

$$g \ := \ (X-\alpha^2)(X-\alpha^6)(X-\alpha^{18})\ .$$

Dann ist g offenbar ein Teiler von $\overline{\Phi_{13}}$, und g ist nicht zu f assoziiert. Um die Koeffizienten von g zu bestimmen, betrachten wir

$$\begin{aligned}
g(X^2) \ &= \ (X^2-\alpha^2)(X^2-\alpha^6)(X^2-\alpha^{18}) \\
&= \ (X-\alpha)(X+\alpha)(X-\alpha^3)(X+\alpha^3)(X-\alpha^9)(X+\alpha^9) \\
&= \ f\cdot(-f(-X)) \\
&= \ (X^3+2X+2)\cdot(X^3+2X-2) \\
&= \ (X^3+2X)^2-2^2 \\
&= \ X^6+X^4+X^2-1\ .
\end{aligned}$$

Daraus folgt

$$g \ = \ X^3+X^2+X-1 \ \in \ \mathbb{F}_3[X]\ .$$

Da g vom Grade 2 oder 3 und ohne Nullstelle in $\mathbb{F}_3$ ist, ist g irreduzibel in $\mathbb{F}_3[X]$.