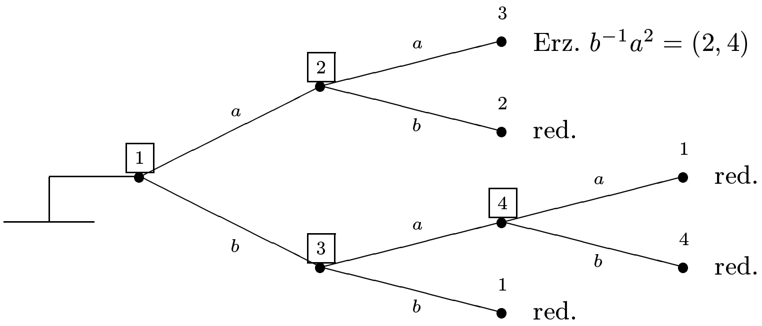
G. Nebe, M. Künzer 29.03.2005

Algebra I, WS 04/05

Lösung Nachklausur

Aufgabe 1.

(1) Wählt man z.B. 1 als erstes Element der base, so erhalten wir folgenden Baum.



Daraus ergeben sich die folgenden strong generators.

$$\begin{array}{lllll} w_1(1) & = & 1 & = & \mathrm{id} \\ w_1(2) & = & a & = & (1,2,3,4) \\ w_1(3) & = & b & = & (1,3) \\ w_1(4) & = & ab & = & (1,4)(2,3) \end{array}$$

Es ist $\mathrm{Stab}_G(1) = \langle ba^2 \rangle = \langle (2,4) \rangle$.
Wählt wir z.B. 2 als zweites Basiselement und schreiben $c := ba^2$, so ergeben sich aus dem Baum

$$\boxed{2} \xrightarrow{c} \boxed{4} \xrightarrow{c} 2 \ : \ \text{red.}$$

die strong generators

$$\begin{array}{lllll} w_2(2) & = & 1 & = & \mathrm{id} \\ w_2(4) & = & ba^2 & = & (2,4) \end{array}$$

Es ist nun bereits $\mathrm{Stab}_G(1,2) = 1$.

(2) Es ist $(1,2)(3,4) \in G$ genau dann, wenn $w_1(2)^{-1}(1,2)(3,4) = (2,4) \in \mathrm{Stab}_G(1)$. Dies ist der Fall (da $w_2(4)^{-1}(2,4) = 1 \in \mathrm{Stab}_G(1,2)$, wenn man möchte), und in der Tat ist

$$w_1(2)^{-1}(1,2)(3,4) \ = \ ba^2 \ ,$$

und also z.B. $(1,2)(3,4) = w_1(2)ba^2 = aba^2$.

Aufgabe 2.

(1) Es ist $\mu_{\alpha,\mathbf{Q}}(X) = X^2 - 2X + 2$, speziell also $\alpha^2 = 2\alpha - 2$ und $2/\alpha = 2 - \alpha$. Da $2 = (1+i)(1-i) \in (\alpha)$, ist

$$\begin{array}{lll} R/(\alpha) & = & \mathbf{Z}[\alpha]/(2,\alpha) \\ & \simeq & \mathbf{Z}[X]/(X^2 - 2X + 2, 2, X) \\ & \simeq & \mathbf{F}_2[X]/(X) \\ & \simeq & \mathbf{F}_2 \end{array}$$

ein Integritätsbereich, und damit $\alpha \in R$ ein Primelement. Außerdem folgt $|R/(\alpha^k)| = 2^k$ für $k \geq 1$.
Da ferner $\alpha^2/2 = i$ eine Einheit in R ist, ist $(\alpha^2) = (2)$.

(2) Umformen gibt z.B.

$$\left(\begin{array}{cccc} 2 & \alpha & 4 & 0 \\ \alpha & 0 & 0 & 2 \\ \hline 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right) \quad \rightsquigarrow \quad \left(\begin{array}{cccc} \alpha & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ \hline 1 & 0 & 0 & \alpha-2 \\ 0 & 1 & 2\alpha-4 & 2-2\alpha \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right).$$

Somit wird $\operatorname{Cokern}(u) \simeq R/(\alpha) \oplus R/(\alpha)$.

Ferner ergibt sich die Elementarteilerform von $\left(\begin{smallmatrix} 0 & \alpha-2 \\ 2\alpha-4 & 2-2\alpha \end{smallmatrix}\right)$ zu $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & 2\alpha \end{smallmatrix}\right)$. Es wird somit $\operatorname{Bild}(u) \simeq R/(\alpha) \oplus R/(2\alpha)$.

Probe: $|\operatorname{Cokern}(u)| = 2^{1+1}$, $|\operatorname{Bild}(u)| = 2^{1+3}$ und $|Y| = 2^{4+2}$ ist in Ordnung.

Aufgabe 3.

(1) Die Menge der Teiler von $385 = 5 \cdot 7 \cdot 11$ ist $\{1, 5, 7, 11, 35, 55, 77, 385\}$. Somit gibt es eine zyklische 7-Sylowgruppe P_5, eine zyklische 11-Sylowgruppe P_{11}, und entweder eine oder elf 5-Sylowgruppen. Gäbe es nur eine 5-Sylowgruppe P_5, notwendig zyklisch, so wäre G isomorph zu $P_5 \times P_7 \times P_{11}$, und damit abelsch. Also gibt es elf 5-Sylowgruppen, und also $11 \cdot (5-1) = 44$ Elemente der Ordnung 5.

(2) Um ein nichtabelsches semidirektes Produkt von $C_7 \times C_{11}$ mit C_5 zu erhalten, brauchen wir einen nichttrivialen Gruppenmorphismus von C_5 nach $\operatorname{Aut}(C_7 \times C_{11})$, i.e. wir brauchen ein Element der Ordnung 5 in $\operatorname{Aut}(C_7 \times C_{11}) \simeq \operatorname{Aut}(C_7) \times \operatorname{Aut}(C_{11})$. Nun ist $\operatorname{Aut}(C_{11}) \simeq (\mathbf{Z}/11\mathbf{Z})^* \simeq C_{10}$, enthält also insbesondere ein Element der Ordnung 5.

Aufgabe 4 **(20 Punkte)**

Berechnung des Zerfällungskörpers E.

Sei $K_0 := K$.

Schritt 1 a. Wir zerlegen $f(X)$ in irreduzible Faktoren in $K_0[X]$ (erübrigt sich hier nach Voraussetzung). Wir sind fertig, falls alle diese irreduziblen Faktoren von $f(X)$ Grad 1 haben.

Schritt 1 b. Sei K_1 ein Wurzelkörper über K_0 eines irreduziblen Faktors $f_1(X) \in K_0[X]$ von $f(X)$ von Grad > 1, sei a_1 eine Wurzel dieses Faktors, und sei $K_1 := K_0(a_1)$.

Schritt 2 a. Wir zerlegen $f(X)$ in irreduzible Faktoren in $K_1[X]$. Wir sind fertig, falls alle diese irreduziblen Faktoren von $f(X)$ Grad 1 haben.

Schritt 2 b. Sei K_2 ein Wurzelkörper über K_1 eines irreduziblen Faktors $f_2(X) \in K_1[X]$ von $f(X)$ von Grad > 1, sei a_2 eine Wurzel dieses Faktors, und sei $K_2 := K_1(a_2)$.

Schritt 3 a. Wir zerlegen $f(X)$ in irreduzible Faktoren in $K_2[X]$. Wir sind fertig, falls alle diese irreduziblen Faktoren von $f(X)$ Grad 1 haben.

Schritt 3 b. Sei K_3 ein Wurzelkörper über K_2 eines irreduziblen Faktors $f_3(X) \in K_2[X]$ von $f(X)$ von Grad > 1, sei a_3 eine Wurzel dieses Faktors, und sei $K_3 := K_2(a_3)$.

Und so fort.

Das Verfahren bricht ab, sobald $f(X)$ in $K_j[X]$ in Faktoren von Grad 1 zerfällt. Dann ist K_j von diesen Wurzeln erzeugt über K (sogar schon von einer j-elementigen Teilmenge der Menge der Wurzeln). (Da sich in jedem Schritt die Zahl der irreduziblen Faktoren von $f(X)$ um wenigstens 1 erhöht, bricht das Verfahren auch tatsächlich nach höchstens $\deg(f) - 1$ Schritten ab.) Somit können wir $E := K_j$ setzen.

Berechnung der Galoisgruppe $\operatorname{Gal}(E|K)$ *als Menge.*

Schreibe $f(X) = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n) \in E[X]$, wobei $n := \deg(f)$. Sei $E = K(\alpha_1, \ldots, \alpha_j)$.

Ein Automorphismus ist gegeben durch ein Tupel $(\beta_1, \ldots, \beta_j)$ mit allen β_i in $A := \{\alpha_1, \ldots, \alpha_n\}$, unter folgender Bedingung.

Zu Anfang ist das leere Tupel $()$ *zulässig.*

Sei $(\beta_1, \ldots, \beta_{i-1})$ bereits auf zulässige Weise gewählt. Dieses Tupel definiert einen Isomorphismus

$$K(\alpha_1, \ldots, \alpha_{i-1}) \xrightarrow[\sim]{\varphi_{i-1}} K(\beta_1, \ldots, \beta_{i-1})$$

über K von Teilkörpern von E, welcher α_s auf β_s schickt für alle $s \in [1, i-1]$. Nun ist β_i als Nullstelle von $f_i^{\varphi_{i-1}}(X)$ zu wählen, i.e. als Nullstelle des aus $f_i(X)$ durch Ersetzung von α_s durch β_s für alle $s \in [1, i-1]$ hervorgehenden Polynoms. Ist dies der Fall, so ist $(\beta_1, \ldots, \beta_{i-1}, \beta_i)$ *zulässig.* Diese Wahl definiert dann ihrerseits einen Isomorphismus $K(\alpha_1, \ldots, \alpha_i) \xrightarrow[\sim]{\varphi_i} K(\beta_1, \ldots, \beta_i)$, mit dem man fortfahren kann.

Die Menge der zulässigen Tupel $(\beta_1,\ldots,\beta_j)$ der Länge j definiert einen Automorphismus von E, und steht so in Bijektion zur Menge $\mathrm{Gal}(E|K)$. In anderen Worten, als Menge läßt sich $\mathrm{Gal}(E|K)$ über die zulässigen Tupel von Länge j beschreiben.

Berechnung der Galoisgruppe $\mathrm{Gal}(E|K)$ *als Gruppe.*

Sei ein Automorphismus σ von E über K durch das Bildtupel $(\beta_1,\ldots,\beta_j)$ von $(\alpha_1,\ldots,\alpha_j)$ gegeben.

Das Bild von α_s mit $s\in[j+1,n]$ berechnet sich folgendermaßen. Es ist $\alpha_s\in E=K(\alpha_1,\ldots,\alpha_j)$, und folglich gibt es ein Polynom $g_s(X_1,\ldots,X_j)\in K[X_1,\ldots,X_j]$ mit $\alpha_s=g_s(\alpha_1,\ldots,\alpha_j)$. Dann ist notwendig das Bild β_s von α_s unter dem gegebenen Automorphismus gleich $\beta_s=g_s(\alpha_1,\ldots,\alpha_s)$.

(Ist $j=n-1$, so erübrigt sich diese Rechnung, da man in $A\smallsetminus\{\beta_1,\ldots,\beta_{n-1}\}$ nur noch eine Wahl für β_n hat.)

Nun können wir einbetten und $\sigma\in\mathrm{Gal}(E|K)$ auf $\tilde\sigma\in\mathcal{S}_n$ schicken vermöge $\beta_i=\alpha_{\tilde\sigma(i)}$ für $i\in[1,n]$ – dies legt eine Permutation $\tilde\sigma$ eindeutig fest, und $\sigma\longmapsto\tilde\sigma$ definiert einen injektiven Gruppenmorphismus von $\mathrm{Gal}(E|K)$ nach $\mathcal{S}_n$. Man hat so $\mathrm{Gal}(E|K)$ bis auf Isomorphie als Untergruppe von $\mathcal{S}_n$ berechnet.

Aufgabe 5.

Sei z.B. $\mathbf{F}_9:=\mathbf{F}_3(\iota)$ mit $\iota^2=-1$. Dies ist gestattet, da $X^2+1\in\mathbf{F}_3[X]$ mangels Nullstelle irreduzibel ist.

Sei z.B. $\mathbf{F}_{81}:=\mathbf{F}_9(\kappa)$ mit $\kappa^2=\iota+1$. Dies ist gestattet, da $X^2-(\iota+1)\in\mathbf{F}_9[X]$ mangels Nullstelle irreduzibel ist.

Nun ist die Frobeniusbahn von κ über $\mathbf{F}_3$ gegeben durch $\{\kappa,\kappa^3,\kappa^9,\kappa^{27}\}=\{\kappa,\iota\kappa+\kappa,-\kappa,-\iota\kappa-\kappa\}$, und enthält somit 4 verschiedene Elemente. Also ist $\mathbf{F}_{81}=\mathbf{F}_3(\kappa)$. Und in der Tat erhalten wir das normierte irreduzible Polynom

$$\mu_{\kappa,\mathbf{F}_3}(X) \;=\; X^4+X^2-1\,.$$

Aufgabe 6.

Es ist $\mathrm{Gal}(\mathbf{Q}(\zeta_5)|\mathbf{Q})\simeq(\mathbf{Z}/(5))^*$, wobei $k+(5)\in(\mathbf{Z}/(5))^*$ das Element $\zeta:=\zeta_5$ auf ζ^k schickt.

Erster Lösungsweg.

Die Galoiskonjugierten von ζ sind in $\{\zeta,\zeta^2,\zeta^3,\zeta^4\}$. Und in der Tat ist das Tupel $(\zeta,\zeta^2,\zeta^3,\zeta^4)$ linear unabhängig über $\mathbf{Q}$, da mit $\zeta^4=-1-\zeta-\zeta^2-\zeta^3$ bezüglich der Basis $(1,\zeta,\zeta^2,\zeta^3)$ die Matrix

$$\begin{pmatrix}0&0&0&-1\\1&0&0&-1\\0&1&0&-1\\0&0&1&-1\end{pmatrix}$$

zu betrachten ist, und diese ist regulär. Alternativ, da die Multiplikation mit ζ auf $\mathbf{Q}(\zeta)$ ein $\mathbf{Q}$-linearer Isomorphismus ist, ist mit $(1,\zeta,\zeta^2,\zeta^3)$ auch $(\zeta,\zeta^2,\zeta^3,\zeta^4)$ eine Basis. Jedenfalls ist

$$(\;\zeta,\;\zeta^2,\;\zeta^3,\;\zeta^4\;)$$

eine Normalbasis von $\mathbf{Q}(\zeta)|\mathbf{Q}$.

Zweiter Lösungsweg (nur im Notfall).

Wir verwenden die Notation von Aufgabe 56. Es ist $\mu_{\zeta,\mathbf{Q}}(X)=\Phi_4(X)=X^4+X^3+X^2+X+1$, und so wird

$$f(X) \;=\; \frac{1}{5}\left(((\zeta^2-\zeta)X^3+(\zeta^3-\zeta)X^2+(-\zeta^3-\zeta^2-2\zeta-1)X+(-\zeta+1)\right)\,,$$

und damit

$$\begin{array}{rcl} d(X) & = & \frac{1}{25}\Big((-8\zeta^3-8\zeta^2-4)X^9+(-8\zeta^3-8\zeta^2-4)X^8+(-24\zeta^3-24\zeta^2-12)X^7+(-52\zeta^3-52\zeta^2-26)X^6\\ & & +(-48\zeta^3-48\zeta^2-24)X^5+(-52\zeta^3-52\zeta^2-26)X^4+(-32\zeta^3-32\zeta^2-16)X^3+(-16\zeta^3-16\zeta^2-8)X^2\\ & & +(-8\zeta^3-8\zeta^2-4)X+(-2\zeta^3-2\zeta^2-1)\Big)\,. \end{array}$$

Glücklicherweise ist bereits $d(0)=-2\zeta^3-2\zeta^2-1\neq0$ (was man auch durch Berechnen der Determinante der Matrix erkennen kann, in welcher in den Einträgen bereits 0 eingesetzt wird). Somit ist z.B. $5f(0)=1-\zeta$ geeignet, was die Normalbasis

$$(\;1-\zeta,\;1-\zeta^2,\;1-\zeta^3,\;1-\zeta^4\;)$$

von $\mathbf{Q}(\zeta)|\mathbf{Q}$ liefert.

Aufgabe 7.

Faktorisiert in irreduzible Faktoren wird $X^3-1=(X-1)(X^2+X+1)$. Der euklidsche Algorithmus liefert

$$\frac{1}{3}(X^2+X+1)-\frac{1}{3}(X+2)(X-1) \;=\; 1\,.$$

Also ist z.B. das Bild von $\frac{1}{3}(X^2+X+1)$ in

$$\mathbf{Q}[X]/(X^3-1) \simeq \mathbf{Q}[X]/(X^2+X+1) \times \mathbf{Q}[X]/(X-1) \qquad (\simeq \mathbf{Q}[\zeta_3] \times \mathbf{Q})$$

gegeben durch $(0,1) \notin \{(0,0),\,(1,1)\}$.

Aufgabe 8.

(1) Die Aussage ist falsch. Denn in $\mathbf{Q}[X_1, X_2, X_3]$ sind die elementarsymmetrischen Polynome gegeben durch $s_1 = X_1 + X_2 + X_3$, $s_2 = X_1X_2 + X_1X_3 + X_2X_3$ und $s_3 = X_1X_2X_3$. Und z.B. $s_1^2 = (X_1^2 + X_2^2 + X_3^2) + 2(X_1X_2 + X_1X_3 + X_2X_3)$ ist kein elementarsymmetrisches Polynom (wie etwa der Koeffizient von X_1^2 zeigt).

(2) Die Aussage ist falsch. Es ist z.B. $X^4 + 4 = (X^2 + 2X + 2)(X^2 - 2X + 2)$.

(3) Die Aussage ist falsch. Dafür gibt es mehrere alternative Lösungen. In jeder sei zunächst angenommen, es gäbe so eine Gruppe G.

1. Lösung. Die Tatsache, daß G einen Normalteiler N_1 isomorph zu $\mathcal{A}_5$ enthält, liefert wegen der Einfachheit von $\mathcal{A}_5$, daß G genau die Kompositionsfaktoren $\mathcal{A}_5$ und C_2 besitzt (im Sinne des Satzes von Jordan-Hölder). Die Tatsache, daß G einen Normalteiler N_2 mit $G/N_2 \simeq C_3$ enthält, impliziert aber, daß G auch einen Kompositionsfaktor C_3 besitzen muß, was aber nicht der Fall ist. Somit haben wir einen Widerspruch.

2. Lösung. Es ist $|N_2/(N_1 \cap N_2)| = |(N_1N_2)/N_1| \in \{1, 2\}$, da $[G : N_1] = 2$. Nun ist aber $N_1 \cap N_2$ ein Normalteiler von N_1 von Ordnung $\leq |N_2| = 40$, und also ist $N_1 \cap N_2 = 1$ wegen N_1 einfach. Insgesamt ist $40 = |N_2| = |N_2/(N_1 \cap N_2)||N_1 \cap N_2| \in \{1, 2\}$, Widerspruch.

3. Lösung. Sei G' die Kommutatoruntergruppe von G. Es ist $G' \leq N_1$, da $G/N_1 \simeq C_2$ abelsch ist, und auch $G' \leq N_2$, da $G/N_2 \simeq C_3$ abelsch ist. Also ist $G' \leq N_1 \cap N_2$. Nun ist aber $N_1 \cap N_2$ als Normalteiler von Ordnung ≤ 40 der einfachen Gruppe N_1 abelsch, und somit ist $N_1 \cap N_2 = 1$ (wie in der 2. Lösung). Folglich ist $G' = 1$, d.h. G ist abelsch. Da nun $N_2 \simeq \mathcal{A}_5$ nicht abelsch ist, und zugleich abelsch als Untergruppe einer abelschen Gruppe, sind wir bei einem Widerspruch angelangt.