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

Algebra I

13. Übungsblatt

keine Abgabe

Aufgabe 1: Sei G eine endliche abelsche Gruppe der Ordnung n.

(a) Zeigen Sie: für jeden Teiler d von n existiert eine Untergruppe $H \subset G$ mit d Elementen. (Hinweis: benutzen Sie den Hauptsatz über endlich erzeugte abelsche Gruppen, um das Problem auf zyklische Gruppen zurückzuführen.)

(b) Folgern Sie aus (a): wenn $n = p_1 p_2 \cdot \ldots \cdot p_m$ die Zerlegung von n in Primfaktoren ist, dann gibt es eine Folge von Untergruppen

$$\{1\} = H_0 \subset H_1 \subset \cdots \subset H_m = G$$

mit $|H_i| = p_1 \cdot \ldots \cdot p_i$.

(c) Nun sei $G = (\mathbb{Z}/17)^\times$, also gilt $n = 16 = 2^4$. In diesem Fall ist die Folge von Untergruppen H_i in (b) eindeutig, und jedes H_i ist zyklisch. Bestimmen Sie einen Erzeuger von H_i, für $i = 1, \ldots, 4$.

Lösung:

(a)
- Wir nehmen zunächst an, die Gruppe G sei zyklisch, etwa $G = \langle g \rangle$. Dann gilt $\mathrm{ord}(g) = n$ und daher $\mathrm{ord}(g^{n/d}) = d$. Also ist $H := \langle g^{n/d} \rangle$ eine Untergruppe von G mit d Elementen.
- Nach dem Hauptsatz über endlich erzeugte ablesche Gruppen können wir annehmen, daß gilt

  $$G \;=\; \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_k\mathbb{Z} \;,$$

  wobei $d_i | d_{i+1}$ gilt für $i = 1, \ldots, k-1$. Wegen $n = d_1 \cdot \ldots \cdot d_k$ und $d|n$ gibt es Teiler $e_1, \ldots, e_k$ von $d_1, \ldots, d_k$ mit $d = e_1 \cdot \ldots \cdot e_k$. Nach obigem gibt zu jedem i eine Untergruppe U_i von $\mathbb{Z}/d_i\mathbb{Z}$ der Ordnung $|U_i| = e_i$. Dann ist

  $$U \;:=\; U_1 \times \ldots \times U_k$$

  eine Untergruppe von G mit d Elementen.

(b) Wir führen Induktion nach m. Im Falle $m = 0$ ist die Behauptung klar. Im Induktionsschritt nehmen wir $m \geq 1$ an, und die Behauptung sei für $m-1$ bewiesen. Nach (a) gibt es eine Untergruppe H_{m-1} von G mit $p_1 \cdot \ldots \cdot p_{m-1}$ Elementen. Wendet man nun die Induktionshypothese auf H_{m-1} an, so folgt sofort die Behauptung.

(c) Die Gruppe $G = (\mathbb{Z}/17\mathbb{Z})^\times$ ist zyklisch nach Vorlesung. Die Folge von Untergruppen ist eindeutig, da es bei zyklischen Gruppen $G = \langle g \rangle$ zu jedem Teiler

d der Gruppenordnung n stets eine eindeutig bestimmte Untergruppe mit d Elementen gibt, nämlich $\langle g^{n/d} \rangle$, und diese ist wiederum zyklisch.

Wir suchen einen Erzeuger von G. Es gilt

$$3^8 \equiv (81)^2 \equiv (-4)^2 \equiv 16 \not\equiv 1 \mod 17 .$$

Also gilt $\operatorname{ord} \overline{3} = 16$ in $(\mathbb{Z}/17\mathbb{Z})^\times$, d.h. es gilt $G = \langle \overline{3} \rangle$. Also ist

$$H_i = \langle 3^{2^{4-i}} \rangle ,$$

d.h.

$$H_1 = \langle 3^8 \rangle = \langle 16 \rangle , \quad H_2 = \langle 3^4 \rangle = \langle 13 \rangle , \quad H_3 = \langle 3^2 \rangle = \langle 9 \rangle , \quad H_4 = \langle 3 \rangle .$$

Aufgabe 2: Seien G_1, G_2 endliche Gruppen (nicht notwendigerweise abelsch) und $H \subset G_1 \times G_2$ eine Untergruppe. Wir bezeichnen für $i = 1, 2$ mit $p_i : G_1 \times G_2 \to G_i$ die Projektion auf den $i$ten Faktor. Beweisen oder widerlegen Sie folgende Aussage:
Wenn $p_i(H) = G_i$ für $i = 1, 2$, dann gilt $H = G_1 \times G_2$.

Lösung: Es sei $G_1 := G_2 := G := \mathbb{Z}/2\mathbb{Z}$. Man rechnet leicht nach, daß

$$H := \{(z_1, z_2) \in G \times G |\ z_1 = z_2\}$$

eine Untergruppe von G ist. Nun gilt offenbar $p_i(H) = G = G_i$ für $i = 1, 2$, aber $H \neq G_1 \times G_2$.

Lemma *Es sei L/K eine Galoiserweiterung vom Grad n, und es sei $U \leq \operatorname{Gal}(L/K)$. Dann gilt*

$$[L^U : K] = \frac{n}{|U|} .$$

Beweis: Die Erweiterung L/L^U ist ebenfalls galoissch, und nach dem Hauptsatz gilt $\operatorname{Gal}(L/L^U) = U$. Daraus folgt

$$[L : L^U] = |\operatorname{Gal}(L/L^U)| = |U| .$$

Mit dem Gradsatz $n = [L : K] = [L : L^U] \cdot [L^U : K]$ folgt die Behauptung. □

Aufgabe 3: Sei $\zeta := \exp(2\pi i/12)$ und $L = \mathbb{Q}[\zeta]$ der Körper der 12ten Einheitswurzeln. Nach der Vorlesung gibt es einen Gruppenisomorphismus

$$(\mathbb{Z}/12)^\times \xrightarrow{\sim} \operatorname{Gal}(L/\mathbb{Q}),$$

der ein $a \in (\mathbb{Z}/12)^\times$ auf einen Automorphismus σ_a mit $\sigma_a(\zeta) = \zeta^a$ abbildet.

(a) Zeigen Sie: $L = \mathbb{Q}[i, \sqrt{3}] \subset \mathbb{C}$.

(b) Was ist der Effekt von σ_a auf den Elementen i und $\sqrt{3}$, für $a = 5, 7, 11$?

(c) Bestimme die Untergruppe von $\operatorname{Gal}(L/\mathbb{Q})$, die zu dem Teilkörper $\mathbb{Q}[\sqrt{3}] \subset L$ gehört.

(d) Bestimme den Fixkörper $L^{\langle \sigma_7 \rangle}$ der von σ_7 erzeugten Untergruppe.

(e) Zeigen Sie: $\alpha := i+\sqrt{3}$ ist ein primitives Element, d.h. $L = \mathbb{Q}[\alpha]$.

Lösung:

(a) Es gilt $[L:\mathbb{Q}] = \varphi(12) = \varphi(3)\varphi(4) = 4$. Ferner gilt $\zeta^3 = i$ und $\zeta+\zeta^{-1} = 2\cos(\pi/6) = \sqrt{3}$. Also ist

$$\mathbb{Q}[i,\sqrt{3}] \;\subseteq\; \mathbb{Q}[\zeta] \;=\; L\,.$$

Andererseits gilt

$$[\mathbb{Q}[i,\sqrt{3}]:\mathbb{Q}] \;=\; [\mathbb{Q}[i,\sqrt{3}]:\mathbb{Q}[\sqrt{3}]]\cdot[\mathbb{Q}[\sqrt{3}]:\mathbb{Q}] \;=\; 2\cdot 2 \;=\; 4 \;=\; [L:\mathbb{Q}]\,.$$

Daraus folgt die Behauptung. Alternativ beachte man, daß

$$\zeta \;=\; \cos(\pi/6)+i\sin(\pi/6) \;=\; \frac{\sqrt{3}+i}{2}\,.$$

(b) Es wird

$$\begin{aligned}
\sigma_a(i) &= \sigma_a(\zeta^3) = \zeta^{3a} &&= i^a\,,\\
\sigma_a(\sqrt{3}) &= \sigma_a(\zeta+\zeta^{-1}) = \zeta^a+\zeta^{-a} &&= 2\cos(a\pi/6)\,.
\end{aligned}$$

Es gilt also

$$\begin{array}{llll}
\sigma_5: & i\mapsto i\,, & \sqrt{3}\mapsto 2\cos(5\pi/6) & = -\sqrt{3}\\
\sigma_7: & i\mapsto -i\,, & \sqrt{3}\mapsto 2\cos(7\pi/6) & = -\sqrt{3}\\
\sigma_{11} & i\mapsto -i & \sqrt{3}\mapsto 2\cos(11\pi/6) & = \sqrt{3}\,.
\end{array}$$

(c) Die gesuchte Untergruppe ist nach (b) gegeben durch

$$\mathrm{Gal}(L/\mathbb{Q}[\sqrt{3}]) \;=\; \{\sigma\in\mathrm{Gal}(L/\mathbb{Q})|\;\sigma(\sqrt{3})=\sqrt{3}\} \;=\; \{\sigma_1,\sigma_{11}\}\,.$$

(d) Nach (b) gilt

$$\sigma_7(i\sqrt{3}) = i\sqrt{3}\,,$$

d.h. es gilt

$$\mathbb{Q}[i\sqrt{3}] \;\subseteq\; L^{\langle\sigma_7\rangle}\,.$$

Nach obigem Lemma gilt

$$[L^{\langle\sigma_7\rangle}:\mathbb{Q}] \;=\; \frac{4}{\operatorname{ord}\sigma_7} \;=\; 2\,.$$

Da ferner auch $[\mathbb{Q}[i\sqrt{3}]:\mathbb{Q}] = 2$, folgt

$$L^{\langle\sigma_7\rangle} \;=\; \mathbb{Q}[i\sqrt{3}]\,.$$

(e) Es sei $M := \mathbb{Q}[\alpha]$. Dann ist nach (b)

$$\mathrm{Gal}(L/M) \;=\; \{\mathrm{id}\} \;=\; \mathrm{Gal}(L/L)\,.$$

Nach dem Hauptsatz der Galoistheorie folgt $L = M$.

Aufgabe 4: Sei $q = p^n$ eine Primzahlpotenz, $\mathbb{F}_q$ der Körper mit q Elementen.

(a) Zeigen Sie: Die Erweiterung $\mathbb{F}_q/\mathbb{F}_p$ ist eine Galois-Erweiterung. Der Automorphismus $\alpha \mapsto \alpha^p$ ist ein Erzeuger der Galois-Gruppe $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. Insbesondere gilt:

$$\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) \cong \mathbb{Z}/n.$$

(b) Bestimme alle Teilkörper $M \subset \mathbb{F}_q$ (in Abhängigkeit von n).

(c) Sei $q' = p^m$. Folgern Sie aus (b):

$$\mathbb{F}_{q'} \subset \mathbb{F}_q \quad \Leftrightarrow \quad m|n.$$

(d) Das Polynom $f = X^4 + X + 1 \in \mathbb{F}_2[X]$ ist irreduzibel in $\mathbb{F}_2$. Bezeichnet α eine Nullstelle von f, so ist dann der Körper $\mathbb{F}_2[\alpha]$ ein Körper mit 16 Elementen. Schreiben Sie alle Elemente des eindeutigen Teilkörpers mit 4 Elementen als Polynome in α.

Lösung:

(a) Nach Vorlesung ist $\mathbb{F}_q$ Zerfällungskörper des Polynoms $X^q - X$, welches als Nullstellen genau die q Elemente von $\mathbb{F}_q$ hat. Also ist $X^q - X$ separabel und $\mathbb{F}_q$ ist galoissch über $\mathbb{F}_p$. Die Galoisgruppe $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ hat die Ordnung $n = [\mathbb{F}_q : \mathbb{F}_p]$. Es sei

$$\sigma : \mathbb{F}_q \to \mathbb{F}_q,\ \alpha \mapsto \alpha^p$$

und $d := \mathrm{ord}(\sigma) \leq n$. Nach Vorlesung ist die Gruppe $\mathbb{F}_q^\times$ zyklisch, d.h. es gibt ein $\alpha \in \mathbb{F}_q^\times$ mit $\mathrm{ord}(\alpha) = q - 1$ in $\mathbb{F}_q^\times$. Dann folgt

$$\alpha^{p^d - 1} \ = \ \sigma^d(\alpha)/\alpha \ = \ 1 \ .$$

Daher ist $q - 1 = p^n - 1$ ein Teiler von $p^d - 1$. Insbesondere folgt $n \leq d$, d.h. $n = d$. Folglich ist σ ein Erzeuger von $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$.

(b) Die Untergruppen von $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \langle \sigma \rangle$ sind genau die Gruppen $\langle \sigma^d \rangle$, wobei d ein Teiler von n ist. Nach dem Hauptsatz der Galoistheorie erhält man alle Unterkörper von $\mathbb{F}_q$, d.h. alle Zwischenkörper von $\mathbb{F}_q/\mathbb{F}_p$, indem man

$$\mathbb{F}_q^{\langle \sigma^d \rangle} \ = \ \{a \in \mathbb{F}_q |\ a^{p^d} = a\}$$

bestimmt für alle Teiler d von n. Es folgt nach obigem Lemma

$$[\mathbb{F}_q^{\langle \sigma^d \rangle} : \mathbb{F}_p] \ = \ \frac{n}{\mathrm{ord}(\sigma^d)} \ = \ d \ .$$

Dann ist $\{a \in \mathbb{F}_q |\ a^{p^d} = a\}$ ein Körper der Dimension d über $\mathbb{F}_p$, also gleich dem Körper $\mathbb{F}_{p^d}$.

(c) Das folgt direkt aus dem Ergebnis von (b).

(d) Zunächst ist $(1, \alpha, \alpha^2, \alpha^3)$ eine Basis von $\mathbb{F}_2[\alpha]$ über $\mathbb{F}_2$. Daher ist $\alpha^3 \neq 1$ Ferner ist

$$\alpha^5 \ = \ \alpha \cdot \alpha^4 \ = \ \alpha(\alpha + 1) \ = \ \alpha^2 + \alpha \ \neq \ 1 \ .$$

Daher ist $\mathrm{ord}(\alpha) = 15$ in der Gruppe $(\mathbb{F}_2[\alpha])^\times$. Mithin ist α ein Erzeuger von $(\mathbb{F}_2[\alpha])^\times$, d.h. es gilt

$$\mathbb{F}_2[\alpha] \ = \ \{0, 1, \alpha, \ \ldots \ , \alpha^{14}\} \ .$$

Nach der Rechnung in Teil (b) ist der Unterkörper mit 4 Elementen gegeben durch

$$\{a \in \mathbb{F}_2[\alpha] |\ a^4 = a\} \ = \ \{0, 1, \alpha^5, \ \alpha^{10}\} \ = \ \{0, 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\} \ .$$

Aufgabe 5: Sei R ein nullteilerfreier Hauptidealring mit Quotientenkörper K und $u, v, n \in R$ mit $n = uv \neq 0$, und u, v seien teilerfremd in R. Zeigen Sie: Jedes Element aus K der Form $\frac{m}{n}$, mit $m \in R$, kann man schreiben als

$$\frac{m}{n} = \frac{a}{u} + \frac{b}{v},$$

mit $a, b \in R$.

Gilt diese Aussage auch für alle faktoriellen Ringe?

Lösung: Es sei $I := (u, v) = Ru + Rv$ das von u und v erzeugte Ideal in R. Dann gibt es ein $w \in R$ so, daß $I = (w) = Rw$. Wegen $u \in I$ und $v \in I$ ist w gemeinsamer Teiler von u und w. Aus der Teilerfremdheit folgt daher $w \in R^\times$, d.h. $I = R$. Mithin ist $1 \in I$, d.h. es gibt $a, b \in R$ derart, daß

$$1 = au + bv .$$

Es folgt

$$\frac{m}{n} = \frac{m(au + bv)}{uv} = \frac{ma}{v} + \frac{mb}{u} .$$

Diese Aussage gilt i.a. nicht in faktoriellen Ringen. Es sei etwa $R := \mathbb{Q}[X, Y]$ und $u := X$, $v := Y$. Dann sind u, v teilerfremd. Gäbe es $a, b \in R$ mit $\frac{1}{XY} = \frac{a}{X} + \frac{b}{Y}$, so folgte daraus $1 = aY + bX$. Betrachtet man nun Einsetzungshomomorphismus $R \to \mathbb{Q}$, $f \mapsto f(0, 0)$, so folgte dann $1 = 0$, ein Widerspruch.

Aufgabe 6: Sei $G \subset S_4$ die von den zwei Permutationen

$$\sigma = (1\,2\,3\,4), \quad \tau = (2\,4)$$

erzeugte Untergruppe. Zeigen Sie:

(a) Die kanonische Operation von G auf der Menge $\{1, 2, 3, 4\}$ ist transitiv.

(b) Die von σ erzeugte Untergruppe $N = \langle \sigma \rangle$ ist ein Normalteiler von G. Bestimmen Sie die Ordnungen $|N|$, $|G/N|$ und $|G|$.

(c) Es gibt einen Normalteiler $H \lhd G$ mit $\tau \in H$ und $|H| = 4$. Ist H eine zyklische Gruppe?

(d) Bestimmen Sie die Untergruppe $H \cap N \subset G$.

Was hat die Gruppe G mit dem regelmässigen Viereck (Quadrat) zu tun?

Lösung:

(a) Man beachte, daß gilt $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 4$ und $\sigma(4) = 1$. Also liegen alle 4 Elemente der Menge $\{1, 2, 3, 4\}$ in derselben Bahn bezüglich G.

(b) Eine allgemeines Element von G ist ein Produkt von Faktoren, die σ oder τ sind. Es genügt daher zu zeigen, daß $\tau\sigma\tau^{-1}$ wieder in N liegt. Nun ist $\tau\sigma\tau^{-1} = (1\ 4\ 3\ 2) = \sigma^{-1}$. Daraus folgt, daß N ein Normalteiler von G ist.

Die zyklische Gruppe N hat die Ordnung $|N| = \operatorname{ord} \sigma = 4$. Da ein allgemeines Element von G Produkt von Faktoren σ oder τ ist, und da N Normalteiler ist, ist die zugehörige Linksnebenklasse gN eines Elementes $g \in G$ stets von der Form N oder $\tau N = N\tau$. Mithin folgt $|G/N| = 2$.

Mit der Regel von Lagrange folgt

$$|G| = |G/N| \cdot |N| = 2 \cdot 4 = 8 .$$

(c) Man setze

$$H \;:=\; \{\mathrm{id},\ (2\,4),\ (1\,3) = \sigma\tau\sigma^{-1},\ (1\,3)(2\,4)\}\ .$$

Offenbar handelt es sich bei H um eine Untergruppe von G mit $\tau \in G$, und es gilt $|H| = 4$. Für die Normalteilereigenschaft genügt es zu zeigen, daß $\sigma H \sigma^{-1} \subseteq H$ gilt. Die Konjugation mit dem Element σ vertauscht aber genau $(2\,4)$ und $(1\,3)$. Also ist H Normalteiler.

Alternativ: Wegen $|H| = 4$ gilt $|G/H| = 2$. Und eine Untegruppe vom Index 2 ist stets Normalteiler.

H ist nicht zyklisch, da alle Elemente von H die Ordnung 1 oder 2 haben.

(d) Offenbar gilt $H \cap N = \{\mathrm{id}, (1\,3)(2\,4)\}$.

Aufgabe 7: Sei

$$f := X^4 - 2 = \prod_{j=1}^{4}(X - \alpha_j) \in \mathbb{Q}[X],$$

wobei $\alpha_1 = \sqrt[4]{2} \in \mathbb{R}$ die einzige reelle Nullstelle von f ist und

$$\alpha_j = e^{2\pi i(j-1)/4} \cdot \alpha_1, \qquad j = 1, \ldots, 4.$$

Sei $L \subset \mathbb{C}$ der Zerfällungskörper von f. Wir fassen die Galois-Gruppe $G = \mathrm{Gal}(L/\mathbb{Q})$ als Untergruppe von S_4 auf, vermöge der Operation von G auf der Menge der Nullstellen α_j. Zeigen Sie:

(a) $L = \mathbb{Q}[i, \sqrt[4]{2}]$.

(b) Es gilt $[L : \mathbb{Q}] = 8$. (Hinweis: betrachte den Teilkörper $\mathbb{Q}[\sqrt[4]{2}] \subset L$.)

(c) Der Automorphismus $z = x + iy \mapsto \bar{z} = x - iy$ von $\mathbb{C}$ induziert ein Element $\tau \in G$. Aufgefasst als Permutation ist $\tau = (2\,4)$.

(d) Das Polynom f ist auch über dem Körper $\mathbb{Q}[i] \subset L$ irreduzibel. (Hinweis: benutze (b).)

(e) Die Galoisgruppe G enthält die Permutation $\sigma = (1\,2\,3\,4)$. Der Fixkörper der von σ erzeugten Untergruppe $N = \langle\sigma\rangle$ ist $L^N = \mathbb{Q}[i]$. (Hinweis: benutzen Sie (d)).

(f) Die Galoisgruppe G ist von den beiden Elementen σ, τ erzeugt (und damit identisch mit der in Aufgabe 6 studierten Gruppe).

(g) Bestimmen Sie den Fixkörper der Untergruppen H und $H \cap N$ (H ist definiert wie in Aufgabe 6).

Lösung: Die Erweiterung $L/\mathbb{Q}$ ist galoissch.

(a) Es gilt $\alpha_j = i^{j-1}\sqrt[4]{2}$. Andererseits ist $\mathrm{i} = \alpha_2/\alpha_1$. Also ist

$$L \;=\; \mathbb{Q}[\alpha_1, \ldots, \alpha_4] \;=\; \mathbb{Q}[i, \sqrt[4]{2}]\ .$$

(b) Das Polynom $X^4 - 2$ ist irreduzibel in $\mathbb{Q}[X]$ nach dem Eisensteinschen Kriterium. Daraus folgt $\mathrm{minpol}_{\mathbb{Q}}(\sqrt[4]{2}) = X^4 - 2$ und daher

$$[\mathbb{Q}[\sqrt[4]{2} : \mathbb{Q}] \;=\; 4\ .$$

Ferner ist das Polynom X^2+1 irreduzibel in $\mathbb{Q}[\sqrt[4]{2}][X]$, da $\mathbb{Q}[\sqrt[4]{2}] \subseteq \mathbb{R}$. Also ist $\operatorname{minpol}_{\mathbb{Q}[\sqrt[4]{2}]}(i) = X^2+1$ und daher

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

Nach dem Gradsatz folgt $[L : \mathbb{Q}] = 8$.

(c) Die komplexe Konjugation vertauscht die Elemente $\alpha_2 = i\sqrt[4]{2}$ und $\alpha_4 = -i\sqrt[4]{2}$, während $\alpha_1 = \sqrt[4]{2}$ und $\alpha_3 = -\sqrt[4]{2}$ unverändert bleiben. Daher induziert dies einen Autormorphismus von L, d.h. ein Element von G. Als Nullstellenpermutation ist dies die Transposition (2 4), wie erklärt.

(d) Es gilt $[\mathbb{Q}[i] : \mathbb{Q}] = 2$. Nach (b) und dem Gradsatz folgt daher $[L : \mathbb{Q}[i]] = 4$. Ferner ist $L = \mathbb{Q}[i][\sqrt[4]{2}]$, und f ist ein normiertes Polynom vom Grade 4 mit $f(\sqrt[4]{2}) = 0$. Daraus folgt, daß

$$f \;=\; \operatorname{minpol}_{\mathbb{Q}[i]}(\sqrt[4]{2})\,,$$

und f ist irreduzibel in $\mathbb{Q}[i][X]$.

(e) Es gilt $L = \mathbb{Q}[i][\alpha_1] = \mathbb{Q}[i][\alpha_2]$, und nach (d) haben α_1 und α_2 dasselbe Minimalpolynom über $\mathbb{Q}[i]$, nämlich f. Nach Vorlesung gibt es daher einen Automorphismus $\sigma \in \operatorname{Gal}(Ł/\mathbb{Q}[i])$ mit $\sigma(\alpha_1) = \sigma(\alpha_2)$. Wegen $\sigma(i) = i$ gilt $\sigma(\alpha_2) = \sigma(\alpha_3)$, $\sigma(\alpha_3) = \alpha_4$ und $\sigma(\alpha_4) = \alpha_1$. Also entspricht σ der Nullstellenpermutation (1 2 3 4).

Es gilt offenbar $\mathbb{Q}[i] \subseteq L^N$. Andererseits folgt nach dem Lemma vor Aufgabe 4

$$|L^N : \mathbb{Q}| \;=\; \frac{8}{|N|} \;=\; 2 \;=\; [\mathbb{Q}[i] : \mathbb{Q}]\,.$$

Daraus folgt $L^N = \mathbb{Q}[i]$.

(f) Die von σ und τ erzeugte Untergruppe hat nach Aufgabe 6 genau 8 Elemente. Da $G = \operatorname{Gal}(L/\mathbb{Q})$ ebenfalls $8 = [L : \mathbb{Q}]$ Elemente hat, folgt $G = \langle \sigma, \tau \rangle$.

(g) Wir bestimmen mit dem Lemma vor Aufgabe 4 zuerst die Grade

$$\begin{aligned} [L^H : \mathbb{Q}] &\;=\; \frac{8}{|H|} &&=\; 2\,, \\ [L^{H\cap N} : \mathbb{Q}] &\;=\; \frac{8}{|H \cap N|} &&=\; 4\,. \end{aligned}$$

Es sei $\rho \in G$ durch die Nullstellenpermutation (1 3) definiert. Es gilt also $\rho(\sqrt[4]{2}) = -\sqrt[4]{2}$. Dann gilt $H = \{\mathrm{id}, \tau, \rho, \tau\rho\}$. Wegen

$$\rho(\sqrt{2}) \;=\; \rho((\sqrt[4]{2})^2) \;=\; (\rho(\sqrt[4]{2}))^2 \;=\; \sqrt{2}$$

ist

$$\mathbb{Q}[\sqrt{2}] \;\subseteq\; L^H\,.$$

Aus Dimensionsgründen folgt $L^H = \mathbb{Q}[\sqrt{2}]$.

Ferner gilt $L^{H\cap N} \supseteq L^N = \mathbb{Q}[i]$ und $L^{H\cap N} \supseteq L^H = \mathbb{Q}[\sqrt{2}]$. Daraus folgt

$$L^{H\cap N} \;\supseteq\; \mathbb{Q}[\sqrt{2}, i]\,.$$

Wegen $[\mathbb{Q}[\sqrt{2}, i] : \mathbb{Q}] = 4$ folgt aus Dimensionsgründen $L^{H\cap N} = \mathbb{Q}[\sqrt{2}, i]$.

Zur Teilnahme an der Scheinklausur müssen Sie auf den Übungblättern 1 bis 12 mindestens 60 Punkte erzielt haben. Sollten Sie dieses Ziel verfehlt und trotzdem mindestens 50 Punkte erreicht haben, können Sie evtl. durch Bearbeitung dieses Übungsblattes doch noch die Berechtigung zur Teilnahme erreichen. Geben Sie in diesem Fall ihre Lösungen am Donnerstag, den 9.2. bei Herrn Martin ab (*vor* der Übung!).