Musterlösung Wiederholungsserie

1. Gibt es einen Integritätsbereich mit 15 Elementen?

   Lösung: Let R be a ring with 15 elements. Then $(R,+)$ is an abelian group of order 15. It follows from the classification theorem for finitely generated abelian groups that $(R,+) \cong (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$. Therefore we may thus choose elements $a, b \in R$ of respective orders 3 and 5. Then $a, b \neq 0$, and $3ab = (3a)b = 0b = 0$ and $5ab = (5b)a = 0a = 0$; hence $ab = 2 \cdot 3ab - 5ab = 0$. Thus R is not an integral domain and the answer is no.

2. Sei K ein Körper. Berechne die Elementarteiler des $K[X]$-Moduls

$$M := K[X]/((X+1)^2) \oplus K[X]/\big((X-1)(X^2+1)\big) \oplus K[X]/\big((X+1)(X^2-1)\big).$$

   Lösung: If K has characteristic 2, then $X^2+1 = X^2-1 = (X+1)^2$. This yields

$$M = K[X]/\big((X+1)^2\big) \oplus K[X]/\big((X+1)^3\big) \oplus K[X]/\big((X+1)^3\big).$$

   Since $(X+1)^2 | (X+1)^3 | (X+1)^3$, it follows that the elementary divisors are $e_1 = (X+1)^2$ and $e_2 = e_3 = (X+1)^3$.

   Suppose now that $\mathrm{char}(K) \neq 2$. Then $X^2-1 = (X+1)(X-1)$, and the polynomials $X+1$ and $X-1$ and X^2+1 are pairwise relatively prime. The Chinese remainder theorem therefore allows us to separate terms corresponding to their powers. This yields:

$$\begin{aligned} M \cong \;& K[X]/((X+1)^2) \oplus K[X]/\big(X-1\big) \oplus K[X]/\big((X^2+1)\big) \\ & \oplus K[X]/\big((X+1)^2\big) \oplus K[X]/\big(X-1\big). \end{aligned}$$

   Again using the Chinese remainder theorem to regroup terms, we obtain:

$$M \cong K[X]/\big((X-1)(X+1)^2\big) \oplus K[X]/\big((X-1)(X+1)^2(X^2+1)\big).$$

   The elementary divisors are therefore

$$\begin{aligned} e_1 &= (X-1)(X+1)^2, \\ e_2 &= (X-1)(X+1)^2(X^2+1). \end{aligned}$$

3. Eine Untergruppe $H < G$, welche unter allen Automorphismen von G in sich übergeht, heisst eine *charakteristische Untergruppe von* G. (Vergleiche Aufgabe 1 von Serie 17.)

(a) Zeige, dass jede charakteristische Untergruppe normal ist.

(b) Zeige, dass das Zentrum jeder Gruppe eine charakteristische Untergruppe ist.

(c) Bestimme für jedes n die charakteristischen Untergruppen von S_n.

Lösung:

(a) Sei H eine charakteristische Untergruppe von G. Für jedes $g \in G$ ist dann int_g ein Automorphismus von G und somit ${}^gH = \mathrm{int}_g(H) = H$. Daher ist H normal.

(b) Ein Element $g \in G$ ist genau dann im Zentrum enthalten, wenn $hgh^{-1} = g$ für alle $h \in G$ gilt. Seien nun $g \in Z(G)$ und $\varphi \in \mathrm{Aut}(G)$. Für alle $h \in G$ setzen wir $i := \varphi^{-1}(h)$ und rechnen

$$h\varphi(g)h^{-1} \;=\; \varphi(i)\varphi(g)\varphi(i)^{-1} \;=\; \varphi(igi^{-1}) \;=\; \varphi(g).$$

Somit ist $\varphi(G) \in Z(G)$, woraus die Behauptung folgt.

(c) Nach (a) kommen nur normale Untergruppen in Frage. Im Fall $n \geqslant 5$ sind dies nach Satz 5.1.3 der Vorlesung genau die Untergruppen 1, A_n und S_n, und für $n \leqslant 4$ wissen wir, dass alleine die Kleinsche Vierergruppe $K = \langle (1\,2)(3\,4), (1\,3)(2\,4)\rangle \lhd S_4$ hinzukommt. Für jedes n haben diese Untergruppen, soweit sie verschieden sind, auch verschiedene Ordnung. Nun ist aber das Bild einer normalen Untergruppe unter jedem Automorphismus wieder eine normale Untergruppe derselben Ordnung. Jede der genannten normalen Untergruppen ist also gleich ihrem Bild unter jedem Automorphismus und daher charakteristisch.

4. Bestimme für jede Primzahl p die Ordnung der Automorphismengruppe der Gruppe $(\mathbb{Z}/p^2\mathbb{Z}) \boxplus (\mathbb{Z}/p\mathbb{Z})$.

Lösung: Die Gruppe $G := (\mathbb{Z}/p^2\mathbb{Z}) \boxplus (\mathbb{Z}/p\mathbb{Z})$ ist von den beiden Elementen $(1,0)$ und $(0,1)$ erzeugt. Jeder Automorphismus φ von G ist daher durch die Bilder $(a,b) := \varphi((1,0))$ und $(a',b') := \varphi((0,1))$ bestimmt. Dabei muss jedenfalls (a,b) wie $(1,0)$ ein Element der Ordnung p^2 sein, was äquivalent zu $p \nmid a$ ist. Ausserdem muss (a',b') wie $(0,1)$ ein Element der Ordnung p sein, was äquivalent zu $p|a'$ und $(a',b') \neq (0,0)$ ist. Weiter ist das Element $(0,1)$ nicht in der Untergruppe $\langle (1,0)\rangle$ enthalten, also auch (a',b') nicht in der Untergruppe $\langle (a,b)\rangle = \{(ca, cb) \mid c \in \mathbb{Z}\}$. Wegen $p \nmid a$ und $p|a'$ schliesst dies genau die Elemente $(pda, pdb) = (pda, 0)$ aus für alle $d \in \mathbb{Z}$. Wegen $p \nmid a$ sind dies aber auch genau die Elemente $(pe, 0)$ für alle $e \in \mathbb{Z}$. Insgesamt liefert das die Bedingungen $p \nmid a$ und $p|a'$ und $b' \neq 0$.

Betrachte umgekehrt beliebige (a,b) und $(a',b') \in G$ mit $p \nmid a$ und $p|a'$ und $b' \neq 0$. Dann existiert ein eindeutiger Homomorphismus $\varphi\colon G \to G$ mit $\varphi((1,0)) = (a,b)$ und $\varphi((0,1)) = (a',b')$, nämlich

$$\varphi\colon G \to G,\ (c,d) \mapsto (ca + da', cb + db').$$

Dieser bildet die zyklische Untergruppe $\langle(1,0)\rangle$ der Ordnung p^2 isomorph auf die Untergruppe $\langle(a,b)\rangle$ ab, und die zyklische Untergruppe $\langle(0,1)\rangle$ der Ordnung p isomorph auf die Untergruppe $\langle(a',b')\rangle$, welche nicht in $\langle(a,b)\rangle$ enthalten ist. Diese beiden Bilder erzeugen daher gemeinsam eine Untergruppe der Ordnung $> p^2$ und folglich nach Lagrange die ganze Gruppe G. Somit ist der Homomorphismus surjektiv, und daher bijektiv, also ein Isomorphismus.

Die Anzahl der Automorphismen von G ist also die Anzahl der Möglichkeiten für (a,b) und $(a',b') \in G$ mit $p \nmid a$ und $p|a'$ und $b' \neq 0$, das heisst gleich

$$\big(|\mathbb{Z}/p^2\mathbb{Z}| - |p\mathbb{Z}/p^2\mathbb{Z}|\big)\cdot|\mathbb{Z}/p\mathbb{Z}|\cdot|p\mathbb{Z}/p^2\mathbb{Z}|\cdot\big(|\mathbb{Z}/p\mathbb{Z}|-1\big) = (p^2-p)\cdot p\cdot p\cdot(p-1) = p^3(p-1)^2.$$

5. Betrachte Gruppen G und H. Beweise oder widerlege:

   (a) Besitzt sowohl G als auch H eine Kompositionsreihe, so auch $G \times H$.

   (b) Besitzt G eine Kompositionsreihe, so auch jede Faktorgruppe von G.

   (c) Besitzt G eine Kompositionsreihe, so auch jede Untergruppe von G.

   Lösung: Betrachte eine Kompositionsreihe $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_m = G$.

   (a) Nimm eine Kompositionsreihe $1 = H_0 \lhd H_1 \lhd \ldots \lhd H_n = H$. Dann gilt

   $$1 \;=\; G_0 \times 1 \;\lhd \ldots \lhd\; G_m \times 1 \;=\; G \times H_0 \;\lhd \ldots \lhd\; G \times H_n \;=\; G \times H$$

   mit den Subfaktoren $(G_i \times 1)/(G_{i-1} \times 1) \cong G_i/G_{i-1}$ und $(G \times H_j)/(G \times H_{j-1}) \cong H_j/H_{j-1}$, die nach Voraussetzung einfache Gruppen sind. Somit haben wir eine Kompositionsreihe von $G \times H$.

   (b) Für jeden Normalteiler $N \lhd G$ ist nach Proposition 5.2.3 (b) der Vorlesung

   $$1 \;=\; G_0N/N \;\lhd\; G_1N/N \;\lhd \ldots \lhd\; G_mN/N \;=\; G/N$$

   eine Subnormalreihe von G/N, deren Subfaktoren Faktorgruppen der Subfaktoren G_i/G_{i-1} sind. Da die Gruppen G_i/G_{i-1} einfach sind, ist jede Faktorgruppe davon trivial oder isomorph dazu und daher wieder einfach. Durch Weglassen der Schritte mit trivialer Faktorgruppe erhalten wir also eine Kompositionsreihe von G/N.

   (c) Diese Aussage gilt im Allgemeinen nicht. Da jede endliche Gruppe eine Kompositionsreihe hat, brauchen wir als Gegenbeispiel eine unendliche Gruppe. In §5.1 der Vorlesung haben wir gesehen, dass die Gruppe $G := \mathrm{PSL}(2,\mathbb{Q})$ einfach ist; insbesondere besitzt sie also die Kompositionsreihe $1 \lhd G$. Dagegen besitzt $\mathbb{Z}$ keine Kompositionsreihe. Das Bild des injektiven Homomorphismus $\mathbb{Z} \hookrightarrow \mathrm{PSL}(2,\mathbb{Q})$, $n \mapsto \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$ ist also ein Gegenbeispiel.

6. Eine Gruppe G mit der Eigenschaft $[G,G] = G$ heisst *perfekt*. Zeige für alle $N \lhd G$:

   (a) Ist G perfekt, so auch G/N.

   (b) Sind N und G/N perfekt, so auch G.

   (c) Jede endliche Gruppe ist in einer perfekten Gruppe enthalten.

   Lösung: (a) Die Kommutatoren von Elementen in G/N sind genau die Bilder der Kommutatoren von Elementen in G. Ist G perfekt, so erzeugen die letzteren die Gruppe G, also die ersteren die Gruppe G/N; daher ist G/N perfekt.

   (b) Nach Konstruktion gilt $[N,N] < [G,G]$; da N perfekt ist, also $N < [G,G]$. Aus demselben Grund wie in (a) ist nun $[G,G]/N = [G/N, G/N]$. Da G/N perfekt ist, ist dieses gleich G/N. Somit ist $[G,G] = G$, also G perfekt.

   (c) Nach Cayley liefert die Operation von G auf sich durch Linkstranslation eine Einbettung von G in die symmetrische Gruppe $S(G) \cong S_{|G|}$. Nach Serie 4, Aufgabe 1 existiert eine weitere Einbettung $S_{|G|} \hookrightarrow A_{|G|+2}$. Lassen wir die $A_{|G|+2}$ auf den Ziffern $|G|+3$ bis $|G|+5$ trivial operieren, so liefert dies eine dritte Einbettung $A_{|G|+2} \hookrightarrow A_{|G|+5}$. Wegen $|G|+5 \geqslant 5$ ist nun $A_{|G|+5}$ nichtabelsch einfach und somit perfekt. Die Komposition der genannten Einbettungen liefert dann eine Einbettung $G \hookrightarrow A_{|G|+5}$ mit der gesuchten Eigenschaft.

7. Beweise oder widerlege:

   (a) Jede Gruppe der Ordnung 35 ist abelsch.

   (b) Jede Gruppe der Ordnung 55 ist abelsch.

   (c) Es existiert eine einfache Gruppe der Ordnung 1365.

   Lösung: Für $|G| = 5 \cdot 7$ implizieren die Sylowsätze $|\operatorname{Syl}_5(G)| = |\operatorname{Syl}_7(G)| = 1$; somit hat G eine normale 5-Sylowgruppe der Ordnung 5 und eine normale 7-Sylowgruppe der Ordnung 7, ist also das direkte Produkt dieser beiden und daher abelsch. Also gilt (a).

   Weiter gilt $|\mathbb{F}_{11}^\times| = 10$; somit besitzt $\mathbb{F}_{11}^\times$ ein Element der Ordnung 5, und daher existiert ein nicht-trivialer Homomorphismus $Z_5 \to \mathbb{F}_{11}^\times$. Das entsprechende semidirekte Produkt $Z_{11} \rtimes Z_5$ ist dann nicht-abelsch der Ordnung 55, also ist (b) falsch.

   Nehme an, es existierte eine einfache Gruppe G mit $|G| = 1365 = 3 \cdot 5 \cdot 7 \cdot 13$.

   Dann folgte aus den Sylowsätzen $|\operatorname{Syl}_3(G)| = 1 \mod 3$ und $|\operatorname{Syl}_3(G)| \mid 455$. Aus der Einfachheit von G erhielten wir ausserdem $|\operatorname{Syl}_3(G)| > 1$ und somit ist $|\operatorname{Syl}_3(G)| \in \{7, 13, 91\}$, da dies die einzigen nichttrivialen Teiler von 455 sind, die Modulo 3 gleich 1 sind.

   Genauso folgten $|\operatorname{Syl}_5(G)| \in \{1, 21, 91\}$ und $|\operatorname{Syl}_7(G)| = 15$ und $|\operatorname{Syl}_{13}(G)| = 105$. Jedes nicht-triviale Element in einer p-Sylowgruppe erzeugt jene Gruppe und hat

somit Ordnung p. Sodann gäbe es mindestens $2\dot{7} = 14$ Elemente der Ordnung 3, mindestens $4 \cdot 21 = 84$ Elemente der Ordnung 5, genau $6 \cdot 15 = 90$ Elemente der Ordnung 7 und genau $12 * 105 = 1260$ Elemente der Ordnung 13.

Also gäbe es mindestens $1 + 14 + 84 + 90 + 1260 = 1449$ unterschiedliche Elemente, ein Widerspruch zu $|G| = 1365 < 1449$.

8. Sei G eine Gruppe und P eine p-Sylowuntergruppe von G. Zeige für beliebige Untergruppen H von G:

$$\mathrm{Norm}_G(P) < H \implies H = \mathrm{Norm}_G(H).$$

Lösung: Sei $H < G$ eine Untergruppe mit $\mathrm{Norm}_G(P) < H$. Die Inklusion $H \subset \mathrm{Norm}_G(H)$ gilt bereits nach Konstruktion. Für die Umkehrung betrachte ein beliebiges $x \in \mathrm{Norm}_G(H)$. Wegen $P < \mathrm{Norm}_G(P) < H$ gilt dann

$$xPx^{-1} < xHx^{-1} = H.$$

Nun ist $|P| = |xPx^{-1}|$ die maximale p-Potenz in $|G|$, also a fortiori auch in dessen Teiler $|H|$. Somit sind P und xPx^{-1} beides p-Sylowuntergruppen von H. Nach den Sylowsätzen existiert deshalb ein $h \in H$ mit

$$P = hxPx^{-1}h^{-1}.$$

Somit liegt hx in $\mathrm{Norm}_G(P)$, also nach Voraussetzung in H, und es folgt $x = h^{-1}(hx) \in H$. Daher gilt die umgekehrte Inklusion $H \supset \mathrm{Norm}_G(H)$.

9. Sei G eine nilpotente endliche Gruppe. Zeige:

   (a) Jede echte Untergruppe $H \subsetneqq G$ ist echt in ihrem Normalisator $\mathrm{Norm}_G(H)$ enthalten.

   (b) Jede Sylowuntergruppe von G ist normal in G.

   (c) Die Gruppe G ist das innere direkte Produkt ihrer Sylowuntergruppen.

   Lösung:

   (a) Da G nilpotent ist, wird ihre aufsteigende Zentralreihe $\{1\} = Z_0 \lhd Z_1 \lhd \ldots$ stationär mit $Z_n = G$ für ein n. Daher existiert ein Index $k \geqslant 0$ mit $Z_k < H$ und $Z_{k+1} \not< H$. Nach der Definition der aufsteigenden Zentralreihe ist nun Z_{k+1}/Z_k das Zentrum von G/Z_k. Für alle $z \in Z_{k+1}$ und $h \in H$ kommutieren dann die Nebenklassen zZ_k, $hZ_k \in G/Z_k$, also gilt $zhz^{-1}Z_k = hZ_k$. Wegen $Z_k < H$ impliziert dies $zhz^{-1} \in H$, und durch Variieren von $h \in H$ folgt $zHz^{-1} \subset H$. Da dasselbe auch für z^{-1} anstelle von z gilt, folgt sogar $zHz^{-1} = H$. Variieren von z zeigt nun, dass Z_{k+1} im Normalisator $\mathrm{Norm}_G(H)$ enthalten ist. Wegen $Z_{k+1} \not< H$ ist dieser Normalisator also echt grösser als H.

(b) Sei P eine p-Sylowgruppe von G, und setze $H := \mathrm{Norm}_G(P)$. Nach der obigen Aufgabe 6 gilt dann $\mathrm{Norm}_G(H) = H$. Nach (a) folgt daraus $H = G$; somit ist P normal in G.

(c) Für jeden Primteiler von $n := |G|$ sei S_p die nach (b) normale p-Sylowgruppe von G. Für je zwei verschiedene Primteiler p und q ist dann $|S_p \cap S_q|$ ein Teiler von $|S_p|$ und von $|S_q|$ und daher gleich 1. Somit ist $S_p \cap S_q = 1$. Wegen $S_p \trianglelefteq G$ und $S_q \trianglelefteq G$ ist nun aber der Kommutator jedes Elements von S_p mit jedem Element von S_q sowohl in S_p als auch in S_q enthalten. Also muss dieser Kommutator gleich 1 sein, mit anderen Worten: Jedes Element von S_p kommutiert mit jedem Element von S_q. Daher ist die Abbildung

$$\bigtimes_{p|n} S_p \to G,\ (g_p)_p \mapsto \prod_p g_p$$

unabhängig von der Reihenfolge der Multiplikation und ein Homomorphismus. Ausserdem ist ihr Bild N als Produkt von Normalteilern ein Normalteiler von G.

Wäre nun N nicht gleich G, so gäbe es in G/N ein Element gN von Primzahlordnung p. Die von g erzeugte Untergruppe hat dann eine Ordnung m mit $p|m$. Schreibe $m = p^k m'$ mit $p \nmid m'$. Dann ist m' invertierbar modulo p und folglich auch $g^{m'}N \neq 1$ in G/N. Nun ist aber $g^{m'}$ ein Element von p-Potenzordnung und daher in einer p-Sylowgruppe von G enthalten. Somit ist $g^{m'} \in S_p < N$, und wir haben einen Widerspruch. Also ist $N = G$ und der obige Homomorphismus surjektiv.

Nach der Definition von p-Sylowgruppen gilt schliesslich $\prod_{p|n} |S_p| = |G|$. Da der Homomorphismus surjektiv ist, muss er folglich schon bijektiv sein, und alles ist gezeigt.

10. Sei $n \geqslant 3$ ungerade. Finde alle Isomorphieklassen von Gruppen G mit den Eigenschaften

(a) $|G| = 2n$ und

(b) G enthält eine zyklische Untergruppe H der Ordnung n.

Hinweis: Zeige, dass G ein semidirektes Produkt von H mit einer Untergruppe C der Ordnung 2 ist. Beschreibe die möglichen Homomorphismen $C \to \mathrm{Aut}(H)$ und zeige, dass die entsprechenden semidirekten Produkte nicht isomorph sind.

Lösung: Setze $X := \{x \in (\mathbb{Z}/n\mathbb{Z})^\times \mid x^2 = 1\}$. Dann sind die Homomorphismen $\mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ genau die Abbildungen der Form $a \mapsto x^a$ für alle $x \in X$. Zu jedem solchen x assoziieren wir das semidirekte Produkt

$$G_x := \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$$

mit der entsprechenden Operation. Dies ist eine Gruppe mit den gewünschten Eigenschaften. Wir behaupten, dass jede Gruppe mit den genannten Eigenschaften isomorph zu G_x ist für ein eindeutiges $x \in X$.

Sei also G eine Gruppe mit den genannten Eigenschaften. Da $|G| = 2n$ ist mit n ungerade, hat G nach dem ersten Sylow-Satz eine Untergruppe C mit $|C| = 2$. Da die Ordnungen von H und C teilerfremd sind, gilt $H \cap C = \{1_G\}$. Die Gruppe H hat Index 2 in G, also ist sie ein Normalteiler von G, und somit ist $HC \subset G$ eine Untergruppe. Deren Ordnung ist durch 2 und durch n teilbar, also ist sie gleich $2n$ und es gilt $HC = G$. Daraus folgt, dass G ein inneres semidirektes Produkt von H mit C ist. Somit ist $G \cong H \rtimes C \cong G_x$ für ein $x \in X$.

Es bleibt zu zeigen, dass $G_x \ncong G_{x'}$ ist für alle $x \neq x'$. Dafür beweisen und verwenden wir den folgenden Satz:

Satz: Ist G eine endliche Gruppe der Ordnung nk mit $\mathrm{ggT}(n,k) = 1$, und ist $N \lhd G$ ein Normalteiler der Ordnung n, so hat G ausser N keine Untergruppe der Ordnung n.

Beweis: Sei $H < G$ eine beliebige Untergruppe der Ordnung n. Nach dem zweiten Isomorphiesatz ist dann HN eine Untergruppe von G mit $HN/N \cong H/(H \cap N)$. Nach Lagrange ist $|H/(H \cap N)|$ ein Teiler von $|H| = n$. Also ist auch $|HN/N|$ ein Teiler von n. Dies ist aber auch ein Teiler von $|G/N| = k$. Die Voraussetzung $\mathrm{ggT}(n,k) = 1$ impliziert also $|HN/N| = 1$. Somit ist $HN = N$ und $H \subset N$, und aus Kardinalitätsgründen deshalb $H = N$. □

Betrachte nun $x, x' \in X$ und einen Isomorphismus $f\colon G_x \xrightarrow{\sim} G_{x'}$. Das Bild der Untergruppe $\mathbb{Z}/n\mathbb{Z} < G_x$ unter f ist dann eine Untergruppe von $G_{x'}$ der Ordnung n, also nach obigem Satz gleich $\mathbb{Z}/n\mathbb{Z} < G_{x'}$. Somit induziert f einen Isomorphismus $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z}$. Dieser ist gegeben durch $a \mapsto ka$ für ein $k \in (\mathbb{Z}/n\mathbb{Z})^\times$. Sei andererseits h das nichttriviale Element von $\mathbb{Z}/2\mathbb{Z}$ als Element von G_x oder $G_{x'}$. Wegen $f(\mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$ gilt dann $f(h) = hu$ für ein $u \in \mathbb{Z}/n\mathbb{Z}$. Für jedes $a \in C_n$ gilt dann ${}^u(ka) = ka$ und somit

$$kxa \overset{\text{in } G_x}{=} f(xa) = f({}^h a) = {}^{f(h)} f(a) = {}^{hu}(ka) = {}^h(ka) \overset{\text{in } G_{x'}}{=} x'ka.$$

Wegen $k \in (\mathbb{Z}/n\mathbb{Z})^\times$, und da $a \in \mathbb{Z}/n\mathbb{Z}$ beliebig ist, folgt daraus $x = x'$. Also ist $G_x \cong G_{x'}$ genau dann, wenn $x = x'$ ist, wie gewünscht.

11. Sei p eine Primzahl. Gibt es eine nicht-abelsche Gruppe der Ordnung p^4 ...

    (a) mit einem Element der Ordnung p^4?

    (b) mit einem Element der Ordnung p^3, aber ohne ein Element der Ordnung p^4?

    (c) mit einem Element der Ordnung p^2, aber ohne ein Element der Ordnung p^3?

    (d) ohne ein Element der Ordnung p^2?

Lösung:

(a) Nein, denn jedes Element der Ordnung p^4 erzeugt die ganze Gruppe; diese ist also zyklisch und daher abelsch.

(b) Ja, nämlich das semidirekte Produkt $(\mathbb{Z}/p^3\mathbb{Z}) \rtimes (\mathbb{Z}/p\mathbb{Z})$, bei dem die Operation von $\mathbb{Z}/p\mathbb{Z}$ auf $\mathbb{Z}/p^3\mathbb{Z}$ gegeben ist durch den Homomorphismus

$$\mathbb{Z}/p\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{Z}/p^3\mathbb{Z}) = (\mathbb{Z}/p^3\mathbb{Z})^\times, \quad [a] \mapsto [1 + ap^2].$$

Man rechnet direkt nach, dass dies ein nicht-trivialer Homomorphismus ist. Also ist das semidirekte Produkt nicht-abelsch und besitzt ein Element der Ordnung p^3 und wegen (a) keines der Ordnung p^4.

(c) Ja: In der Vorlesung haben wir gesehen, dass es eine nicht-abelsche Gruppe G der Ordnung p^3 gibt mit einem Element der Ordnung p^2 und ohne ein Element der Ordnung p^3. Dann hat die Gruppe $G \times Z_p$ die gesuchten Eigenschaften.

(d) Für p ungerade haben wir in der Vorlesung gesehen, dass es eine nicht-abelsche Gruppe G der Ordnung p^3 gibt ohne ein Element der Ordnung p^2. Dann hat die Gruppe $G \times Z_p$ die gesuchten Eigenschaften. Für $p = 2$ hätte eine solche Gruppe aber den Exponenten 2 und wäre folglich abelsch nach Proposition 1.4.11 der Vorlesung. Die Antwort lautet daher ja für p ungerade und nein für $p = 2$.

12. Gibt es eine nicht-abelsche endliche Gruppe der Ordnung 15, 25, 35, 45, 55, 65, 75, 85, beziehungsweise 95?

Lösung: Nach der Lösung der Aufgabe 3 von Serie 18 existiert für je zwei Primzahlen $p < q$ eine nicht-abelsche Gruppe der Ordnung pq genau dann, wenn $q \equiv 1 \bmod p$ ist. Daher existiert eine der Ordnung $5 \cdot 11$, aber keine der Ordnung $3 \cdot 5$ oder $5 \cdot 7$ oder $5 \cdot 13$ oder $5 \cdot 17$ oder $5 \cdot 19$.

Weiter existiert keine nicht-abelsche Gruppe der Ordnung p^2 für eine Primzahl p, also auch keine der Ordnung 5^2.

Für $|G| = 45 = 3^2 \cdot 5$ folgt aus den Sylowsätzen, dass die Anzahl der 3-Sylowgruppen und die Anzahl der 5-Sylowsätzen gleich 1 ist. Ausserdem sind diese Untergruppen als Gruppen der Ordnung 3^2 beziehungsweise 5 abelsch. Somit ist G das direkte Produkt dieser abelschen Gruppen und daher abelsch.

Schliesslich ist $|\mathrm{Aut}(\mathbb{F}_5^2)| = |\mathrm{GL}_2(\mathbb{F}_5)| = (5^2 - 1) \cdot (5^2 - 5) = 24 \cdot 20$ ein Vielfaches von 3. Daher besitzt $\mathrm{Aut}(\mathbb{F}_5^2)$ ein Element der Ordnung 3, und somit existiert ein nicht-trivialer Homomorphismus $Z_3 \to \mathrm{Aut}(\mathbb{F}_5^2)$. Das mit der zugehörigen Operation von Z_3 auf $\mathbb{F}_5^2$ gebildete semidirekte Produkt $\mathbb{F}_5^2 \rtimes Z_3$ ist daher eine nicht-abelsche Gruppe der Ordnung $3 \cdot 5^2 = 75$.

Insgesamt existiert also eine nicht-abelsche endliche Gruppe der Ordnung 55 beziehungsweise 75, aber keine für die übrigen Ordnungen.

13. Der *Satz von Wilson* besagt, dass für jede Primzahl p gilt $(p-1)! \equiv -1 \bmod (p)$. Beweise dies vermittels einer Rechnung in $\mathbb{F}_p^\times$.

Lösung: Für $p = 2$ ist die Aussage offensichtlich. Sei also p ungerade. Dann ist $\mathbb{F}_p^\times$ eine zyklische Gruppe gerader Ordnung $p-1$. Darin sind 1 und -1 gleich ihrem Inversen, und alle übrigen Elemente tauchen als Paare mit ihren Inversen auf. Das Produkt über alle Elemente von $\mathbb{F}_p^\times$ ist folglich gleich $1 \cdot (-1)$ mal ein Produkt von gewissen $\alpha \cdot \alpha^{-1}$, also insgesamt gleich -1. Somit gilt $\prod_{i=1}^{p-1} i \equiv -1$ modulo (p).

14. Zeige: Für jede Primpotenz $p^n \geqslant 3$ ist

$$(\mathbb{Z}/p^n\mathbb{Z})^\times \;\cong\; \begin{cases} Z_{p-1} \times Z_{p^{n-1}} & \text{im Fall } p > 2, \\ Z_p \times Z_{p^{n-2}} & \text{im Fall } p = 2 \text{ und } n \geqslant 2. \end{cases}$$

Lösung: Zuerst sei $p > 2$. Dann ist $(\mathbb{Z}/p^n\mathbb{Z})^\times$ eine abelsche Gruppe der Ordnung $\varphi(p^n) = (p-1)p^{n-1}$. Da $p-1$ und p^{n-1} zueinander teilerfremd sind, ist sie also das direkte Produkt einer abelschen Gruppe G der Ordnung $p-1$ mit einer abelschen Gruppe H der Ordnung p^{n-1}. Andererseits haben wir einen natürlichen surjektiven Homomorphismus

$$\pi\colon (\mathbb{Z}/p^n\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/p\mathbb{Z})^\times, \quad a + p^n\mathbb{Z} \mapsto a + p\mathbb{Z}.$$

Dessen Zielbereich $\mathbb{F}_p^\times$ ist eine zyklische Grupe der Ordnung $p-1$. Somit ist $\mathrm{Kern}(\pi)$ eine Untergruppe der Ordnung p^{n-1} und daher gleich H. Ausserdem bildet π den anderen Faktor G isomorph auf $\mathbb{F}_p^\times$ ab; daher ist $G \cong Z_{p-1}$.

Nun untersuchen wir H. Für $n = 1$ ist $H = 1$ und nichts zu zeigen; sei also $n \geqslant 2$. Betrachte eine ganze Zahl der Form $a = 1 + p^i b$ mit $i \geqslant 1$ und $p \nmid b$. Dann ist

$$a^p \;=\; (1 + p^i b)^p \;=\; \sum_{j=0}^{p} \binom{p}{j} p^{ij} b^j.$$

Für jedes $0 < j < p$ ist $p \mid \binom{p}{j}$ und $ij \geqslant i + 1$ und folglich $\binom{p}{j} p^{ij} b^j \equiv 0 \bmod (p^{i+2})$. Wegen $p > 2$ ist ausserdem $\binom{p}{p} p^{ip} b^p \equiv 0 \bmod (p^{i+2})$. Somit ist

$$a^p \;\equiv\; 1 + p^{i+1} b \;\bmod\; (p^{i+2}).$$

Für jedes $1 \neq a \in 1 + p\mathbb{Z}$ ist also $\mathrm{ord}_p(a^p - 1) = \mathrm{ord}_p(a-1) + 1$. Durch Induktion folgt daraus $\mathrm{ord}_p(a^{p^r} - 1) = \mathrm{ord}_p(a-1) + r$ für alle $r \geqslant 0$. Für $a = 1 + p$ und $r = n - 2$ gilt also insbesondere $\mathrm{ord}_p(a^{p^{n-2}} - 1) = \mathrm{ord}_p(a-1) + n - 2 = n - 1$ und somit $a^{p^{n-2}} \not\equiv 1 \bmod (p^n)$. Die Restklasse $\bar{a}$ von a ist damit ein Element von H mit $\bar{a}^{p^{n-2}} \neq \bar{1}$. Da H die Ordnung p^{n-1} hat, ist $\bar{a}$ somit ein Element der Ordnung p^{n-1} und erzeugt H. Insbesondere ist H zyklisch der Ordnung p^{n-1} und wir sind fertig im Fall $p > 2$.

Im Fall $p = 2$ nehmen wir $n \geqslant 2$ an und betrachten den natürlichen surjektiven Homomorphismus

$$\pi\colon (\mathbb{Z}/2^n\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/4\mathbb{Z})^\times, \quad a + 2^n\mathbb{Z} \mapsto a + 4\mathbb{Z}.$$

Dessen Kern H ist die Untergruppe aller Restklassen in $1 + 4\mathbb{Z}$ und hat Ordnung 2^{n-2}. Ausserdem bildet π die Untergruppe $\{\pm\bar{1}\}$ isomorph auf $(\mathbb{Z}/4\mathbb{Z})^\times$ ab; somit ist $(\mathbb{Z}/2^n\mathbb{Z})^\times \cong \{\pm\bar{1}\} \times H$.

Um H zu untersuchen, betrachte eine ganze Zahl der Form $a = 1 + 2^i b$ mit $i \geqslant 2$ und $2 \nmid b$. Dann ist

$$a^2 \;=\; (1 + 2^i b)^2 \;=\; 1 + 2^{i+1}b + 2^{2i}b^2 \;\equiv\; 1 + 2^{i+1}b \mod (2^{i+2})$$

wegen $i \geqslant 2$. Wie oben folgt daraus $\operatorname{ord}_2(a^{2^r} - 1) = \operatorname{ord}_2(a - 1) + r$ für alle $1 \neq a \in 1 + 4\mathbb{Z}$ und $r \geqslant 0$. Für $a = 1 + 4$ und $r = n - 3$ gilt also insbesondere $\operatorname{ord}_2(a^{2^{n-3}} - 1) = \operatorname{ord}_2(a - 1) + n - 3 = n - 1$ und somit $a^{2^{n-3}} \not\equiv 1 \bmod (2^n)$. Die Restklasse $\bar{a}$ von a ist damit ein Element von H mit $\bar{a}^{2^{n-3}} \neq \bar{1}$. Da H die Ordnung 2^{n-2} hat, ist $\bar{a}$ somit ein Element der Ordnung 2^{n-2} und erzeugt H. Insbesondere ist H zyklisch der Ordnung 2^{n-2} und wir sind fertig im Fall $p > 2$.

15. Zeige: Für endliche Körper k und ℓ existiert ein Homomorphismus $k \to \ell$ genau dann, wenn $|\ell|$ eine Potenz von $|k|$ ist.

Lösung: Wenn ein Homomorphismus $k \to \ell$ existiert, macht dieser ℓ zu einem endlich dimensionalen k-Vektorraum. Ist dessen Dimension n, so ist ℓ als k-Vektorraum isomorph zu k^n; also folgt $|\ell| = |k^n| = |k|^n$.

Sei umgekehrt $|\ell| = |k|^n$, und sei $p := \operatorname{char}(k)$. Laut Satz 6.7.1 der Vorlesung ist k ein Zerfällungskörper des Polynoms $X^{|k|} - X$ über $\mathbb{F}_p$. Analog ist ℓ ein Zerfällungskörper des Polynoms $X^{|\ell|} - X = X^{|k|^n} - X$ über $\mathbb{F}_p$. Aber

$$\frac{X^{|k|^n} - X}{X^{|k|} - X} = \frac{(X^{|k|-1})^{\frac{|k|^n-1}{|k|-1}} - 1}{X^{|k|-1} - 1}$$

ist eine endliche geometrische Summe, also ein Polynom; folglich ist $X^{|k|} - X$ ein Teiler von $X^{|k|^n} - X$. Damit enthält ℓ einen Zerfällungskörper von $X^{|k|} - X$ über $\mathbb{F}_p$, und da Zerfällungskörper eindeutig bis auf Isomorphie sind, ist dieser Unterkörper isomorph zu k. Dieser Isomorphismus liefert den gesuchten Homomorphismus.

Aliter: Sei $\overline{\ell}$ ein algebraischer Abschluss von ℓ. Da $k/\mathbb{F}_p$ algebraisch ist, existiert eine Einbettung $k \hookrightarrow \overline{\ell}$; ohne Beschränkung der Allgemeinheit sei also $k \subset \overline{\ell}$. Da $|k|$ eine Potenz von p ist, ist $\operatorname{Frob}_{|k|}$ ein Körperautomorphismus von $\overline{\ell}$, und k sein Fixkörper. Aus dem gleichen Grund ist ℓ der Fixkörper von $\operatorname{Frob}_{|\ell|}$ in $\overline{\ell}$. Im Fall $|\ell| = |k|^n$ ist aber $\operatorname{Frob}_{|\ell|} = \operatorname{Frob}_{|k|}^n$; also wird jedes von $\operatorname{Frob}_{|k|}$ festgelassene Element von $\overline{\ell}$ auch von $\operatorname{Frob}_{|\ell|}$ festgelassen. Somit gilt $k \subset \ell$.

16. Zeige: Jede Körpererweiterung von $\mathbb{Q}$ vom Transzendenzgrad $\leqslant |\mathbb{R}|$ ist isomorph zu einem Unterkörper von $\mathbb{C}$.

Lösung: Sei $K/\mathbb{Q}$ eine Körpererweiterung vom Transzendenzgrad $\leqslant |\mathbb{R}|$ mit Transzendenzbasis $\{x_i\}_{i\in I}$. Sei andererseits $\{y_j\}_{j\in J}$ eine Transzendenzbasis von $\mathbb{R}/\mathbb{Q}$. Nach Beispiel 6.1.9 der Vorlesung ist dann $|J| = |\mathbb{R}|$; also existiert eine injektive Abbildung $\kappa\colon I \hookrightarrow J$. Aufgrund der universellen Eigenschaft des Polynomrings existiert ein eindeutiger Ringhomomorphismus $\varphi\colon \mathbb{Q}[\{x_i\}_{i\in I}] \to \mathbb{R}$ mit $x_i \mapsto y_{\kappa(i)}$ für alle $i \in I$. Da κ injektiv ist, sind die $y_{\kappa(i)}$ algebraisch unabhängig über $\mathbb{Q}$ und folglich ist φ injektiv. Es setzt sich somit fort zu einem eindeutigen Körperhomomorphismus $\varphi\colon \mathbb{Q}(\{x_i\}_{i\in I}) \to \mathbb{R}$. Da $K/\mathbb{Q}(\{x_i\}_{i\in I})$ algebraisch und $\mathbb{C}$ algebraisch abgeschlossen ist, lässt sich dieser nach Satz 6.2.8 der Vorlesung zu einem Homomorphismus $K \to \mathbb{C}$ fortsetzen. Dieser ist ein Isomorphismus von K auf einen Unterkörper von $\mathbb{C}$.

17. Finde alle Körperhomomorphismen $K := \mathbb{Q}(\sqrt[4]{2}, e^{\frac{\pi i}{4}}) \to \mathbb{C}$. Ist $K/\mathbb{Q}$ normal?

Lösung: Nach dem Eisensteinkriterium mit $p = 2$ ist das Polynom $X^4 - 2$ irreduzibel über $\mathbb{Q}$ und daher $[\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}] = 4$. Wegen $e^{\frac{\pi i}{4}} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} = (\sqrt[4]{2})^2 \cdot \frac{1+i}{2}$ gilt weiter $K := \mathbb{Q}(\sqrt[4]{2}, e^{\frac{\pi i}{4}}) = \mathbb{Q}(\sqrt[4]{2}, i)$. Wegen $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R} \not\ni i$ ist ausserdem $[K/\mathbb{Q}(\sqrt[4]{2})] = 2$ und somit $[K/\mathbb{Q}] = 8$. Da $\mathbb{C}$ algebraisch abgeschlossen ist, folgt daraus $|\operatorname{Hom}(\mathbb{Q}(\sqrt[4]{2}, i), \mathbb{C})| = 8$.

Die Minimalpolynome von $\sqrt[4]{2}$ und i über $\mathbb{Q}$ sind respektive $X^4 - 2$ und $X^2 + 1$. Jeder Körperhomomorphismus $K \to \mathbb{C}$ muss $\sqrt[4]{2}$ und i auf Nullstellen dieser jeweiligen Minimalpolynome abbilden. Für $\sqrt[4]{2}$ gibt es dafür die 4 Möglichkeiten $\pm\sqrt[4]{2}$ und $\pm i\sqrt[4]{2}$, und für i die 2 Möglichkeiten $\pm i$. Insgesamt ergibt dies $4 \cdot 2 = 8$ Möglichkeiten. Wegen $|\operatorname{Hom}(\mathbb{Q}(\sqrt[4]{2}, i), \mathbb{C})| = 8$ muss jede dieser Möglichkeiten einem Homomorphismus $K \to \mathbb{C}$ entsprechen.

Schliesslich ist $K = \mathbb{Q}(\sqrt[4]{2}, i) = K(\pm\sqrt[4]{2}, \pm i\sqrt[4]{2})$ ein Zerfällungskörper des Polynoms $X^4 - 2$ über $\mathbb{Q}$ und daher normal über $\mathbb{Q}$.

18. Wann ist eine Körpererweiterung vom Grad 2 inseparabel?

Lösung: Jede Körpererweiterung vom Grad 2 hat die Form $L = K(a)/K$ für ein Element a mit einem Minimalpolynom der Form $X^2 + bX + c$ über K. Ein solches irreduzibles Polynom ist genau dann inseparabel, wenn $\operatorname{char}(K) = 2$ und $b = 0$ ist. Also ist eine Körpererweiterung vom Grad 2 genau dann inseparabel, wenn sie eine Radikalerweiterung vom Grad 2 eines Körpers der Charakteristik 2 ist.

19. Sei H die Gruppe aller Automorphismen von $\mathbb{C}(X)$ der Form $f(X) \mapsto f(X + a)$ für alle $a \in \mathbb{C}$. Bestimme den Fixkörper $\mathbb{C}(X)^H$.

Lösung: Betrachte ein Element $f \in \mathbb{C}(X)^H \smallsetminus \{0\}$ und schreibe es in der Form $f = g/h$ für teilerfremde $g, h \in \mathbb{C}[X] \smallsetminus \{0\}$. Für jedes a gilt dann

$$\frac{g(X)}{h(X)} = \frac{g(X+a)}{h(X+a)}.$$

Da auch $g(X+a)$ und $h(X+a)$ teilerfremd sind, ist dies nur möglich mit $g(X+a) = \lambda g(X)$ für ein $\lambda \in \mathbb{C}^\times$. Vergleich der höchsten Koeffizienten impliziert dann $\lambda = 1$. Also gilt $g(X+a) = g(X)$. Für jede Nullstelle $z \in \mathbb{C}$ von g ist dann auch $z+a$ eine Nullstelle. Da a beliebig ist, aber g nur endlich viele Nullstellen haben kann, ist dies nur möglich, wenn g konstant ist. Dasselbe Argument für h zeigt, dass h und folglich auch f konstant ist. Umgekehrt sind alle Konstanten in $\mathbb{C}$ offenbar invariant unter H. Folglich ist der Fixkörper $\mathbb{C}(X)^H = \mathbb{C}$.

Aliter: Wäre der Fixkörper nicht $\mathbb{C}$, so enthielte er ein transzendentes Element, und $\mathbb{C}(X)$ wäre endlich darüber. Dann wäre aber $|H| \leqslant |\operatorname{Aut}_{\mathbb{C}(X)^H}(\mathbb{C}(X))| \leqslant [\mathbb{C}(X)/\mathbb{C}(X)^H] < \infty$. Widerspruch.

20. Finde ein primitives Element eines Zerfällungskörpers des Polynoms X^3-7 über $\mathbb{Q}$.

Lösung: Das Polynom hat die drei verschiedenen Nullstellen $a := \sqrt[3]{7}$ sowie ζa und $\zeta^2 a$ für $\zeta := \frac{-1+\sqrt{3}\,i}{2}$ und ist daher separabel. Egal, was seine Galoisgruppe genau ist (man sieht unschwer, dass dies die S_3 ist), operiert jedes Element σ davon durch Vertauschung dieser Nullstellen, also durch $\sigma(a) = \zeta^r a$ und $\sigma(\zeta) = \zeta^s$ für $r \in \{0,1,2\}$ und $s \in \{1,2\}$. Wird nun $a+\zeta$ von σ festgelassen, so gilt $\zeta^r a + \zeta^s = a + \zeta$ und folglich $(\zeta^r - 1)a = \zeta - \zeta^s$. Im Fall $s = 1$ folgt daraus $\zeta^r - 1 = 0$ und folglich $r = 0$ und daher $\sigma = \mathrm{id}$. Im Fall $s = 2$ ist dagegen $|\zeta - \zeta^s| = \sqrt{3} \neq 0$ und daher $\zeta^r - 1 \neq 0$. Dann ist aber auch $|\zeta^r - 1| = \sqrt{3}$ und es folgt $|a| = 1$, im Widerspruch zu $a = \sqrt[3]{7}$. Somit wird das Element $a + \zeta$ von keinem nichttrivialen Element der Galoisgruppe festgelassen, liegt also in keinem echten Unterkörper des Zerfällungskörpers, und ist daher ein primitives Element.

21. Beschreibe, wie man ein primitives Element eines Zerfällungskörpers eines beliebigen Polynoms f vom Grad 3 über K findet.

Lösung: Sei $\bar{K}$ ein algebraischer Abschluss von K. Hat f eine dreifache Nullstelle in K, so erzeugt diese bereits einen Zerfällungskörper, ist also ein primitives Element.

Hat f zwei Nullstellen $a, b \in \bar{K}$ der Vielfachheiten 2 und 1, so geschieht Folgendes: Ohne Beschränkung der Allgemeinheit ist f normiert, also gleich $(X-a)^2(X-b)$. Seine Ableitung ist dann $f' = 2(X-a)(X-b) + (X-a)^2$. Im Fall $\mathrm{char}(K) = 2$ ist also $f' = (X-a)^2$ und daher $\mathrm{ggT}(f, f') = (X-a)^2$. Dieser grösste gemeinsame Teiler liegt schon in $K[X]$; also erzeugt a höchstens eine quadratische Erweiterung von K, und die letzte Nullstelle liegt bereits in K. In diesem Fall ist a ein primitives Element. Im Fall $\mathrm{char}(K) \neq 2$ ist a nur eine einfache Nullstelle von f'

und $f'(b) \neq 0$, somit ist $\mathrm{ggT}(f, f') = X - a$. Da dieser grösste gemeinsame Teiler schon in $K[X]$ liegt, liegt also a bereits in K, und dasselbe folgt auch für b. Also ist K schon selbst ein Zerfällungskörper von f über K und jedes Element ist ein primitives Element.

Es bleibt der Fall, dass f separabel ist. Wenn es über K in Linearfaktoren zerfällt, so ist K schon selbst ein Zerfällungskörper über K und jedes Element ist ein primitives Element. Zerfällt f in einen linearen und einen quadratischen Faktor, so erzeugt jede Nullstelle des quadratischen Faktors einen Zerfällungskörper und ist daher ein primitives Element.

Es verbleibt der Fall, dass f separabel und irreduzibel ist. Dann operiert die Galoisgruppe transitiv auf den 3 Nullstellen und entspricht daher der A_3 oder der S_3. Im ersteren Fall erzeugt jede Nullstelle schon eine Körpererweiterung vom Grad $3 = |A_3|$ und damit einen Zerfällungskörper, ist also ein primitives Element.

Zuletzt sei f separabel mit der Galoisgruppe S_3 und den Nullstellen $a_1, a_2, a_3 \in \bar{K}$. Dann ist $K(a_1, a_2)$ ein Zerfällungskörper. Da die Galoisgruppe nicht-abelsch ist, kann K kein endlicher Körper sein. Nach dem Beweis des Satzes vom primitiven Element existiert also ein primitives Element der Form $a_1 + ba_2$ für ein $b \in K$. Genauer ist dies dann und nur dann ein primitives Element, wenn $a_1 + ba_2$ verschieden von seinen echten Konjugierten ist, also von $a_{\sigma 1} + ba_{\sigma 2}$ für alle $\sigma \neq \mathrm{id}$. Da keine Nullstelle in K liegt, sind insbesondere alle $a_i \neq 0$. Da sie ausserdem alle verschieden sind, ist die Gleichung $a_{\sigma 1} + ba_{\sigma 2} = a_1 + ba_2$ für $\sigma \neq \mathrm{id}$ nur möglich mit $\sigma 1 \neq 1$ und $\sigma 2 \neq 2$. Für $\sigma = (1\ 2)$ ist die Gleichung äquivalent zu $a_2 + ba_1 = a_1 + ba_2$ und somit zu $(b-1)(a_2 - a_1) = 0$, was schon durch $b \neq 1$ ausgeschlossen werden kann. Wir müssen also nur noch die Permutationen $(1\ 2\ 3)$ und $(3\ 2\ 1)$ betrachten. Da jede davon das Quadrat der anderen ist, genügt es, eine davon zu nehmen. Wir müssen also nur noch vermeiden, dass $a_2 + ba_3 = a_1 + ba_2$ ist. Dies ist äquivalent zu $b(a_3 - a_2) = a_1 - a_2$. Wäre dies nun so, so wäre auch $b(a_{\sigma 3} - a_{\sigma 2}) = a_{\sigma 1} - a_{\sigma 2}$ für jedes $\sigma \in S_3$. Durch Multiplizieren all dieser Gleichungen erhielten wir dann $b^6 c = c$ für $c := \prod_{i \neq j}(a_i - a_j) \neq 0$. Dies können wir aber einfach ausschliessen, indem wir $b^6 \neq 1$ nehmen. Insgesamt zeigt dies, dass $a_1 + ba_2$ für jedes $b \in K$ mit $b^6 \neq 1$ ein primitives Element des Zerfällungskörpers ist.

22. Zeige: Eine algebraische Körpererweiterung L/K ist dann und nur dann galoissch, wenn der Fixkörper von L unter der Gruppe $\mathrm{Aut}_K(L)$ gleich K ist.

Lösung: Zuerst sei L/K galoissch. Fixiere $a \in L \setminus K$ und betrachte sein Minimalpolynom f über K. Da L/K normal ist, enthält L einen Zerfällungskörper L' von f über K. Als Zwischenkörper der separablen Erweiterung L/K ist auch dieser separabel über K; also ist er normal und separabel und daher galoissch über K. Nach der Galoiskorrespondenz für endliche Galoiserweiterungen ist der Fixkörper von L' unter $\mathrm{Aut}_K(L')$ daher gleich K. Wegen $a \in L' \setminus K$ existiert also ein $\sigma \in \mathrm{Aut}_K(L')$ mit $\sigma(a) \neq a$. Sei nun $\bar{L}$ ein algebraischer Abschluss von L. Da

L/L' algebraisch ist, besitzt $\sigma\colon L' \to L'$ eine Fortsetzung zu einem Körperhomomorphismus $\tilde{\sigma}\colon L \to \bar{L}$ über K. Da L/K normal ist, gilt dann aber $\tilde{\sigma}(L) = L$. Somit ist $\tilde{\sigma} \in \mathrm{Aut}_K(L)$ mit $\tilde{\sigma}(a) \neq a$. Durch Variieren von a zeigt dies, dass der Fixkörper von L unter der Gruppe $\mathrm{Aut}_K(L)$ in K enthalten ist. Da er umgekehrt K enthält, ist damit die Richtung „nur dann, wenn“ gezeigt.

Nun nehmen wir umgekehrt an, dass der Fixkörper von L unter der Gruppe $\mathrm{Aut}_K(L)$ gleich K ist. Fixiere $a \in L$ und betrachte sein Minimalpolynom f über K. Für jedes $\sigma \in \mathrm{Aut}_K(L)$ ist dann $\sigma(a)$ wieder eine Nullstelle von f. Somit ist $A := \{\sigma(a) \mid \sigma \in \mathrm{Aut}_K(L)\}$ eine endliche Menge. Betrachte das Polynom

$$g(X) \;:=\; \prod_{a' \in A} (X - a') \;\in\; L[X].$$

Dann gilt $\sigma(g) = g$ für alle $\sigma \in \mathrm{Aut}_K(L)$; aus der Annahme folgt daher $g \in K[X]$. Nach Konstruktion gilt nun aber $g|f$ in $L[X]$; und somit gilt dies auch in $K[X]$. Da f irreduzibel ist und $\deg(g) > 0$ ist und beide Polynome normiert sind, folgt daraus $f = g$. Da g nach Konstruktion separabel ist, ist daher a separabel über K. Ausserdem zerfällt g in $L[X]$ in Linearfaktoren, also enthält L einen Zerfällungskörper des Minimalpolynoms von a über K. Da $a \in L$ beliebig war, ist damit L/K separabel und normal und daher galoissch, und die Richtung „wenn“ ist gezeigt.

23. Zeige: Sind L/K und L'/K endliche Galoiserweiterungen von teilerfremdem Grad, so ist LL'/K endlich galoissch mit einem natürlichen Isomorphismus

$$\mathrm{Gal}(LL'/K) \;\cong\; \mathrm{Gal}(L/K) \times \mathrm{Gal}(L'/K).$$

Lösung: Da L/K und L'/K endlich sind, ist auch LL'/K endlich. Da L/K und L'/K galoissch sind, ist jedes Element von $L \cup L'$ separabel über K und LL' enthält einen Zerfällungskörper seines Minimalpolynoms über K. Da LL' von $L \cup L'$ über K erzeugt ist, ist diese Erweiterung separabel nach Proposition 6.8.5 und normal nach Proposition 6.10.1 der Vorlesung. Somit ist LL'/K endlich und galoissch. Da die Zwischenkörper L und L' selbst galoissch über $\mathbb{Q}$ sind, sind sie invariant unter $\mathrm{Gal}(LL'/K)$; somit erhalten wir einen natürlichen Homomorphismus

$$\mathrm{Gal}(LL'/K) \xrightarrow{\sim} \mathrm{Gal}(L/K) \times \mathrm{Gal}(L'/K), \quad \sigma \mapsto (\sigma|L, \sigma|L').$$

Jedes Element von dessem Kern operiert trivial auf $L \cup L'$ und daher auch auf LL' und ist somit trivial. Also ist der Homomorphismus injektiv. Ausserdem ist die Projektion auf jeden Faktor surjektiv nach Teil (e) des Hauptsatzes der Galoistheorie. Daher ist die Ordnung von $\mathrm{Gal}(LL'/K)$ ein Vielfaches der Ordnung von $\mathrm{Gal}(L/K)$ und der Ordnung von $\mathrm{Gal}(L'/K)$. Nach Voraussetzung sind diese aber teilerfremd; somit ist $|\mathrm{Gal}(LL'/K)|$ ein Vielfaches von $|\mathrm{Gal}(L/K) \times \mathrm{Gal}(L'/K)|$. Da der Homomorphismus schon injektiv ist, ist er daher bijektiv und somit ein Isomorphismus.

24. Zeige oder widerlege: Es existiert eine Körpererweiterung mit genau $50'000$ echten Zwischenkörpern.

Lösung: Für jede natürliche Zahl n existiert eine zyklische Körpererweiterung vom Grad n, zum Beispiel eine Erweiterung $\mathbb{F}_{p^n}/\mathbb{F}_p$ vom Grad n für p prim, oder die Erweiterung $\mathbb{C}(X)/\mathbb{C}(X^n)$. Nach dem Hauptsatz der Galoistheorie ist die Anzahl der Zwischenkörper dann gleich der Anzahl der Untergruppen einer zyklischen Gruppe der Ordnung n, also gleich der Anzahl der Teiler von n. Für die echten Zwischenkörper sind die Teiler 1 und n wegzulassen, also suchen wir eine ganze Zahl $n > 1$ mit genau $50'002$ Teilern. Ein Beispiel hierfür ist $n = r^{50'001}$ für eine Primzahl r, oder $k = r_1 r_2^{25'000}$ für Primzahlen r_1, r_2, oder $k = r_1 r_2^{22} r_3^{1086}$ für Primzahlen r_1, r_2, r_3.

25. Bestimme die Galoisgruppen der folgenden Polynome über $\mathbb{Q}$:

(a) $X^3 - 2X + 1$,

(b) $X^3 + X + 1$,

(c) $X^3 - 6X + 1$,

(d) $X^3 - 12X + 8$.

Lösung:

(a) Die Faktorisierung $X^3 - 2X + 1 = (X - 1)(X^2 + X - 1)$ zeigt, dass das Polynom eine rationale Nullstelle und zwei nichtrationale Nullstellen $\frac{-1\pm\sqrt{5}}{2}$ hat. Somit hat ein Zerfällungskörper den Grad 2 über $\mathbb{Q}$ und die Galoisgruppe ist zyklisch der Ordnung 2.

(b) Jede rationale Nullstelle des Polynoms X^3+X+1 muss ein ganzzahliger Teiler des konstanten Koeffizienten sein. Da aber ± 1 keine Nullstellen sind, besitzt das Polynom keine rationale Nullstelle, und da es den Grad 3 hat, ist es somit irreduzibel über $\mathbb{Q}$ und damit insbesondere separabel. Ausserdem erkennen wir am Graphen der Funktion $\mathbb{R} \to \mathbb{R}$, $x \mapsto x^3 + x + 1$, dass das Polynom nur eine reelle Nullstelle hat. Diese Nullstelle erzeugt also einen Stammkörper des Polynoms vom Grad 3 über $\mathbb{Q}$, und die beiden übrigen Nullstellen erfordern eine weitere Erweiterung vom Grad 2. Der Zerfällungskörper hat somit den Grad $6 = |S_3|$ über $\mathbb{Q}$ und seine Galoisgruppe ist die S_3.

(c) Jede rationale Nullstelle des Polynoms $X^3 - 6X + 1$ muss ein ganzzahliger Teiler des konstanten Koeffizienten sein. Da aber ± 1 keine Nullstellen sind, besitzt das Polynom keine rationale Nullstelle, und da es den Grad 3 hat, ist es somit irreduzibel über $\mathbb{Q}$ und damit insbesondere separabel. Seine Galoisgruppe operiert also transitiv auf den drei Nullstellen und muss daher gleich A_3 oder S_3 sein. Schliesslich hat das Polynom die Diskriminante 837. Da diese kein Quadrat in $\mathbb{Q}$ ist, ist die Galoisgruppe nach Beispiel 7.5.1 der Vorlesung nicht in A_3 enthalten, muss also gleich S_3 sein.

(d) Jede rationale Nullstelle des Polynoms $X^3-12X+8$ muss ein ganzzahliger Teiler des konstanten Koeffizienten sein. Wir rechnen nach, dass $\pm1, \pm2, \pm4, \pm8$ alle keine Nullstellen sind. Also besitzt das Polynom keine rationale Nullstelle, und da es den Grad 3 hat, ist es somit irreduzibel über $\mathbb{Q}$ und damit insbesondere separabel. Seine Galoisgruppe operiert also transitiv auf den drei Nullstellen und muss daher gleich A_3 oder S_3 sein. Schliesslich hat das Polynom die Diskriminante $5184 = 72^2$. Da diese ein Quadrat in $\mathbb{Q}$ ist, ist die Galoisgruppe nach Beispiel 7.5.1 der Vorlesung in A_3 enthalten, muss also gleich A_3 sein.

26. Sei L ein Zerfällungskörper des Polynoms $X^6 - 5$ über $\mathbb{Q}$. Bestimme alle Zwischenkörper von $L/\mathbb{Q}$ mitsamt Inklusionen sowie, falls sie galoissch über $\mathbb{Q}$ sind, deren Galoisgruppen über $\mathbb{Q}$.

Lösung: Da $\mathbb{C}$ algebraisch abgeschlossen ist, können wir L als in $\mathbb{C}$ eingebettet annehmen. Sei a die positive reelle sechste Wurzel aus 5. Sei ζ eine primitive dritte Einheitswurzel in $\mathbb{C}$. Für $1 \leqslant i \leqslant 6$ sei $a_i := a \cdot (-\zeta)^{i-1}$. Dann ist $a_i^6 - 5 = a^6 \cdot (-\zeta)^{6i-6} - 5 = 0$, also sind $a_1, \ldots, a_6$ gerade die sechs verschiedenen Nullstellen von $X^6 - 5$. Somit ist $L = \mathbb{Q}(a_1, \ldots, a_6) \subset \mathbb{Q}(a, \zeta)$, und wegen $a_1 = a$ und $-\frac{a_2}{a_1} = -\frac{a\cdot(-\zeta)}{a} = \zeta$ ist sogar $L = \mathbb{Q}(a, \zeta)$.

Für $1 \leqslant i \leqslant 6$ ist $[\mathbb{Q}(a_i)/\mathbb{Q}] = 6$, da $X^6 - 5$ nach dem Eisenstein-Kriterium mit $p = 5$ irreduzibel ist. Wegen $\mathbb{Q}(a) \subset \mathbb{R}$ und $\zeta \notin \mathbb{R}$ ist zudem $L \neq \mathbb{Q}(a)$. Da $\zeta = \frac{-1\pm\sqrt{-3}}{2}$ bereits eine quadratische Gleichung über $\mathbb{Q}$ löst, folgt daraus $[L/\mathbb{Q}(a)] = 2$ und somit $[L/\mathbb{Q}] = [L/\mathbb{Q}(a)] \cdot [\mathbb{Q}(a)/\mathbb{Q}] = 12$. Insbesondere hat auch $\mathrm{Gal}(L/\mathbb{Q})$ die Ordnung 12.

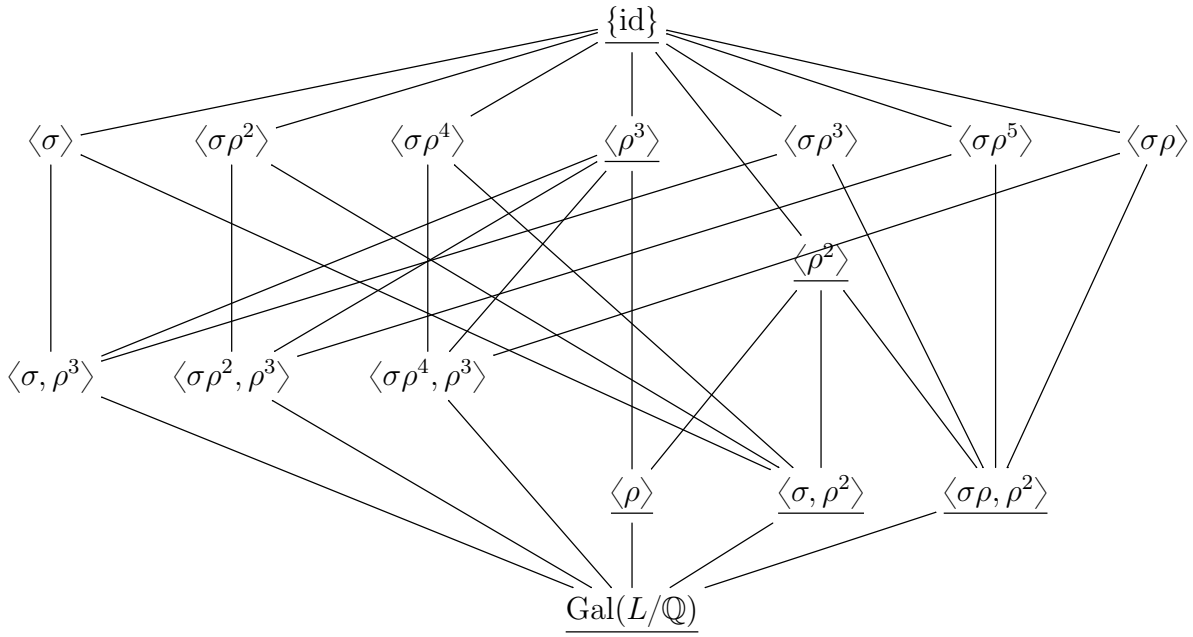
Wir fassen im Folgenden $\mathrm{Gal}(L/\mathbb{Q})$ durch die durch $a_i \mapsto i$ induzierte Einbettung als Untergruppe von S_6 auf.

Da $L/\mathbb{Q}$ normal ist, ist die Einschränkung σ der komplexen Konjugation auf L ein Element von $\mathrm{Gal}(L/\mathbb{Q})$. Konkret entspricht σ der Permutation $(2\,6)(3\,5)$.

Da $X^6 - 5$ irreduzibel ist, operiert $\mathrm{Gal}(L/\mathbb{Q})$ transitiv auf dessen Nullstellen; es existiert also ein $\rho \in \mathrm{Gal}(L/\mathbb{Q})$ mit $\rho(a_1) = a_2$. Wegen $\sigma(a_1) = a_1$ gilt auch $(\rho\sigma)(a_1) = a_2$. Da σ die beiden Nullstellen ζ und ζ^2 des irreduziblen Polynoms $X^2 + X + 1$ vertauscht und ρ sie als $\mathbb{Q}$-Homomorphismus vertauscht oder festlässt, können wir also (nachdem wir allenfalls ρ durch $\rho\sigma$ ersetzen) ohne Beschränkung der Allgemeinheit annehmen, dass $\rho(\zeta) = \zeta$ ist. Dann ist $\rho(a_i) = \rho\big(a \cdot (-\zeta)^{i-1}\big) = a \cdot (-\zeta)^i$, also hat ρ die Darstellung $(1\,2\,3\,4\,5\,6)$.

Die Rechnung $\sigma\rho\sigma^{-1} = (2\,6)(3\,5)(1\,2\,3\,4\,5\,6)(2\,6)(3\,5) = (6\,5\,4\,3\,2\,1) = \rho^{-1}$ zeigt nun, dass die von ρ und σ erzeugte Untergruppe eine Surjektion auf D_6 besitzt, also mindestens Ordnung 12 hat. Wegen $|D_6| = 12 = |\,\mathrm{Gal}(L/\mathbb{Q})| \geqslant |\langle\rho, \sigma\rangle|$ folgt dann aber schon $\mathrm{Gal}(L/\mathbb{Q}) = \langle\rho, \sigma\rangle \cong D_6$.

Wir machen nun eine Aufstellung aller Untergruppen von $\mathrm{Gal}(L/\mathbb{Q}) \cong D_6$ (die detaillierte Überprüfung überlassen wir dem Leser); normale Untergruppen sind unterstrichen:



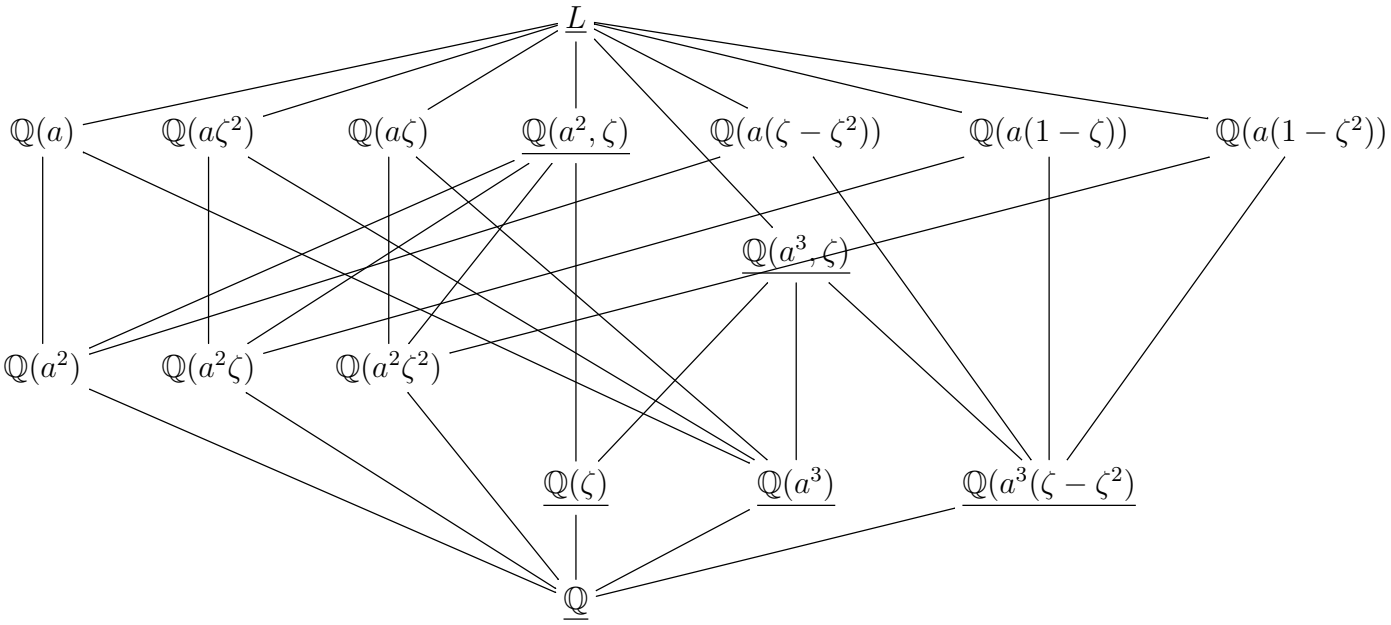
Daraus folgern wir die Aufstellung aller Zwischenkörper. Die Galois-Korrespondenz ordnet einer Untergruppe $H < \mathrm{Gal}(L/\mathbb{Q})$ den Fixkörper L^H mit dem Erweiterungsgrad $[L^H/\mathbb{Q}] = \frac{|\mathrm{Gal}(L/\mathbb{Q})|}{|H|} = \frac{12}{|H|}$ zu:

- $L^{\{\mathrm{id}\}} = L$.
- $L^{\mathrm{Gal}(L/\mathbb{Q})} = \mathbb{Q}$.
- Es ist $\sigma(a) = a$, also $\mathbb{Q}(a) \subset L^{\langle\sigma\rangle}$. Zudem ist $[\mathbb{Q}(a)/\mathbb{Q}] = 6 = \frac{12}{|\langle\sigma\rangle|}$, also $L^{\langle\sigma\rangle} = \mathbb{Q}(a)$.
- Analog ist $(\sigma\rho^2)(a\zeta^2) = a\zeta^2$, also $\mathbb{Q}(a\zeta^2) \subset L^{\langle\sigma\rho^2\rangle}$. Zudem ist $[\mathbb{Q}(a\zeta^2)/\mathbb{Q}] = 6 = \frac{12}{|\langle\sigma\rho^2\rangle|}$, also $L^{\langle\sigma\rho^2\rangle} = \mathbb{Q}(a\zeta^2)$.
- Analog ist $(\sigma\rho^4)(a\zeta) = a\zeta$, also $\mathbb{Q}(a\zeta) \subset L^{\langle\sigma\rho^4\rangle}$. Zudem ist $[\mathbb{Q}(a\zeta)/\mathbb{Q}] = 6 = \frac{12}{|\langle\sigma\rho^4\rangle|}$, also $L^{\langle\sigma\rho^4\rangle} = \mathbb{Q}(a\zeta)$.
- Es ist $\sigma(a^2) = \rho^3(a^2) = a^2$, also $\mathbb{Q}(a^2) \subset L^{\langle\sigma,\rho^3\rangle}$. Zudem ist a^2 eine Nullstelle des über $\mathbb{Q}$ irreduziblen Polynoms $X^3 - 5$, also $[\mathbb{Q}(a^2)/\mathbb{Q}] = 3 = \frac{12}{|\langle\sigma,\rho^3\rangle|}$ und somit $L^{\langle\sigma,\rho^3\rangle} = \mathbb{Q}(a^2)$.
- Analog ist $(\sigma\rho^2)(a^2\zeta) = \rho^3(a^2\zeta) = a^2\zeta$, also $\mathbb{Q}(a^2\zeta) \subset L^{\langle\sigma\rho^2,\rho^3\rangle}$. Zudem ist $a^2\zeta$ eine Nullstelle des über $\mathbb{Q}$ irreduziblen Polynoms $X^3 - 5$, also $[\mathbb{Q}(a^2\zeta)/\mathbb{Q}] = 3 = \frac{12}{|\langle\sigma\rho^2,\rho^3\rangle|}$ und somit $L^{\langle\sigma\rho^2,\rho^3\rangle} = \mathbb{Q}(a^2\zeta)$.

- Analog ist $(\sigma\rho^4)(a^2\zeta^2) = \rho^3(a^2\zeta^2) = a^2\zeta^2$, also $\mathbb{Q}(a^2\zeta^2) \subset L^{\langle\sigma\rho^4,\rho^3\rangle}$. Zudem ist $a^2\zeta^2$ eine Nullstelle des über $\mathbb{Q}$ irreduziblen Polynoms $X^3 - 5$, also $[\mathbb{Q}(a^2\zeta^2)/\mathbb{Q}] = 3 = \frac{12}{|\langle\sigma\rho^4,\rho^3\rangle|}$ und somit $L^{\langle\sigma\rho^4,\rho^3\rangle} = \mathbb{Q}(a^2\zeta^2)$.
- Es ist $\rho(\zeta) = \zeta$, also $\mathbb{Q}(\zeta) \subset L^{\langle\rho\rangle}$. Zudem ist $[\mathbb{Q}(\zeta)/\mathbb{Q}] = 2 = \frac{12}{|\langle\rho\rangle|}$, also $\mathbb{Q}(\zeta) = L^{\langle\rho\rangle}$.
- Es ist $\sigma(a^3) = \rho^2(a^3) = a^3$, also $\mathbb{Q}(a^3) \subset L^{\langle\sigma,\rho^2\rangle}$. Zudem ist a^3 eine Nullstelle des über $\mathbb{Q}$ irreduziblen Polynoms $X^2 - 5$, also ist $[\mathbb{Q}(a^3)/\mathbb{Q}] = 2 = \frac{12}{|\langle\sigma,\rho^2\rangle|}$ und somit $\mathbb{Q}(a^3) = L^{\langle\sigma,\rho^2\rangle}$.
- Es ist $\rho^2(a^3) = a^3$ und $\rho^2(\zeta) = \zeta$, also $\mathbb{Q}(a^3,\zeta) \subset L^{\langle\rho^2\rangle}$. Wegen $\zeta \notin \mathbb{Q}(a^3) \subset \mathbb{R}$ ist $[\mathbb{Q}(a^3,\zeta)/\mathbb{Q}] = [\mathbb{Q}(a^3,\zeta)/\mathbb{Q}(a^3)][\mathbb{Q}(a^3)/\mathbb{Q}] = 4$, also $[\mathbb{Q}(a^3,\zeta)/\mathbb{Q}] = \frac{12}{|\langle\rho^2\rangle|}$ und somit $L^{\langle\rho^2\rangle} = \mathbb{Q}(a^3,\zeta)$.
- Analog ist $\rho^3(a^2) = a^2$ und $\rho^3(\zeta) = \zeta$, also $\mathbb{Q}(a^2,\zeta) \subset L^{\langle\rho^3\rangle}$. Wegen $\zeta \notin \mathbb{Q}(a^2) \subset \mathbb{R}$ ist $[\mathbb{Q}(a^2,\zeta)/\mathbb{Q}] = [\mathbb{Q}(a^2,\zeta)/\mathbb{Q}(a^2)][\mathbb{Q}(a^2)/\mathbb{Q}] = 6$, also $[\mathbb{Q}(a^2,\zeta)/\mathbb{Q}] = \frac{12}{|\langle\rho^3\rangle|}$ und somit $L^{\langle\rho^3\rangle} = \mathbb{Q}(a^2,\zeta)$.
- Es gilt $(\sigma\rho^3)(a\zeta) = -a\zeta^2$ und somit $(\sigma\rho^3)(a(\zeta - \zeta^2)) = a(\zeta - \zeta^2)$ wegen $(\sigma\rho^3)^2 = \mathrm{id}_L$; also ist $\mathbb{Q}(a(\zeta-\zeta^2)) \subset L^{\langle\sigma\rho^3\rangle}$. Zudem ist $a(\zeta-\zeta^2)$ eine Nullstelle des Polynoms X^6+135, und dieses ist irreduzibel über $\mathbb{Q}$ nach dem Eisensteinkriterium bezüglich der Primzahl 5. Also ist $[\mathbb{Q}(a(\zeta - \zeta^2))/\mathbb{Q}] = 6 = \frac{12}{|\langle\sigma\rho^3\rangle|}$ und somit $L^{\langle\sigma\rho^3\rangle} = \mathbb{Q}(a(\zeta - \zeta^2))$.
- Analog gilt $(\sigma\rho^5)(a) = -a\zeta$ und somit $(\sigma\rho^5)(a(1 - \zeta)) = a(1 - \zeta)$ wegen $(\sigma\rho^5)^2 = \mathrm{id}_L$; also ist $\mathbb{Q}(a(1-\zeta)) \subset L^{\langle\sigma\rho^5\rangle}$. Zudem ist $a(1-\zeta)$ eine Nullstelle des Polynoms $X^6 + 135$. Also ist $[\mathbb{Q}(a(1 - \zeta))/\mathbb{Q}] = 6 = \frac{12}{|\langle\sigma\rho^5\rangle|}$ und somit $L^{\langle\sigma\rho^5\rangle} = \mathbb{Q}(a(1 - \zeta))$.
- Analog gilt $(\sigma\rho)(a) = -a\zeta^2$ und somit $(\sigma\rho)(a(1 - \zeta^2)) = a(1 - \zeta^2)$ wegen $(\sigma\rho)^2 = \mathrm{id}_L$; also ist $\mathbb{Q}(a(1-\zeta^2)) \subset L^{\langle\sigma\rho\rangle}$. Zudem ist $a(1-\zeta^2)$ eine Nullstelle des Polynoms $X^6 + 135$. Also ist $[\mathbb{Q}(a(1 - \zeta^2))/\mathbb{Q}] = 6 = \frac{12}{|\langle\sigma\rho\rangle|}$ und somit $L^{\langle\sigma\rho\rangle} = \mathbb{Q}(a(1 - \zeta^2))$.
- Es ist $L^{\langle\sigma\rho,\rho^2\rangle} = L^{\langle\sigma\rho\rangle} \cap L^{\langle\rho^2\rangle} = \mathbb{Q}(a^3,\zeta) \cap \mathbb{Q}(a(1 - \zeta^2)) \ni (a(1 - \zeta^2))^3 = 3a^3(\zeta - \zeta^2)$. Wegen $[L^{\langle\sigma\rho,\rho^2\rangle}/\mathbb{Q}] = \frac{12}{|\langle\sigma\rho,\rho^2\rangle|} = 2$ und $a^3(\zeta - \zeta^2) \notin \mathbb{Q} \subset \mathbb{R}$ gilt also $L^{\langle\sigma\rho,\rho^2\rangle} = \mathbb{Q}(a^3(\zeta - \zeta^2))$.

Bemerkung: An einigen Stellen hätte man auch ausnutzen können, dass mehrere der Untergruppen von $\mathrm{Gal}(L/\mathbb{Q})$ zu einander konjugiert sind. Sind nämlich zwei Untergruppen H, H' unter φ konjugiert, so ist $L^{H'} = \varphi(L^H)$.

Insgesamt ergibt sich die folgende Aufstellung:



Dabei ist ein Zwischenkörper unterstrichen, wenn die entsprechende Untergruppe von $\mathrm{Gal}(L/\mathbb{Q})$ normal ist. Nach dem Hauptsatz der Galoistheorie ist das genau dann der Fall, wenn der Zwischenkörper galoissch über $\mathbb{Q}$ ist, und dann gilt weiter $\mathrm{Gal}(L^H/\mathbb{Q}) \cong \mathrm{Gal}(L/\mathbb{Q})/H$. Daraus ergeben sich die folgenden Galoisgruppen:

$$\begin{aligned}
\mathrm{Gal}(\mathbb{Q}(a^2,\zeta)/\mathbb{Q}) &\cong D_3,\\
\mathrm{Gal}(\mathbb{Q}(a^3,\zeta)/\mathbb{Q}) &\cong (\mathbb{Z}/2\mathbb{Z})^2,\\
\mathrm{Gal}(\mathbb{Q}(a^3)/\mathbb{Q}) &\cong \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(a^3(\zeta-\zeta^2))/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}.
\end{aligned}$$

27. Finde für jede Primzahl p ein irreduzibles Polynom $f \in \mathbb{Q}[X]$ vom Grad p mit der Galoisgruppe S_p.

Lösung: Nach Aufgabe 1 von Serie 28 genügt es, dass f irreduzibel ist und genau zwei nicht reelle Nullstellen hat. Wir konstruieren ein solches Polynom, indem wir mit einem geeigneten Polynom vom Grad p beginnen, welches genau zwei nichtreelle Nullstellen hat, und seine Koeffizienten nur wenig abändern, so dass diese Eigenschaft erhalten bleibt und das Polynom irreduzibel über $\mathbb{Q}$ wird. Die Irreduzibilität garantieren wir mit dem Eisensteinkriterium bei irgendeiner Primzahl, zum Beispiel bei 2.

Für jedes $t \in \mathbb{R}$ setzen wir

$$f_t(x) := (x^2+1)\prod_{j=1}^{p-2}(x-j) + t.$$

Behauptung: Es existiert ein $\varepsilon > 0$, sodass f_t für jedes t mit $|t| < \varepsilon$ in $\mathbb{C}$ genau $p-2$ verschiedene reelle, sowie 2 komplex konjugierte nicht-reelle Nullstellen hat.

Beweis: Das Polynom f_0 hat die komplexen Nullstellen $z_k := k$ für $1 \leqslant k \leqslant p-2$, sowie $z_{p-1}, z_p := \pm i$. Betrachte die Kreisscheiben $G_k := \{z \in \mathbb{C} \mid |z - z_k| < \frac{1}{3}\}$ und setze $G := \bigcup_{k=1}^{n} G_k$. Da ∂G keine Nullstelle von f_0 enthält und f_0 eine stetige Funktion darstellt, ist $\varepsilon := \min_{z \in \partial G} |f_0(z)| > 0$. Für jedes $t \in \mathbb{R}$ mit $|t| < \varepsilon$ und jedes $1 \leqslant k \leqslant p$ gilt nun

$$\forall z \in \partial G_k : |f_t(z) - f_0(z)| < |f_t(z)| + |f_0(z)|.$$

Nach dem Satz von Rouché haben f_t und f_0 nun gleich viele Nullstellen in G_k, also genau eine. Die beiden Nullstellen von f_t in G_{p-1} und G_p sind nicht-reell und komplex konjugiert. Die Nullstellen von f_t in $G_1, \ldots, G_{p-2}$ sind alle reell; wäre nämlich $z \in G_k$ eine nicht-reelle Nullstelle von f_t, so müsste dies auch für $\overline{z} \in G_k$ gelten, im Widerspruch dazu, dass f_t genau eine Nullstelle in G_k hat. □

Sei nun ε wie oben, wähle $k \in \mathbb{Z}^{>0}$ mit $t := \frac{2}{(2k)^p} < \varepsilon$, und setze

$$f(x) \;:=\; f_t(x/2k) \cdot (2k)^p \;=\; (x^2 + 4k^2) \prod_{j=1}^{p-2} (x - 2kj) + 2 \;\in\; \mathbb{Z}[X].$$

Nach obiger Behauptung hat f_t und somit auch f genau $p-2$ relle, sowie 2 komplex konjugierte nicht-reelle Nullstellen. Ausserdem ist f irreduzibel nach dem Eisensteinkriterium bezüglich der Primzahl 2.

28. Beweise oder widerlege: Für jede endliche Gruppe G existiert ein Körper K und eine Galoiserweiterung L/K mit Galoisgruppe $\mathrm{Gal}(L/K) \cong G$.

Lösung: Die Aussage ist korrekt. Mit dem Satz von Cayley wähle eine Einbettung von G in eine symmetrische Gruppe S_n. Ist dann L/K_0 eine endliche Galoiserweiterung mit der Galoisgruppe S_n, so ist L/L^G nach dem Hauptsatz der Galoistheorie eine endliche Galoiserweiterung mit der Galoisgruppe G, wie gewünscht.

Eine Galoiserweiterung mit der Galoisgruppe S_n kann man auf verschiedene Weise finden. Am einfachsten betrachtet man unabhängige Variable $X_1, \ldots, X_n$ über einem Körper k und setzt $L := k(X_1, \ldots, X_n)$. Dann operiert die S_n treu auf L durch Permutation der Variablen, und nach Folge 7.3.14 der Vorlesung ist die Erweiterung $k(X_1, \ldots, X_n)/k(X_1, \ldots, X_n)^{S_n}$ endlich galoissch mit Galoisgruppe S_n.

29. Sei R ein Ring, und seien $f, g \in R[X]$ normierte Polynome. Zeige:

$$\mathrm{Disc}_{fg} = \mathrm{Disc}_f \cdot \mathrm{Disc}_g \cdot \mathrm{Res}_{f,g}^2 .$$

Lösung: Zuerst seien f und g in Linearfaktoren zerlegt, also $f(X) = \prod_{i=1}^{n}(X - \lambda_i)$ und $g(X) = \prod_{j=1}^{m}(X - \lambda'_j)$. Dann wissen wir

$$\begin{aligned} \mathrm{Disc}_f &= \prod_{1\leqslant i<j\leqslant n} (\lambda_i - \lambda_j)^2, \\ \mathrm{Disc}_g &= \prod_{1\leqslant i<j\leqslant m} (\lambda'_i - \lambda'_j)^2, \\ \mathrm{Res}_{f,g} &= \prod_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant m}} (\lambda_i - \lambda'_j). \end{aligned}$$

Andererseits ist $fg(X) = \prod_{i=1}^{n+m}(X-\mu_i)$ mit $\mu_i := \lambda_i$ für $1 \leqslant i \leqslant n$ und $\mu_i := \lambda'_{i-n}$ für $n+1 \leqslant i \leqslant n+m$. Dadurch erhalten wir

$$\begin{aligned} \mathrm{Disc}_{fg} &= \prod_{1\leqslant i<j\leqslant n+m} (\mu_i - \mu_j)^2 \\ &= \prod_{1\leqslant i<j\leqslant n} (\mu_i - \mu_j)^2 \prod_{n+1\leqslant i<j\leqslant n+m} (\mu_i - \mu_j)^2 \prod_{\substack{1\leqslant i\leqslant n \\ n+1\leqslant j\leqslant n+m}} (\mu_i - \mu_j)^2 \\ &= \prod_{1\leqslant i<j\leqslant n} (\lambda_i - \lambda_j)^2 \prod_{1\leqslant i<j\leqslant m} (\lambda'_i - \lambda'_j)^2 \prod_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant m}} (\lambda_i - \lambda'_j)^2 \\ &= \mathrm{Disc}_f \cdot \mathrm{Disc}_g \cdot \mathrm{Res}_{f,g}^2 . \end{aligned}$$

Dadurch ist die Aussage für alle Polynome, die Produkte von Linearfaktoren sind, bewiesen.

Insbesondere gilt die Aussage dann, wenn die Nullstellen der Polynome unabhängige Variablen sind, also wenn $f(X) = \prod_{i=1}^{n}(X-Y_i)$ und $g(X) = \prod_{j=1}^{m}(X-Z_j)$ ist. In diesem Fall sind die Koeffizienten von f und g also $\pm$ die elementarsymmetrischen Polynome in den Y_i, bzw. in den Z_j. Nach dem Hauptsatz über symmetrische Polynome können die elementarsymmetrischen Polynome als unabhängige Variablen betrachtet werden und wir können sie durch beliebige Werte aus dem Ring R ersetzen. Dieses Verfahren liefert also das Resultat für alle normierten Polynome in $R[X]$.

30. Zeige: Für beliebige positive ganze Zahlen $q_1, \ldots, q_n$ gilt

$$L := \mathbb{Q}\big(\sqrt{q_1}, \ldots, \sqrt{q_n}\big) \;=\; \mathbb{Q}\big(\sqrt{q_1} + \ldots + \sqrt{q_n}\big).$$

Lösung: Als Zerfällungskörper des Polynoms $(X^2 - q_1)\cdots(X^2 - q_n)$ ist L endlich galoissch über $\mathbb{Q}$. Für jedes Element γ seiner Galoisgruppe und jedes i gilt $\gamma(\sqrt{q_i}) \in \{\pm\sqrt{q_i}\}$. Mit $a := \sqrt{q_1} + \ldots + \sqrt{q_n}$ gilt also $\gamma(a) = \pm\sqrt{q_1} \pm \ldots \pm \sqrt{q_n}$ mit gewissen voneinander unabhängigen Vorzeichen. Da alle $\sqrt{q_i} > 0$ sind, ist folglich $\gamma(a) = a$ nur dann, wenn alle diese Vorzeichen + sind. In diesem Fall gilt $\gamma(\sqrt{q_i}) = \sqrt{q_i}$ für

jedes i, also ist γ schon die Identität auf ganz L. Somit ist der Stabilisator von a in $\mathrm{Gal}(L/\mathbb{Q})$ trivial. Dieser Stabilisator ist aber gleich $\mathrm{Gal}(L/\mathbb{Q}(a))$; darum ist $\mathbb{Q}(a) = L$, was zu zeigen war.

31. Sei $f \in \mathbb{Q}[X]$ ein irreduzibles Polynom, das in $\mathbb{C}$ sowohl reelle als auch nicht-reelle Nullstellen hat. Zeige, dass die Galoisgruppe von f über $\mathbb{Q}$ nicht abelsch ist.

Lösung: Wir realisieren den Zerfällungskörper von f als Unterkörper von $\mathbb{C}$. Seien α eine reelle und β eine nicht-reelle komplexe Nullstelle von f. Da f irreduzibel ist, operiert die Galoisgruppe Gal_f transitiv auf den Nullstellen von f; also existiert ein $\tau \in \mathrm{Gal}_f$ mit $\tau(\beta) = \alpha$. Sei weiter $\sigma \in \mathrm{Gal}_f$ die Einschränkung der komplexen Konjugation. Dann gilt $\sigma(\tau(\beta)) = \sigma(\alpha) = \alpha$, aber $\tau(\sigma(\beta)) = \tau(\overline{\beta}) \neq \tau(\beta) = \alpha$ wegen der Injektivität von τ. Also ist $\sigma \circ \tau \neq \tau \circ \sigma$ und somit Gal_f nicht-abelsch.

Aliter: Ist Gal_f abelsch, so wissen wir aus Aufgabe 3 von Serie 24, dass der Zerfällungskörper von f bereits von jeder einzelnen Nullstelle über $\mathbb{Q}$ erzeugt wird. Insbesondere gilt dies für jede reelle Nullstelle, also liegt der Zerfällungskörper schon insgesamt in $\mathbb{R}$, im Widerspruch zur Annahme. Also ist Gal_f nicht abelsch.

32. Sei $\zeta \in \mathbb{C}$ eine primitive n-te Einheitswurzel. Für welche ganzen Zahlen k ist $\zeta + \zeta^k$ ein primitives Element der Erweiterung $\mathbb{Q}(\zeta)/\mathbb{Q}$?

Lösung: Nach Satz 7.6.4 ist $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, wobei jede Restklasse $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ der Substitution $\zeta \mapsto \zeta^a$ entspricht. Die Untergruppe $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta+\zeta^k))$ entspricht also der Untergruppe aller $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ mit

$$(*) \qquad \zeta^a + \zeta^{ak} \;=\; \zeta + \zeta^k.$$

Nach dem Hauptsatz der Galoistheorie ist daher $\mathbb{Q}(\zeta + \zeta^k) = \mathbb{Q}(\zeta)$ genau dann, wenn diese Gleichung nur für $\bar{a} = \bar{1}$ gilt.

Behauptung: Die Gleichung $(*)$ gilt genau in den drei Fällen

$$\begin{cases} n \text{ gerade und } k - 1 \equiv \frac{n}{2} \bmod (n), \\ a \equiv 1 \bmod (n), \text{ sowie} \\ a \equiv k \bmod (n) \text{ und } k^2 \equiv 1 \bmod (n). \end{cases}$$

Beweis: Natürlich gilt die Gleichung im Fall $a \equiv 1 \bmod (n)$. Weiter ist $\zeta + \zeta^k = 0$ genau dann, wenn $\zeta^{k-1} = -1$ ist, also wenn n gerade und $k - 1 \equiv \frac{n}{2} \bmod (n)$ ist. In diesem Fall ist $\zeta + \zeta^k$ natürlich gleich allen seinen Konjugierten. Im Folgenden sei also $\zeta + \zeta^k \neq 0$. Aus $(*)$ folgt dann

$$\left|1 + \zeta^{ak-a}\right| \;=\; \left|\zeta^a + \zeta^{ak}\right| \;=\; \left|\zeta + \zeta^k\right| \;=\; \left|1 + \zeta^{k-1}\right|$$

Da ζ^{ak-a} und ζ^{k-1} auf dem Einheitskreis liegen, sehen wir geometrisch sofort, dass dies genau dann gilt, wenn ζ^{ak-a} gleich ζ^{k-1} oder $\bar{\zeta}^{k-1} = \zeta^{1-k}$ ist. Da ζ eine

primitive n-te Einheitswurzel ist, ist dies äquivalent zu $ak-a \equiv \pm(k-1) \bmod (n)$. Im Fall $ak - a \equiv k - 1 \bmod (n)$ ist $(*)$ äquivalent zu

$$\zeta^{a-1} \cdot (\zeta + \zeta^k) \;=\; \zeta^a + \zeta^{a+k-1} \;=\; \zeta + \zeta^k.$$

Wegen $\zeta + \zeta^k \neq 0$ dies äquivalent zu $\zeta^{a-1} = 1$ und folglich zu $a \equiv 1 \bmod (n)$; diese Möglichkeit ist schon aufgeführt. Im Fall $ak - a \equiv 1 - k \bmod (n)$ ist $(*)$ äquivalent zu

$$\zeta^{a-k} \cdot (\zeta^k + \zeta) \;=\; \zeta^a + \zeta^{a+1-k} \;=\; \zeta + \zeta^k.$$

Wegen $\zeta + \zeta^k \neq 0$ ist dies äquivalent zu $\zeta^{a-k} = 1$ und folglich zu $a \equiv k \bmod (n)$. Für ein solches a ist die Kongruenz $ak - a \equiv 1 - k \bmod (n)$ dann äquivalent zu $k^2 \equiv ak \equiv a+1-k \equiv 1 \bmod (n)$, was die letzte aufgeführte Möglichkeit liefert. $\square$

Nach der Behauptung besitzt die Gleichung $(*)$ eine Lösung $a \not\equiv 1 \bmod (n)$ genau in den Fällen

$$\begin{cases} n \geqslant 4 \text{ gerade und } k - 1 \equiv \frac{n}{2} \bmod (n), \\ k \not\equiv 1 \bmod (n) \text{ und } k^2 \equiv 1 \bmod (n). \end{cases}$$

In diesen Fällen ist also $\mathbb{Q}(\zeta + \zeta^k) \neq \mathbb{Q}(\zeta)$ und in allen übrigen $\mathbb{Q}(\zeta + \zeta^k) = \mathbb{Q}(\zeta)$.

33. Beweise oder widerlege: Für jede ganze Zahl $n \geqslant 1$ existiert eine zyklische Erweiterung $K/\mathbb{Q}$ vom Grad n.

Lösung: Die Aussage ist korrekt. Zuerst sei $n = p^r$ für eine Primzahl p. Setze $s := r + 1$ im Fall $p > 2$ und $s := r + 2$ im Fall $p = 2$. Dann ist $\mathbb{Q}(\mu_{p^s})/\mathbb{Q}$ galoissch und $G := \mathrm{Gal}(\mathbb{Q}(\mu_{p^s})/\mathbb{Q}) \cong (\mathbb{Z}/p^s\mathbb{Z})^\times$. Nach der obigen Aufgabe 14 besitzt G also eine normale Untergruppe N mit G/N zyklisch der Ordnung p^r. In der Galoiskorrespondenz entspricht diese Untergruppe einem Zwischenkörper $K/\mathbb{Q}$ mit $\mathrm{Gal}(K/\mathbb{Q})$ zyklisch der Ordnung $n = p^r$, wie gewünscht.

Der allgemeine Fall folgt daraus durch Induktion über n. Sei nämlich $n = mm'$ für zwei teilerfremde ganze Zahlen $m, m' > 1$. Nach Induktionsannahme existieren dann zyklische Erweiterungen $L/\mathbb{Q}$ und $L'/\mathbb{Q}$ vom Grad m beziehungsweise m'. Nach der obigen Aufgabe 23 ist nun $LL'/\mathbb{Q}$ endlich galoissch mit der Galoisgruppe

$$\mathrm{Gal}(LL'/\mathbb{Q}) \;\cong\; \mathrm{Gal}(L/\mathbb{Q}) \times \mathrm{Gal}(L'/\mathbb{Q}) \;\cong\; \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m'\mathbb{Z}.$$

Nach dem chinesischen Restsatz ist letztere aber isomorph zu $\mathbb{Z}/mm'\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}$. Somit folgt die gewünschte Aussage für n, und durch Induktion folgt sie allgemein.

34. Betrachte eine Körpererweiterung der Form $K(a)/K$ mit $a^n \in K$ für ein $n \geqslant 1$. Beweise oder widerlege: Alle Zwischenkörper haben die Form $K(a^m)$ für natürliche Zahlen $m \geqslant 1$.

Lösung: Betrachte den Spezialfall $a = e^{2\pi i/8}$ über $K = \mathbb{Q}$. Nach Satz 7.6.4 der Vorlesung ist dann $\mathbb{Q}(a)/\mathbb{Q}$ galoissch mit der Galoisgruppe $(\mathbb{Z}/8\mathbb{Z})^\times$. Diese ist nicht-zyklisch der Ordnung 4 und besitzt drei verschiedene Untergruppen der Ordnung 2. Nach der Galoiskorrespondenz entsprechen diese drei verschiedenen Zwischenkörpern vom Grad 2 über $\mathbb{Q}$. Wir behaupten, dass nur einer von diesen die genannte Form hat.

Für jede natürliche Zahl $m \geqslant 1$ schreibe $m = 2^i k$ mit k ungerade. Dann ist $k^2 \equiv 1 \mod (8)$ und daher $(a^m)^k = a^{2^i k^2} = a^{2^i}$. Also gilt $a^{2^i} \in \mathbb{Q}(a^m)$ und $a^m \in \mathbb{Q}(a^{2^i})$ und damit $\mathbb{Q}(a^m) = \mathbb{Q}(a^{2^i})$. Wegen $a^4 = -1 \in \mathbb{Q}$ ist dieser Körper gleich $\mathbb{Q}$ für alle $i \geqslant 2$. Im Fall $i = 1$ ist er gleich $\mathbb{Q}(i)$ und im Fall $i = 0$ gleich $\mathbb{Q}(a)$. Der einzige solche Zwischenkörper vom Grad 2 über $\mathbb{Q}$ ist also $\mathbb{Q}(i)$. Die übrigen Zwischenkörper $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(i\sqrt{2})$ haben deshalb nicht die gesuchte Form.

35. Sei $L = K(a_1, \ldots, a_r)/K$ eine Erweiterung von Körpern der Charakteristik $\neq 2$ mit der Eigenschaft $b_i := a_i^2 \in K^\times$ für alle i. Sei $(K^\times)^2 := \{x^2 \mid x \in K^\times\}$ und betrachte die von den Restklassen aller b_i erzeugte Untergruppe $B \subset K^\times/(K^\times)^2$. Zeige:

    (a) L/K ist galoissch.

    (b) Es gibt eine wohldefinierte Abbildung

    $$\varphi\colon \quad \mathrm{Gal}(L/K) \times B \longrightarrow \mu_2 = \{\pm 1\}, \quad (\gamma, [b]) \mapsto \varphi(\gamma, [b])$$

    mit der Eigenschaft $\varphi(\gamma, [b]) := \gamma(a)/a$ für alle $a \in L^\times$ mit $[b] = [a^2]$.

    (c) Die Abbildung φ ist linear in der ersten Variablen.

    (d) Die Abbildung φ ist linear in der zweiten Variablen.

    (e) Für jedes $\gamma \in \mathrm{Gal}(L/K) \smallsetminus \{\mathrm{id}\}$ existiert ein $[b] \in B$ mit $\varphi(\gamma, [b]) \neq 1$. (Man nennt ein solches φ *links nicht-ausgeartet*.)

    (f) Für jedes $[b] \in B \smallsetminus \{[1]\}$ existiert ein $\gamma \in \mathrm{Gal}(L/K)$ mit $\varphi(\gamma, [b]) \neq 1$. (Man nennt ein solches φ *rechts nicht-ausgeartet*.)

    (g) Es existiert ein natürlicher Isomorphismus $\mathrm{Gal}(L/K) \cong \mathrm{Hom}(B, \mu_2)$.

    Lösung:

    (a) Als Zerfällungskörper des Polynoms $\prod_{i=1}^r (X^2 - b_i)$ ist L eine normale algebraische Körpererweiterung von K. Zudem ist jeder Faktor $X^2 - b_i$ wegen $b_i \neq 0$ und $\mathrm{char}(L) \neq 2$ separabel, also ist jedes a_i separabel über K und daher auch L/K separabel. Somit ist L/K galoissch.

    (b) Nach Konstruktion von B existiert für jede Restklasse $[b] \in B$ ein Element $a \in L^\times$ mit $[b] = [a^2]$, das heisst, mit $b = a^2 x^2$ für ein $x \in K^\times$. Für jedes $\gamma \in \mathrm{Gal}(L/K)$ gilt dann $a^2 x^2 = b = \gamma(b) = \gamma(a)^2 x^2$ und somit $\gamma(a)/a = \pm 1$.

Für jedes weitere Element $a' \in L^\times$ mit $[b] = [a'^2]$, das heisst, mit $b = a'^2x'^2$ für ein $x' \in K^\times$, ist dann $a'^2x'^2 = b = a^2x^2$ und somit $a'/a = \pm x/x' \in K^\times$. Daher gilt $\gamma(a')/\gamma(a) = \gamma(a'/a) = a'/a$ und darum $\gamma(a')/a' = \gamma(a)/a$. Die Formel $\varphi(\gamma, [b]) := \gamma(a)/a$ ergibt daher eine wohldefinierte Abbildung.

(c) Betrachte zwei Elemente $\gamma, \gamma' \in \mathrm{Gal}(L/K)$. Nach der Definition von φ gilt dann für $[b]$ und a wie oben

$$\varphi(\gamma\gamma', [b]) \;=\; \frac{\gamma\gamma'(a)}{a} \;=\; \frac{\gamma(a)}{a}\cdot\frac{\gamma\gamma'(a)}{\gamma(a)} \;=\; \frac{\gamma(a)}{a}\cdot\gamma\left(\frac{\gamma'(a)}{a}\right) \;=\; \varphi(\gamma, [b])\cdot\gamma(\varphi(\gamma, [b])).$$

Wegen $\varphi(\gamma, [b]) \in \{\pm 1\}$ ist aber $\gamma(\varphi(\gamma, [b])) = \varphi(\gamma, [b])$; also ist φ linear in der ersten Variablen.

(d) Betrachte zwei Restklassen $[b], [b'] \in B$ und wähle $a, a' \in L^\times$ mit $[b] = [a^2]$ und $[b'] = [a'^2]$. Dann ist $[bb'] = [(aa')^2]$, und die Definition von φ impliziert

$$\varphi(\gamma, [bb']) \;=\; \frac{\gamma(aa')}{aa'} \;=\; \frac{\gamma(a)}{a}\cdot\frac{\gamma(a')}{a'} \;=\; \varphi(\gamma, [b])\cdot\varphi(\gamma, [b']).$$

Also ist φ linear in der zweiten Variablen.

(e) Betrachte ein $\gamma \in \mathrm{Gal}(L/K)$ mit der Eigenschaft $\varphi(\gamma, [b]) = 1$ für alle $[b] \in B$. Dann ist insbesondere $\varphi(\gamma, [b_i]) = 1$ für alle i. Wegen $[b_i] = [a_i^2]$ und der Definition von φ bedeutet dies $\gamma(a_i)/a_i = 1$ und daher $\gamma(a_i) = a_i$ für alle i. Wegen $L = K(a_1, \ldots, a_r)$ folgt daraus $\gamma = \mathrm{id}$. Umgekehrt zeigt dies, dass für jedes $\gamma \in \mathrm{Gal}(L/K) \smallsetminus \{\mathrm{id}\}$ ein $[b] \in B$ existiert mit $\varphi(\gamma, [b]) \neq 1$.

(f) Betrachte ein $[b] \in B$ mit der Eigenschaft $\varphi(\gamma, [b]) = 1$ für alle $\gamma \in \mathrm{Gal}(L/K)$. Mit $[b] = [a^2]$ für $a \in L^\times$ wie oben ist dann $\gamma(a)/a = 1$ für alle $\gamma \in \mathrm{Gal}(L/K)$. Dies bedeutet aber $\gamma(a) = a$ und somit $a \in K^\times$. Nach der Konstruktion von B bedeutet dies $[b] = 1$. Umgekehrt zeigt dies, dass für jedes $[b] \in B \smallsetminus \{[1]\}$ ein $\gamma \in \mathrm{Gal}(L/K)$ existiert mit $\varphi(\gamma, [b]) \neq 1$.

(g) Da φ linear in der zweiten Variablen ist, ist durch $\psi(\gamma)([b]) := \varphi(\gamma, [b])$ eine natürliche Abbildung $\psi\colon \mathrm{Gal}(L/K) \to \mathrm{Hom}(B, \mu_2)$ wohldefiniert. Da φ linear in der ersten Variablen ist, ist ψ ein Homomorphismus. Die Links-Nichtausgeartetheit von φ besagt dann, dass für jedes $\gamma \in \mathrm{Gal}(L/K) \smallsetminus \{\mathrm{id}\}$ ein $[b] \in B$ existiert mit $\psi(\gamma)([b]) \neq 1$; das heisst, dass $\psi(\gamma) \neq 1$ ist. Also ist ψ injektiv und insbesondere $|\mathrm{Gal}(L/K)| \leqslant |\mathrm{Hom}(B, \mu_2)|$.

Nun wiederholen wir dieselbe Argumentation in der anderen Variablen: Da φ linear in der ersten Variablen ist, ist durch $\omega([b])(\gamma) := \varphi(\gamma, [b])$ eine natürliche Abbildung $\omega\colon B \to \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_2)$ wohldefiniert. Da φ linear in der zweiten Variablen ist, ist ω ein Homomorphismus. Die Rechts-Nichtausgeartetheit von φ besagt dann, dass für jedes $[b] \in B \smallsetminus \{[1]\}$ ein $\gamma \in \mathrm{Gal}(L/K)$ existiert mit $\varphi(\gamma, [b]) \neq 1$; das heisst, dass $\omega([b]) \neq 1$ ist. Also ist ω injektiv und insbesondere $|B| \leqslant |\mathrm{Hom}(\mathrm{Gal}(L/K), \mu_2)|$.

Aus dieser Ungleichung folgern wir nun die Surjektivität von ψ wie folgt. Beachte zunächst, dass $K^\times/(K^\times)^2$ eine endliche abelsche Gruppe ist mit der Eigenschaft $y^2 = 1$ für jedes Element y. Schreiben wir sie additiv anstatt multiplikativ, bedeutet dies $2v = 0$ für jedes Element v. Damit wird $K^\times/(K^\times)^2$ ein Modul über dem Ring $\mathbb{Z}/2\mathbb{Z}$, das heisst, ein Vektorraum über dem Körper $\mathbb{F}_2$. Nach Konstruktion ist dann B ein $\mathbb{F}_2$-Untervektorraum davon. Analog wird dadurch auch $\mu_2 = \{\pm 1\}$ ein $\mathbb{F}_2$-Vektorraum, und zwar der Dimension 1, da er genau 2 Elemente hat. Somit ist $\operatorname{Hom}(B, \mu_2) \cong \operatorname{Hom}_{\mathbb{F}_2}(B, \mathbb{F}_2)$ isomorph zum Dualraum von B, also einem $\mathbb{F}_2$-Vektorraum derselben endlichen Dimension wie B. Der injektive Homomorphismus ψ identifiziert dann $\operatorname{Gal}(L/K)$ mit einem Untervektorraum von $\operatorname{Hom}(B, \mu_2)$, und es folgt $|\operatorname{Gal}(L/K)| \leqslant |\operatorname{Hom}(B, \mu_2)| = |B|$. Die Interpretation von $\operatorname{Gal}(L/K)$ als endlich-dimensionaler $\mathbb{F}_2$-Vektorraum zeigt dann auf die gleiche Weise, dass $\operatorname{Hom}(\operatorname{Gal}(L/K), \mu_2)$ ein $\mathbb{F}_2$-Vektorraum derselben endlichen Dimension ist wie $\operatorname{Gal}(L/K)$. Zusammen mit der Injektivität von ω folgt daher

$$|\operatorname{Hom}(B, \mu_2)| \;=\; |B| \;\leqslant\; |\operatorname{Hom}(\operatorname{Gal}(L/K), \mu_2)| \;=\; |\operatorname{Gal}(L/K)| \;<\; \infty.$$

Also ist der injektive Homomorphismus $\psi\colon \operatorname{Gal}(L/K) \to \operatorname{Hom}(B, \mu_2)$ auch surjektiv und somit der gesuchte Isomorphismus.

36. Bestimme die Galoisgruppe des Polynoms $X^4 + 18X^2 - 72X + 81$ über $\mathbb{Q}$.

Lösung: Setze $f := X^4 + 18X^2 - 72X + 81$. Wir werden gleich sehen, dass f modulo (5) separabel ist, also ist auch f selbst separabel. Seine Galoisgruppe Γ können wir also mit einer Untergruppe von S_4 identifizieren. Nach Satz 7.9.4 der Vorlesung sagt uns die Faktorisierung von f modulo einer Primzahl p, wenn sie separabel ist, dass Γ eine Permutation enthält, deren Zykellängen genau die Grade der irreduziblen Faktoren modulo p sind. Wir zerlegen f also in irreduzible Faktoren modulo kleinen Primzahlen:

$f \equiv (X+1)^4 \bmod (2)$	$\rightsquigarrow$ nichts
$f \equiv X^4 \bmod (3)$	$\rightsquigarrow$ nichts
$f \equiv (X+3)(X^3 + 2X^2 + 2X + 2) \bmod (5)$	$\rightsquigarrow$ 3 -Zykel
$f \equiv (X+6)(X^3 + X^2 + 5X + 3) \bmod (7)$	$\rightsquigarrow$ 3 -Zykel
$f \equiv (X+4)(X^3 + 7X^2 + X + 1) \bmod (11)$	$\rightsquigarrow$ 3 -Zykel
$f \equiv (X+6)(X^3 + 7X^2 + 2X + 7) \bmod (13)$	$\rightsquigarrow$ 3 -Zykel
$f \equiv (X^2 + 11X + 4)(X^2 + 6X + 16) \bmod (17)$	$\rightsquigarrow$ zwei 2-Zykel
$f \equiv (X^2 + 3X + 16)(X^2 + 16X + 11) \bmod (19)$	$\rightsquigarrow$ zwei 2-Zykel

Somit enthält die Galoisgruppe von f einen 3-Zykel und ein Produkt von zwei disjunkten 2-Zykeln. Die letztere Permutation ist ein nichttriviales Element der

Kleinschen Vierergruppe, auf deren nichttrivialen Elementen jeder 3-Zykel transitiv durch Konjugation operiert. Also enthält die Galoisgruppe die Kleinsche Vierergruppe und einen 3-Zykel und folglich die A_4.

Die Reduktion modulo weiterer Primzahlen bringt nun nichts mehr. Dafür hat f aber die Diskriminante $241864704 = 2^{12}3^{10}$. Da diese ein Quadrat in $\mathbb{Q}$ ist, ist Γ in der alternierenden Gruppe enthalten. Zusammen folgt also $\Gamma = A_4$.

Aliter: Da die Diskriminante ungleich Null ist, ist f separabel, und da sie ein Quadrat ist, ist $\Gamma < A_4$. Die Reduktion modulo (5) zeigt, dass Γ einen 3-Zykel enthält. Durch Durchprobieren aller Teiler von 81 stellt man fest, dass f keine Nullstelle in $\mathbb{Q}$ hat; also hat f keinen linearen Faktor über $\mathbb{Q}$. Wegen des 3-Zykels kann f dann auch nicht in zwei Faktoren vom Grad 2 zerfallen. Daher ist f irreduzibel, und folglich operiert Γ transitiv auf den 4 Ziffern. Aber jede transitive Untergruppe von A_4, welche einen 3-Zykel enthält, ist bereits die A_4. Also gilt $\Gamma = A_4$.

Sternaufgaben folgen auf einem separaten Blatt.