Thema Nr. 1

(Aufgabengruppe)
Es sind **alle** Aufgaben dieser Aufgabengruppe zu bearbeiten.

Aufgabe 1 (Frühjahr 2006)**.** Sei $(G,+)$ eine abelsche Gruppe und U,V Untergruppen. Zeigen Sie, daß die folgenden beiden Aussagen äquivalent sind: (4 Punkte)

(a) Die Gruppe G ist direkte Summe von U und V.

(b) Für alle $a,b\in G$ haben die Nebenklassen $a+U$ und $b+V$ jeweils genau ein gemeinsames Element.

Lösung. **„(b) ⇒ (a)“:** Wir bezeichnen mit 0 das neutrale Element von G. Für $a=b=0$ haben nach Voraussetzung die Nebenklassen $0+U$ und $0+V$ genau ein gemeinsames Element. Da $0\in 0+U=U$ und $0\in 0+V=V$ gilt also

$$U\cap V=(0+U)\cap(0+V)=\{0\}.$$

Wir müssen noch zeigen, daß $U+V=G$ ist. Da U und V Untergruppen von G sind, ist klar, daß $U+V\subset G$. Sei also $g\in G$. Wir betrachten die Nebenklassen $g+U$ und $0+V=V$. Nach Voraussetzung enthält $(g+U)\cap V$ genau ein Element v. Dafür gilt $v=g+u$ für ein $u\in U$. Es folgt $g=(-u)+v\in U+V$. Also $G\subset U+V$.
Dies zeigt, daß G direktes Produkt von U und V ist.

„(a) ⇒ (b)“: Seien $a,b\in G$. Wir müssen zeigen, daß der Schnitt $(a+U)\cap(b+V)$ genau ein Element enthält. Es ist $a-b\in G$ und da $U+V=G$ gibt es $u\in U$ und $v\in V$ mit $u+v=a-b$. Es folgt $a+(-u)=b+v\in(a+U)\cap(b+V)$. Dies zeigt, daß $(a+U)\cap(b+V)$ mindestens ein Element enthält. Um zu sehen, daß es genau ein solches gibt, sei $g\in(a+U)\cap(b+V)$ beliebig. Also $g=a+u'=b+v'$ mit $u'\in U$ und $v'\in V$. Dann folgt $v'-u'=a-b=u+v$, also $u'+u=v'-v\in U\cap V$. Da aber $U\cap V=\{0\}$ nach Voraussetzung, folgt $u=-u'$ und $v=v'$. Es folgt $g=a+(-u)=b+v$, also genau das Element von oben, welches demnach eindeutig ist.

Aufgabe 2 (Frühjahr 2012)**.** Für welche $a,b\in\mathbb{Q}$ ist das Polynom $(x-1)^2$ ein Teiler von $f=ax^{30}+bx^{15}+1$? (3 Punkte)

Lösung. Für $f\in\mathbb{Q}[x]$ wie angegeben mit $a,b\in\mathbb{Q}$ ist $(x-1)^2$ genau dann ein Teiler, wenn 1 eine doppelte Nullstelle von f ist. Dies ist genau dann der Fall, wenn $f(1)=0$ und $f'(1)=0$. Es ist $f'(x)=30ax^{29}+15bx^{14}$, also ist

$$\begin{aligned}f(1)&=a+b+1\\ f'(1)&=30a+15b\end{aligned}$$

Es gilt also:

$$\begin{aligned}(x-1)^2\big|f &\Leftrightarrow f(1)=0=f'(1)\\ &\Leftrightarrow a+b+1=0 \quad\text{und}\quad 30a+15b=0\\ &\Leftrightarrow a+b+1=0 \quad\text{und}\quad 2a+b=0\\ &\Leftrightarrow a+b+1=0 \quad\text{und}\quad b=-2a\\ &\Leftrightarrow -a+1=0 \quad\text{und}\quad b=-2a\\ &\Leftrightarrow a=1 \quad\text{und}\quad b=-2\end{aligned}$$

Also teilt $(x-1)^2$ genau dann f, wenn $a=1$ und $b=-2$.

Aufgabe 3 (Frühjahr 1995)**.** Sei F/K eine nichttriviale endliche Galoiserweiterung mit auflösbarer Galoisgruppe. Zeigen Sie, daß es einen Zwischenkörper $K\subset E\subset F$ gibt, so daß E/K Galois'sch mit abelscher Galoisgruppe ist. (4 Punkte)

Lösung. Sei $G = \mathrm{Gal}(F/K)$. Nach Vorraussetzung ist G auflösbar, sie besitzt also eine Normalreihe mit abelschen Faktoren, das heißt eine Folge von Untergruppen

$$G = H_0 \supset H_1 \supset \ldots \supset H_m = \{e\},$$

$m \geqslant 0$, so daß $H_{i+1} \triangleleft H_i$ und H_i/H_{i+1} abelsch ist für $0 \leqslant i < m$.
Insbesondere ist H_1 ein Normalteiler in G. Definiere nun $E := \mathrm{Fix}_F(H_1)$. Dies ist der nach dem Hauptsatz der Galoistheorie zu H_1 korrespondierende Zwischenkörper, F/E ist Galois'sch und $\mathrm{Gal}(F/E) = H_1 \subset G$. Da aber H_1 Normalteiler von G ist, ist nach dem zweiten Teil des Hauptsatzes der Galoistheorie auch E/K Galois'sch mit Galoisgruppe $\mathrm{Gal}(E/K) \cong G/H_1$. Nach Voraussetzung ist $G = H_0$ und H_0/H_1 abelsch. Damit ist $\mathrm{Gal}(E/K)$ abelsch, und E/K abelsche Galoiserweiterung, wie gewünscht

Zusatzaufgabe (Frühjahr 1981)**.** Man gebe für die folgenden Fälle jeweils ein Beispiel an oder begründe kurz, warum es ein derartiges Beispiel nicht gibt: (4 Punkte)

(a) eine einfache nicht-abelsche Gruppe,

(b) ein kommutativer Körper mit genau 6 Elementen,

(c) ein maximales Ideal in $\mathbb{Q}[X, Y]$ das nicht Hauptideal ist,

(d) ein irreduzibles Polynom 3. Grades in $\mathbb{R}[X]$.

Lösung. (a) Die alternierende Gruppe $A_5 \subset \mathfrak{S}_5$ ist die kleinste nicht-abelsche einfache Gruppe (enthält keine nicht-trivialen Normalteiler).

(b) Die Ordnung jedes endlichen Körpers ist eine Primzahlpotenzm, also gibt es keinen Körper mit 6 Elementen.

(c) Das Ideal (X, Y) is maximales Ideal (denn $\mathbb{Q}[X, Y]/(X, Y) \cong \mathbb{Q}$ ist ein Körper) aber kein Hauptideal (denn X und Y sind teilerfremd).

(d) DIe Erweiterung $\mathbb{R} \subset \mathbb{C}$ hat Grad 2 und $\mathbb{C}$ ist ein algebraischer Abschluß von $\mathbb{R}$. Also ist jedes Polynom vom Grad $\geqslant 3$ über $\mathbb{R}$ reduzibel.

Thema Nr. 2

(Aufgabengruppe)
Es sind **alle** Aufgaben dieser Aufgabengruppe zu bearbeiten.

Aufgabe 1 (Frühjahr 2014)**.** Es seien A, B komplexe $(n \times n)$-Matrizen mit $AB = BA$. (4 Punkte)

(a) Man zeige, daß B jeden Eigenraum von A invariant lässt, d.h.:
Für jeden Eigenraum U von A gilt $Bu \in U$für alle $u \in U$.

(b) Man zeige, daß A und B einen gemeinsamen Eigenvektor haben, d.h.:
Es gibt $0 \neq v \in \mathbb{C}^n$ und $\lambda, \mu \in \mathbb{C}$ mit $Av = \lambda v$, $Bv = \mu v$.

(c) Man zeige anhand eines Beispiels, daß die Aussage aus (b) ohne die Voraussetzung $AB = BA$ im Allgemeinen nicht gilt.

Lösung. **Zu (a):** Sei $\lambda \in \mathbb{C}$ und $U \subset \mathbb{C}^n$ der Eigenraum von A zum Wert λ. Für $u \in U$ gilt dann

$$A(Bu) = (AB)u = (BA)u = B(Au) = B(\lambda u) = \lambda(Bu).$$

Also ist $Bu \in U$. Dies zeigt die Behauptung.

Zu (b): Sei $\chi_A \in \mathbb{C}[X]$ das charakteristische Polynom von A. Da $\mathbb{C}$ algebraisch abgeschlossen ist, zerfällt es in Linearfaktoren. Also besitzt A mindestens einen Eigenwert $\lambda \in \mathbb{C}$. Sei $U \subset \mathbb{C}^n$ der zugehörige Eigenraum. Da die Matrix B den Eigenraum U nach Teil (a) invariant lässt, induziert ihre Einschränkung auf U einen Endomorphismus

$$\phi : U \to U, v \mapsto Bv.$$

Sei $\chi_\phi \in \mathbb{C}[X]$ das charakteristische Polynom von ϕ. Mit dem gleichen Argument wie oben zerfällt es in Linearfaktoren. Also hat auch ϕ mindestens einen Eigenwert $\mu \in \mathbb{C}$ und einen nichttrivialen zugehörigen Eigenraum $V \subset U \subset \mathbb{C}^n$. Sei $0 \neq v \in U$ ein Eigenvektor von ϕ zum Eigenwert μ. Dann gilt $Av = \lambda v$ und $Bv = \phi(v) = \mu v$. Also haben A und B einen gemeinsamen Eignevektor (mit möglischerweise unterschiedlichen Eigenwerten).

Zu (c): Sei $n = 2$. Zwei Matrize die nciht miteinander vertauschen sind

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \text{und} \qquad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

denn $AB = -BA$. Das charakteristische Polynom von A ist

$$\chi_A = (X - 1)(X + 1),$$

also sind die Eignewerte ± 1 und die zu gehörigen Eigenräume

$$\left\{ \begin{pmatrix} \alpha \\ 0 \end{pmatrix} \mid \alpha \in \mathbb{C} \right\} \quad \text{für } 1$$
$$\left\{ \begin{pmatrix} 0 \\ \beta \end{pmatrix} \mid \beta \in \mathbb{C} \right\} \quad \text{für } -1$$

Doch für $\alpha \in \mathbb{C} \setminus \{0\}$ ist

$$B \begin{pmatrix} \alpha \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \alpha \end{pmatrix}$$
$$B \begin{pmatrix} 0 \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ 0 \end{pmatrix}$$

Also ist kein (nicht-trivialer) Eigenvektor von A ein Eignvektor von B.

Aufgabe 2. Sei $K = \mathbb{C}(t)$ der Quotientenkörper des Polynomrings $\mathbb{C}[t]$ und $f = x^3 - 2tx + t \in K[x]$. Zeigen Sie, daß f irreduzibel in $K[x]$ ist. (3 Punkte)

Lösung. Der Ring $R = \mathbb{C}[t]$ ist als Polynomring über einem Körper ein euklidischer Ring, wobei die euklidische Norm durch die Gradabbildung

$$\mathbb{C}[t]\backslash\{0\} \to \mathbb{N}_0, f \mapsto \deg(f)$$

gegeben ist. Das Element $t \in \mathbb{C}[t]$ ist irreduzibel, denn für jede Zerlegung $t = a \cdot b$ gilt

$$1 = \deg(t) = \deg(a) + \deg(b),$$

also $\deg(a) = 1$ und $\deg(b) = 0$ oder umgekehrt. Dies zeigt, daß t keine echten Teiler hat, also irreduzibel ist. Da R als euklidischer Ring faktoriell ist, ist t sogar ein Primelement.
Wir betrachten f nun als Polynom über dem Integriätsring R. Hier erfüllt es die Voraussetzungen für das Eisensteinkriterium für das Primelement t: da f normiert ist, teilt t nicht den Leitkoeffizienten, andererseits teilt t alles anderen Koeffizienten, aber den konstanten Koeffizienten nicht quadratisch. Also

$$\begin{aligned} t \nmid a_3 &= 1, \\ t \mid a_2 &= 0 \\ t \mid a_1 &= -2t \\ t \mid a_0 &= t \\ t^2 \nmid a_0 &= t \end{aligned}$$

Also ist f irreduzibel in $R[x]$ und nach dem Gauß'schen Lemma irreduzibel in $K[x]$, da K der Quotientenkörper von R ist.

Aufgabe 3 (Herbst 2016)**.** Finden Sie zwei Polynome $f, g \in \mathbb{Q}[X]$ gleichen Grades, so daß $\mathrm{Gal}(f)$ und $\mathrm{Gal}(g)$ gleich viele Elemente habe, aber $\mathrm{Gal}(f)$ abelsch und $\mathrm{Gal}(g)$ nicht abelsch ist. (4 Punkte)

Lösung. Die Ordnung der gesuchten Gruppen kann keine Primzahl sein. Die kleinste mögliche nichtabelsche Gruppe ist $\mathfrak{S}_3$ und hat Ordnung 6. Wir kennen bereits eine Galoiserweiterung mit dieser Galoisgruppe:
Der Zerfällungskörper des Polynoms $X^3 - 2 \in \mathbb{Z}[X]$ ist $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ und hat Ordnung 6 über $\mathbb{Q}$. (Im Examen müsste man das zeigen, hier verweise ich auf die Vorlesungsnotizen.)

$$\mathrm{Gal}(X^3 - 2/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}) \cong \mathfrak{S}_3.$$

Jede abelsche Gruppe der Odrnung 6 ist isomorph zu $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Diese ist zyklisch und insbesondere isomorph zu $(\mathbb{Z}/7\mathbb{Z})^\times$. Wir wissen, daß dies die Galoisgruppe der Erweiterung $\mathbb{Q}^{(7)}/\mathbb{Q}$ ist, also des siebten Kreistielungskörpers $\mathbb{Q}(\zeta_7)$ über $\mathbb{Q}$. Das Minimalpolynom der primitiven siebten Einheitswurzel ζ_7 ist das Kreisteilungspolynom $\phi_7 = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$.

$$\mathrm{Gal}(\phi_7/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z}.$$

Da nicht nach irreduziblen Polynomen gefragt war, können wir das Polynom $X^3 - 2$ mit linearen „trivialen" Polynomen in $\mathbb{Z}[X]$ multiplizieren, um Polynome gleichen Grades zu erhalten. Etwa:

$$\begin{aligned} f &= \phi_7 = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \\ g &= (X^3 - 2)(X - 2)(X - 3)(X - 5) \end{aligned}$$

Dann gilt

$$\begin{aligned} \mathrm{Gal}(f/\mathbb{Q}) &= \mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z} \\ \mathrm{Gal}(g/\mathbb{Q}) &= \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}) \cong \mathfrak{S}_3 \end{aligned}$$

und $|\mathrm{Gal}(f/\mathbb{Q})| = |\mathrm{Gal}(g/\mathbb{Q})| = 6$.

Zusatzaufgabe (Frühjahr 1981)**.** Man gebe für die folgenden Fälle jeweils ein Beispiel an oder begründe kurz, warum es ein derartiges Beispiel nicht gibt: (4 Punkte)

(a) eine auflösbare nicht-abelsche Gruppe,

(b) eine nicht-abelsche Gruppe der Ordnung 7,

(c) ein maximales Ideal in $\mathbb{Q}[X,Y]$ das nicht Hauptideal ist,

(d) ein irreduzibles separables Polynom 2. Grades in $\mathbb{F}_2[X]$.

Lösung. (a) Die symmetrische Gruppe $\mathfrak{S}_3$ ist nicht-abelsch, aber auflösbar mit Normalreihe mit abelschen Faktoren $\mathfrak{S}_3 \supset A_3 \supset \{e\}$.

(b) Jede Gruppe von Primzahlordnung ist zyklisch, also abelsch. Also gibt es keine nicht-abelsche Gruppe der Ordnung 7.

(c) Das Ideal (X,Y) is maximales Ideal (denn $\mathbb{Q}[X,Y]/(X,Y) \cong \mathbb{Q}$ ist ein Körper) aber kein Hauptideal (denn X und Y sind teilerfremd).

(d) Da der Körper $\mathbb{F}_2$ endlich ist, ist er vollkommen, also ist jedes irreduzible Polynom separabel. Ein irreduzibles Polynom ist zum Beispeil $X^2 + X + 1 \in \mathbb{F}_2[X]$, denn es hat keine Nullstelle in $\mathbb{F}_2$.