UNIVERSITÄT REGENSBURG
FAKULTÄT FÜR MATHEMATIK
Prof. Dr. N. Naumann

WS2011/2012
Blatt 1

Übungen zur Vorlesung
Algebra
Abgabe: 26.10.2011, 11.30 Uhr

Aufgabe 1. Sei $\varphi : G \to G'$ ein Gruppenhomomorphismus. Zeigen Sie:

i) Der Kern von φ ist eine Untergruppe $\ker(\varphi) \subseteq G$, und φ ist injektiv genau dann, wenn $\ker(\varphi) = \{e\}$ gilt.

ii) Ist $H \subseteq G$ eine Untergruppe, so auch $\varphi(H) \subseteq G'$. Belegen Sie durch ein Beispiel, dass hier Untergruppe nicht durch Normalteiler ersetzt werden kann.

iii) Ist $H' \subseteq G'$ eine Untergruppe (bzw. ein Normalteiler), so auch das Urbild $\varphi^{-1}(H') \subseteq G$.

Aufgabe 2. Sei G eine Gruppe und $X := G$, aufgefasst als Menge.

i) Zeigen Sie, dass die Abbildung

$$\Phi : G \to \Sigma(X),$$

definiert durch $\Phi(a)(b) = ab$ für alle $a, b \in G$, wohldefiniert und ein Monomorphismus von Gruppen ist.

ii) Seien nun $n \geq 1$ und speziell $G = \mathbb{Z}/n\mathbb{Z}$. Berechnen Sie explizit

$$\Phi(\overline{1}) \in \Sigma(X) = \Sigma(\{\overline{0}, \overline{1}, \dots, \overline{n-1}\}).$$

Aufgabe 3. Sei k ein Körper. Zeigen Sie:

i) Die Teilmenge

$$B := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, d \in k^*, b \in k \right\} \subseteq \mathrm{Gl}_2(k)$$

ist eine Untergruppe. Sie heißt die *Standard-Borel-Untergruppe.*

ii) Die Teilmenge

$$T := \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in k^* \right\} \subseteq B$$

ist eine Untergruppe, aber kein Normalteiler. Diese Gruppe T heißt der *Standard-Torus*.

iii) Die Teilmenge

$$N := \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in k \right\} \subseteq B$$

ist ein Normalteiler (das *unipotente Radikal*), und es gilt $B/N \cong T$.

iv) Die Teilmenge $N \subseteq \mathrm{Gl}_2(k)$ ist eine Untergruppe, aber kein Normalteiler.

Aufgabe 4 Sei $G \neq \{e\}$ eine Gruppe. Zeigen Sie, dass folgende Aussagen äquivalent sind:

i) Die Ordnung $|G|$ ist eine Primzahl.

ii) Die Gruppe G besitzt keine nicht-trivialen Untergruppen.

iii) Es existiert ein Isomorphismus $G \cong \mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p.

Zusatzaufgabe. Zeigen Sie:

i) Die Teilmenge $\mathbb{R}^{>0} := \{x \in \mathbb{R} \mid x > 0\} \subseteq \mathbb{R}^*$ ist eine Untergruppe. (1 Punkt)

ii) Die Abbildung

$$\exp : (\mathbb{R}, +) \to (\mathbb{R}^{>0}, \cdot)\,,\; x \mapsto \exp(x) := e^x$$

ist ein Gruppenisomorphismus. (1 Punkt)

iii) Es gilt

$$(\mathbb{Q}^{>0}, \cdot) \ncong (\mathbb{Q}, +).$$

(4 Punkte)

Hinweis: Die Struktur der Gruppe $\mathbb{Q}^*$ ist aus LA II bekannt.

UNIVERSITÄT REGENSBURG WS2011/2012
FAKULTÄT FÜR MATHEMATIK Blatt 2
Prof. Dr. N. Naumann

Übungen zur Vorlesung
Algebra
Abgabe: 2.11.2011, 11.30 Uhr

Aufgabe 1. Seien G eine Gruppe $H \subseteq G$ eine Untergruppe und $N \trianglelefteq G$ ein Normalteiler. Zeigen Sie:

i) Die Teilmenge $HN := \{hn \mid h \in H, n \in N\} \subseteq G$ ist eine Untergruppe und $N \trianglelefteq HN$ und $H \cap N \trianglelefteq H$ sind Normalteiler.

ii) Die Abbildung

$$H/(H \cap N) \to HN/N\,,\ h(H \cap N) \mapsto hN$$

ist wohldefiniert und ein Isomorphismus.

iii) Für einen Gruppenhomomorphismus $\varphi : G \to G'$ sind äquivalent:

a) Es gilt $N \subseteq \ker(\varphi)$.

b) Es existiert genau ein Gruppenhomomorphismus $f : G/N \to G'$ mit $\varphi = f \circ \pi$, wobei $\pi : G \to G/N$ die kanonische Projektion bezeichnet.

Aufgabe 2.

i) Bestimmen Sie eine ganze Zahl $a \in \mathbb{Z} \setminus 17\mathbb{Z}$ so, dass $\bar{a} \in \mathbb{F}_{17}^*$ ein Erzeuger ist.

ii) Bestimmen Sie die Ordnung aller Elemente $\sigma \in A_4 \subseteq S_4$ und folgern Sie insbesondere, dass A_4 keine Elemente der Ordnung 6 enthält.

Aufgabe 3. Seien A ein kommutativer Ring und $S \subseteq A$ multiplikativ abgeschlossen. Zeigen Sie:

i) Die in der Vorlesung angegebenen Abbildungen $+, \cdot : (S^{-1}A) \times (S^{-1}A) \to (S^{-1}A)$ sind wohldefiniert.

ii) In $S^{-1}A$ gilt das Distributivgesetz.

Aufgabe 4

i) Sei k ein Körper. Zeigen Sie, dass der kanonische Ringhomomorphismus $k \to \mathrm{Quot}(k)$ ein Isomorphismus ist.

ii) Sei p eine Primzahl und $(p) \subseteq \mathbb{Z}_{(p)}$ das von p erzeugte Hauptideal. Zeigen Sie $\mathbb{Z}_{(p)} \setminus (p) \subseteq \mathbb{Z}_{(p)}^*$, und folgern Sie, dass $(p) \subseteq \mathbb{Z}_{(p)}$ das einzige maximale Ideal des Ringes $\mathbb{Z}_{(p)}$ ist.

Zusatzaufgabe. Zeigen Sie

$$\left(\prod_{n\geq 1}(\mathbb{Z}/n\mathbb{Z})\right) \otimes_{\mathbb{Z}} \mathbb{Q} \not\simeq \prod_{n\geq 1}((\mathbb{Z}/n\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Q})\,.$$

Hinweis: Der rechte Modul ist Null, und es existiert ein Monomorphismus abelscher Gruppen $\mathbb{Z} \hookrightarrow \prod(\mathbb{Z}/n\mathbb{Z})$.

UNIVERSITÄT REGENSBURG — WS2011/2012
FAKULTÄT FÜR MATHEMATIK — Blatt 3
Prof. Dr. N. Naumann

Übungen zur Vorlesung
Algebra
Abgabe: 9.11.2011, 11.30 Uhr

Aufgabe 1.
Seien $n \geq 1$ und $\varphi \in \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}^n)$. Zeigen Sie, dass φ genau dann injektiv ist, wenn die Quotientengruppe $\mathbb{Z}^n/im(\varphi)$ endlich ist.
Hinweis: Elementarteilersatz.

Aufgabe 2
Sei $p \neq 2$ eine Primzahl. Zeigen Sie die Äquivalenz der folgenden Aussagen:

i) $\overline{-1} \in (\mathbb{F}_p^*)^2 := \{x^2 \mid x \in \mathbb{F}_p^*\}$.

ii) $p \equiv 1\,(4)$.

Hinweis: Überlegen Sie zunächst, dass für jeden Isomorphismus $f : \mathbb{F}_p^* \to \mathbb{Z}/(p-1)\mathbb{Z}$ gilt: $f(\overline{-1}) = \overline{\left(\frac{p-1}{2}\right)}$.

Aufgabe 3.
Seien R ein faktorieller Ring, $p \in R$ ein Primelement und $f = \sum\limits_{i=0}^{n} a_i X^i$, $g = \sum\limits_{j=0}^{m} b_j X^j \in R[X]$ Polynome, für die gelte : $\exists 0 \leq i \leq n, 0 \leq j \leq m : p$ teilt weder a_i noch b_j. Setzen Sie für alle $0 \leq k \leq m+n : c_k := \sum\limits_{i=0}^{k} a_i b_{k-i}$, und

i) Zeigen Sie, dass ein $0 \leq k \leq m+n$ existiert, für welches p nicht c_k teilt. (4 Punkte)

ii) Zeigen Sie durch ein Beispiel, dass man in Teil i) auf die Voraussetzung $p \in R$ Primelement nicht verzichten kann. (2 Punkte)

Aufgabe 4
Seien k ein Körper, und die Polynome $f(Y), g(Y) \in k[Y]$ seien teilerfremd und beide nicht konstant. Zeigen Sie, dass $f(Y) - g(Y)X \in k(X)[Y]$ irreduzibel ist.
Hinweis: Sie müssen in den Ringen $k(X)[Y], k[X,Y]$ und $k(Y)[X]$ arbeiten.

Zusatzaufgabe.
Seien $n \geq 1$ und $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ paarweise verschieden. Zeigen Sie, dass

$$Y^2 - (X - \alpha_1) \cdot (X - \alpha_2) \cdot \ldots \cdot (X - \alpha_n) \in \mathbb{C}[X,Y]$$

irreduzibel ist.

UNIVERSITÄT REGENSBURG
FAKULTÄT FÜR MATHEMATIK
Prof. Dr. N. Naumann

WS2011/2012
Blatt 4

Übungen zur Vorlesung
Algebra
Abgabe: 16.11.2011, 11.30 Uhr

Aufgabe 1 Seien R ein faktorieller Ring, $\mathcal{P} \subseteq R$ ein Vertretersystem der Primelemente bis auf Assoziiertheit und $v_p : R \setminus \{0\} \to \mathbb{N}$ ($p \in \mathcal{P}$) die p-adische Bewertung wie in der Vorlesung. Dann sind $a, b \in R \setminus \{0\}$ genau dann teilerfremd, wenn für alle $p \in \mathcal{P}$ gilt : $\min\{v_p(a), v_p(b)\} = 0$.

i) Seien $n \geq 1, a_1, \ldots, a_n \in R \setminus \{0\}$ paarweise teilerfremd und $m \geq 1$ so, dass ein $x \in R$ mit

$$a_1 \cdot a_2 \cdot \ldots \cdot a_n = x^m$$

existiert. Zeigen Sie: $\forall 1 \leq i \leq n \exists y_i \in R, \epsilon_i \in R^* : a_i = \epsilon_i \cdot y_i^m$. Das heißt, ist ein Produkt teilerfremder Elemente eine m-te Potenz, so auch bis auf Assoziiertheit jeder einzelne Faktor.

ii) Zeigen Sie, dass der Unterring

$$\mathbb{Z}[\sqrt{-2}] := \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$$

bezüglich $\delta(a + b\sqrt{-2}) := a^2 + 2b^2$ euklidisch ist, und folgern Sie, dass $\mathbb{Z}[\sqrt{-2}]$ faktoriell ist.

iii) Zeigen Sie $(\mathbb{Z}[\sqrt{-2}])^* = \{\pm 1\}$, und dass $\alpha := \sqrt{-2} \in \mathbb{Z}[\sqrt{-2}] =: R$ ein Primelement ist.

Aufgabe 2 Es gelten die Bezeichnungen und Voraussetzungen aus Aufgabe 1.

i) Seien $x, y \in \mathbb{Z}$ Lösungen der Gleichung

$$x^3 = y^2 + 2 = (y - \alpha)(y + \alpha) \text{ in } R.$$

a) Zeigen Sie: Ist $\pi \in R$ ein Primelement mit $\pi|(y-\alpha)$ und $\pi|(y+\alpha)$, so folgt $\pi = \pm\alpha$.

b) In der Situation von Teil a) folgern Sie weiter $x^3 \equiv 0 \equiv y^2+2\,(8)$, Widerspruch. Also sind $y-\alpha$ und $y+\alpha \in R$ teilerfremd.

c) Zeigen Sie, dass $y-\alpha$ und $y+\alpha$ in R nicht assoziiert sind.

ii) (Fermat) Folgern Sie:

$$\{(x,y) \in \mathbb{Z}^2 \mid y^2 = x^3 - 2\} = \{(3,5),(3,-5)\}.$$

Aufgabe 3

i) Sei $\alpha := \frac{1}{2}(-1+i\sqrt{3}) \in \mathbb{C}$. Zeigen Sie für das Minimalpolynom: $\mathrm{Mipo}_{\mathbb{Q}}(\alpha) = X^2+X+1 \in \mathbb{Q}[X]$.

Zeigen Sie, dass folgende Polynome irreduzibel sind:

ii) $2X^4 + 200X^3 + 2000X^2 + 20000X + 20 \in \mathbb{Q}[X]$

iii) $3X^4 + 6X^2 - 12X + 10 \in \mathbb{Q}[X]$

Aufgabe 4

i) Zeigen Sie, dass $X^2+X+1 \in \mathbb{F}_2[X]$ das einzige irreduzible Polynom vom Grad 2 ist.

ii) Zeigen Sie, dass $\frac{7}{8}X^4 + \frac{1}{2}X^3 + 5X^2 + 6X + 12 \in \mathbb{Q}[X]$ irreduzibel ist.

iii) Zeigen Sie, dass kein Element $\alpha \in \mathbb{R}(X,Y) := Quot(\mathbb{R}[X,Y])$ existiert, welches die Gleichung $\alpha^2 = X^4 + X^2Y^2 + XY + X$ erfüllt.

Zusatzaufgabe.
Zeigen Sie, dass für jede Primzahl p das Polynom $X^p - X - 1 \in \mathbb{F}_p[X]$ irreduzibel ist.
Hinweis: Wenden Sie auf die Primfaktorzerlegung des Polynoms den Automorphismus $X \mapsto X+1$ an.

UNIVERSITÄT REGENSBURG — WS2011/2012
FAKULTÄT FÜR MATHEMATIK — Blatt 5
Prof. Dr. N. Naumann

Übungen zur Vorlesung
Algebra
Abgabe: 23.11.2011, 11.30 Uhr

Aufgabe 1

i) Sei $k \subseteq E$ eine Körpererweiterung. Zeigen sie die Äquivalenz der folgenden Aussagen.

   a) Die Erweiterung $k \subseteq E$ ist algebraisch.
   b) Es existiert eine Familie von Zwischenkörpern $k \subseteq k_i \subseteq E$ $(i \in I)$ mit $[k_i : k] < \infty$ für alle $i \in I$ und $E = \bigcup_{i \in I} k_i$.

ii) Seien $k \subseteq E$ eine Körpererweiterung und

$$k \subseteq \bar{k}^E := \{\alpha \in E \mid \alpha \text{ ist algebraisch über } k\} \subseteq E$$

der *algebraische Abschluss von k in E*. Zeigen Sie:

   a) Die Menge $\bar{k}^E$ ist ein Zwischenkörper von $k \subseteq E$.
   b) Ist $\alpha \in E$ algebraisch *über* $\bar{k}^E$, so folgt bereits $\alpha \in \bar{k}^E$.

Man sagt, $\bar{k}^E$ ist algebraisch abgeschlossen in E.

Bemerkung: Aus dem Fundamentalsatz der Algebra ($\mathbb{C}$ ist algebraisch abgeschlossen), folgt mit ii), das $\bar{\mathbb{Q}}$ algebraisch abgeschlossen ist.

Aufgabe 2 Es sei $k \subseteq E$ eine Körpererweiterung.

i) Zeigen Sie: Ist $[E : k]$ eine Primzahl, so existiert ein $\alpha \in E$ mit $E = k(\alpha)$.

ii) Seien $[E : k] = 2^k$ für ein $k \geq 0$ und $f \in k[X]$ ein Polynom vom Grad 3, das eine Nullstelle in E besitzt. Zeigen Sie, dass f bereits in k eine Nullstelle besitzt.

Aufgabe 3

i) Seien k ein Körper und $n \geq 1$. Zeigen Sie, dass für den Unterkörper $k(t^n) \subseteq k(t)$ des rationalen Funktionenkörpers gilt: $[k(t) : k(t^n)] = n$.

ii) Seien $\alpha \in E$ algebraisch über k und $n \geq 1$. Zeigen Sie: $[k(\alpha^n) : k] \geq \frac{1}{n}[k(\alpha) : k]$.

Aufgabe 4 Sei $\alpha \in \mathbb{C}$ eine Lösung der Gleichung $\alpha^3 + 2\alpha - 1 = 0$. Bestimmen Sie explizit $\mathrm{Mipo}_{\mathbb{Q}}(\alpha)$ und $\mathrm{Mipo}_{\mathbb{Q}}(\beta := \alpha^2 + \alpha)$.
Hinweis: Das charakteristische Polynom der $\mathbb{Q}$-linearen Abbildung $\cdot\beta : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$ annuliert β (Cayley-Hamilton).

Zusatzaufgabe.
Seien $n, m \geq 1$ teilerfremd und $\alpha, \beta \in \mathbb{C}$ mit $\alpha^n = 2$, $\beta^m = 3$. Zeigen Sie $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha\beta)$, und folgern Sie $\mathrm{Mipo}_{\mathbb{Q}}(\alpha\beta) = X^{nm} - 2^m \cdot 3^n$.

Hinweis: Zeigen Sie zunächst $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}$, und folgern Sie $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = [\mathbb{Q}(\beta) : \mathbb{Q}] = m$ und analog mit α, β und m, n vertauscht.

UNIVERSITÄT REGENSBURG
FAKULTÄT FÜR MATHEMATIK
Prof. Dr. N. Naumann

WS2011/2012
Blatt 6

Übungen zur Vorlesung
Algebra
Abgabe: 30.11.2011, 11.30 Uhr

Aufgabe 1 Seien k ein Körper und $q \in k(X) \setminus k$.

i) Zeigen Sie, dass teilerfremde $f, g \in k[X]$ existieren, so dass $q = \frac{f}{g}$ gilt.

ii) In der Situation von i) zeigen Sie, dass
$$f(T) - g(T)q \in k(q)[T]$$
ein Polynom minimalen Grades in $k(q)[T]$ ist, welches X annuliert, und folgern Sie $[k(X) : k(q)] = \max\{\deg(f), \deg(g)\}$.

iii) Folgern Sie, dass $k \subseteq k(X)$ algebraisch abgeschlossen ist, d.h. es gilt $\bar{k}^{k(X)} = k$.

Aufgabe 2 Sei $k \subseteq E$ eine Körpererweiterung. Zeigen Sie, dass $k \subseteq E$ genau dann algebraisch ist, wenn für jeden Unterring $R \subseteq E$ mit $k \subseteq R$ gilt, dass R ein Körper ist.

Aufgabe 3 Seien $k \subseteq E = k(\alpha)$ eine einfache algebraische Körpererweiterung, $k \subseteq K \subseteq E$ ein Zwischenkörper, und schreiben Sie
$$\mathrm{Mipo}_K(\alpha) = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in K[X].$$
Zeigen Sie, dass $K = k(a_0, \ldots, a_{n-1})$ gilt.

Aufgabe 4 Sei $k \subseteq E = k(\alpha)$ eine einfache algebraische Körpererweiterung. Zeigen Sie, dass $k \subseteq E$ nur endlich viele Zwischenkörper besitzt.
Hinweis: $\mathrm{Mipo}_k(\alpha) \in E[X]$ hat nur endlich viele Teiler und Aufgabe 3.

Zusatzaufgabe.
Seien p eine Primzahl und $n, m \geq 1$ teilerfremd. Zeigen Sie, dass $X^n - p^m \in \mathbb{Q}[X]$ irreduzibel ist.

UNIVERSITÄT REGENSBURG
FAKULTÄT FÜR MATHEMATIK
Prof. Dr. N. Naumann

WS2011/2012
Blatt 7

Übungen zur Vorlesung
Algebra
Abgabe: 7.12..2011, 11.30 Uhr

Aufgabe 1 Seien k ein Körper und V ein k-Vektorraum. Eine Teilmenge $X \subseteq V$ heisst linear unabhängig, wenn jede ihrer endlichen Teilmengen k-linear unabhängig ist, und heisst eine Basis, wenn jedes Element von V eindeutig endliche Linearkombination von Elementen aus X ist. Zeigen Sie:

i) Ist $X \subseteq V$ linear unabhängig, so ist X in einer maximalen linear unabhängigen Teilmenge von V enthalten.

ii) Jede maximale linear unabhängige Teilmange von V ist eine Basis.

Aufgabe 2 Seien $\alpha \in \mathbb{C}$ mit $\alpha^3 = 2$ und $1 \neq \zeta \in \mathbb{C}$ mit $\zeta^3 = 1$. Nach Beispiel 7.11. der Vorlesung ist dann $\mathbb{Q} \subseteq E := \mathbb{Q}(\alpha, \zeta)$ ein Zerfällungskörper von $X^3 - 2 \in \mathbb{Q}[X]$.

i) Zeigen Sie, dass jeder $\mathbb{Q}$-Homomorphismus $E \to E$ ein Isomorphismus ist, und folgern Sie, dass

$$\mathrm{Aut}(E/\mathbb{Q}) := \{\varphi : E \to E \mid \varphi \text{ ist ein } \mathbb{Q} - \text{Homomorphismus}\}$$

eine Gruppe bezüglich der Komposition ist.

ii) Setzen Sie $\mathcal{N} := \{\alpha, \alpha\zeta, \alpha\zeta^2\} \subseteq \mathbb{C}$ und zeigen Sie, dass die Abbildung

$$\Phi : \mathrm{Aut}(E/\mathbb{Q}) \to \Sigma(\mathcal{N})(\simeq S_3)\,,\ \varphi \mapsto \varphi|_{\mathcal{N}}$$

wohldefiniert und ein injektiver Gruppenhomomorphismus ist.

iii) Zeigen Sie, dass Φ in Teil ii) ein Isomorphismus ist.

Aufgabe 3
Sei $E := \mathbb{Q}(\sqrt[4]{2}, i)$.

i) Zeigen Sie, dass $E/\mathbb{Q}$ Zerfällungskörper des Polynomes $X^4 - 2 \in \mathbb{Q}[X]$ ist.

ii) Zeigen Sie $[E : \mathbb{Q}] = 8$ und bestimmen Sie alle $\mathbb{Q}$-Automorphismen von $E/\mathbb{Q}$. Hinweis: Zeigen Sie zunächst, dass $E' := \mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ nicht normal ist, und folgern Sie $E' \cap \mathbb{Q}(i) = \mathbb{Q}$.

iii) Sei $\alpha := \sqrt[4]{2} + i \in E$. Zeigen Sie, dass α unter keinen zwei $\mathbb{Q}$-Automorphismen von $E/\mathbb{Q}$ dasselbe Bild hat, und folgern Sie $E = \mathbb{Q}(\alpha)$.

Aufgabe 4 Bestimmen Sie einen Zerfällungskörper $E/\mathbb{Q}$ des Polynoms $X^4 + 2X^2 - 2 \in \mathbb{Q}[X]$ und den Grad $[E : \mathbb{Q}]$.

Zusatzaufgabe.

i) Sei $k \subseteq E = k(\alpha_1, \ldots, \alpha_n)$ eine endlich erzeugte algebraische Körpererweiterung. Zeigen Sie, dass E/k genau dann normal ist, wenn es Zerfällungskörper des Polynoms $\prod_{i=1}^n \mathrm{Mipo}_k(\alpha_i) \in k[X]$ ist.

ii) Seien $k \subseteq E_1, E_2$ endliche normale Körpererweiterungen. Zeigen Sie, dass es genau dann einen k-Homomorphismus von E_1 nach E_2 gibt, wenn $f, g \in k[X]$ existieren, so dass $f \mid g$ in $k[X]$ gilt, und E_1 (bzw. E_2) Zerfällungskörper von f (bzw. g) über k ist.

UNIVERSITÄT REGENSBURG
FAKULTÄT FÜR MATHEMATIK
Prof. Dr. N. Naumann

WS2011/2012
Blatt 8

Übungen zur Vorlesung
Algebra
Abgabe: 14.12..2011, 11.30 Uhr

Aufgabe 1 Sei k ein Körper. Zeigen Sie:

i) Für $a \in k$ und $f, g \in k[X]$ gelten: $(af)' = a \cdot f', (f+g)' = f' + g'$ und $(fg)' = f'g + g'f$.

ii)

$$\{f \in k[X] \mid f' = 0\} = \begin{cases} k & , \quad \mathrm{char}(k) = 0 \\ \{g(X^p) \mid g \in k[X]\} & , \quad \mathrm{char}(k) = p > 0. \end{cases}$$

Aufgabe 2 Seien k ein Körper, E/k eine algebraische Körpererweiterung und $\varphi : E \to E$ ein k-Algebrenhomomorphismus. Zeigen Sie, dass φ ein Isomorphismus ist, und belegen Sie durch ein Beispiel, dass auf die Voraussetzung "algebraisch" nicht verzichtet werden kann.
Hinweis: Betrachten Sie zunächst den Fall endlicher Erweiterungen.

Aufgabe 3 Seien k ein Körper und $k \subseteq \bar{k}$ ein algebraischer Abschluss. Zwei Elemente $\alpha, \beta \in \bar{k}$ heissen *konjugiert über* k, falls ein $\sigma \in \mathrm{Hom}_{k-Alg}(\bar{k}, \bar{k})$ mit $\sigma(\alpha) = \beta$ existiert. Zeigen Sie:

i) Es sind äquivalent:

   a) α und β sind über k konjugiert.
   b) Es gilt $\mathrm{Mipo}_k(\alpha)(\beta) = 0$.
   c) Es existiert ein k-Algebrenisomorphismus $\varphi : k(\alpha) \to k(\beta)$ mit $\varphi(\alpha) = \beta$.
   d) Es gilt $\mathrm{Mipo}_k(\alpha) = \mathrm{Mipo}_k(\beta)$.

ii) Über k konjugiert zu sein ist eine Äquivalenzrelation $\sim$ auf der Menge $\bar{k}$, und die Abbildung

$$\bar{k}/\sim \longrightarrow \{f \in k[X] \mid f \text{ ist normiert und irreduzibel}\},\ [\alpha] \mapsto \mathrm{Mipo}_k(\alpha)$$

ist wohldefiniert und bijektiv, d.h. identifiziert die Elemente von $\bar{k}$ bis auf Konjugiertheit mit der Menge der irreduziblen Polynome in $k[X]$.

Aufgabe 4 Sei k ein algebraisch abgeschlossener Körper. Zeigen Sie, dass k unendlich ist.

Zusatzaufgabe.
Bestimmen Sie die allgemeine Normalform und, falls möglich, die Jordansche Normalform der folgenden Matrizen über den angegebenen Körpern:

i)

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in M_2(\mathbb{F}_2).$$

ii)

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in M_2(\mathbb{F}_4).$$

UNIVERSITÄT REGENSBURG WS2011/2012
FAKULTÄT FÜR MATHEMATIK Blatt 9
Prof. Dr. N. Naumann

Übungen zur Vorlesung
Algebra
Abgabe: 21.12..2011, 11.30 Uhr

Aufgabe 1 Seien p eine Primzahl und $n \geq 1$. Zeigen Sie:

i) Ein irreduzibles $f \in \mathbb{F}_p[X]$ ist genau dann ein Teiler von $X^{p^n} - X$ in $\mathbb{F}_p[X]$, wenn $\deg(f)$ ein Teiler von n ist.

ii) In $\mathbb{F}_p[X]$ ist $X^{p^n} - X$ das Produkt über alle irreduziblen, normierten $f \in \mathbb{F}_p[X]$ mit $\deg(f) \mid n$.

Aufgabe 2 Zerlegen Sie für alle $1 \leq n \leq 4$ das Polynom $X^{2^n} - X \in \mathbb{F}_2[X]$ in irreduzible Faktoren, und diskutieren Sie den Zusammenhang mit den endlichen Erweiterungen von $\mathbb{F}_2$ der Grade $1, 2, 3$ und 4.

Aufgabe 3

i) Sei k ein endlicher Körper. Zeigen Sie: $\prod_{\alpha \in k^*} \alpha = -1$.

ii) Zeigen Sie, dass für jede Primzahl $p > 0$ gilt: $p \mid ((p-1)! + 1)$ in $\mathbb{Z}$.

Aufgabe 4 Seien $\eta := \exp(\frac{2\pi i}{5})$, $\zeta := \exp(\frac{2\pi i}{7}) \in \mathbb{C}$. Zeigen Sie: $\eta \notin \mathbb{Q}(\zeta)$.

Zusatzaufgabe.
Seien p eine Primzahl, $\mathbb{F}_p \subseteq \bar{\mathbb{F}}_p$ ein algebraischer Abschluss und $G := < Frob_{\bar{\mathbb{F}}_p} > \subseteq Gal(\bar{\mathbb{F}}_p/\mathbb{F}_p) = G_{\mathbb{F}_p}$ die vom Frobenius erzeugt Untergruppe. Zeigen Sie:

i) $G \simeq \mathbb{Z}$.

ii) $\bar{\mathbb{F}_p}^G = \mathbb{F}_p$.

iii) $G \neq G_{\mathbb{F}_p}$.
Hinweis: Seien l ein Primzahl und $K := \mathbb{F}_{p^{l^\infty}} := \cup_{n \geq 1} \mathbb{F}_{p^{l^n}} \subseteq \bar{\mathbb{F}}_p =: E$. Dann gelten $Gal(E/K) \neq \{id\}$, und für jedes $1 \neq \sigma \in Gal(E/K) \subseteq G_{\mathbb{F}_p}$ gilt $\sigma \notin G$.

UNIVERSITÄT REGENSBURG
FAKULTÄT FÜR MATHEMATIK
Prof. Dr. N. Naumann

WS2011/2012
Blatt 10

Übungen zur Vorlesung
Algebra
Abgabe: 11.1. 2012, 11.30 Uhr

Aufgabe 1 Seien $k \subseteq E$ eine endliche Galoiserweiterung, $k \subseteq K_i \subseteq E$ $(i = 1, 2)$ Zwischenkörper und $H_i = Gal(E/K_i) \subseteq Gal(E/k) =: G$ die korrespondierenden Untergruppen. Zeigen Sie: Für ein $\sigma \in G$ gilt $\sigma(K_1) = K_2$ genau dann, wenn $\sigma H_1 \sigma^{-1} = H_2$ gilt.

Aufgabe 2 Seien $k \subseteq E$ eine endliche Galoiserweiterung und $H \subseteq G := Gal(E/k)$ eine Untergruppe.

i) Das Element $\alpha \in E$ habe die Eigenschaft, dass für alle $\sigma \in G$ $\sigma(\alpha) = \alpha$ genau dann gilt, wenn $\sigma \in H$ gilt. Zeigen Sie $E^H = k(\alpha)$.
Hinweis: Bestimmen Sie $|G\alpha|$.

ii) Zeigen Sie, dass ein $\alpha \in E$ mit der in Teil i) formulierten Eigenschaft existiert.

Aufgabe 3 Sei G eine endliche Gruppe. Zeigen Sie, dass eine Galoiserweiterung $k \subseteq E$ mit $Gal(E/k) \simeq G$ existiert.
Hinweis: $G \subseteq S_n$.

Aufgabe 4 Seien $\alpha := \frac{1+i}{\sqrt{2}} \in \mathbb{C}$ und $k := \mathbb{Q} \subseteq E := k(\alpha) \subseteq \mathbb{C}$. Zeigen Sie, dass E/k galoissch ist und bestimmen Sie $Gal(E/k)$ sowie alle Zwischenkörper von E/k.

Zusatzaufgabe.
Seien $n \geq 1$, $p_1, \ldots, p_n$ paarweise verschiedene Primzahlen und $k := \mathbb{Q} \subseteq E := k(\sqrt{p_1}, \ldots, \sqrt{p_n})$.

i) Zeigen Sie: E/k ist galoissch, und die Abbildung

$$Gal(E/k) \to \prod_{i=1}^{n} Gal(k(\sqrt{p_i})/k) \, (\simeq (\mathbb{Z}/2\mathbb{Z})^n) \, ,$$

$\sigma \mapsto (\sigma|_{k(\sqrt{p_i})})_{1\leq i\leq n}$ ist ein Gruppenisomorphismus.
Hinweis: Induktion über n. Beachten Sie, dass Sie im Induktionsschritt alle quadratischen Teilerweiterungen von $E/\mathbb{Q}$ kennen, und zeigen Sie als Vorüberlegung: Für $a, b \in \mathbb{Q}^*$ gilt $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$ genau dann, wenn ein $q \in \mathbb{Q}^*$ mit $a = q^2 b$ existiert.

ii) Zeigen Sie, dass $\alpha := \sum_{i=1}^{n} \sqrt{p_i} \in E$ ein primitives Element der Erweiterung E/k ist.

iii) Bestimmen Sie explizit $\mathrm{Mipo}_{\mathbb{Q}}(\sqrt{2} + \sqrt{3} + \sqrt{5})$.

Übungen zur Vorlesung
Algebra
Abgabe: 18.1. 2012, 11.30 Uhr

Aufgabe 1 Seien k ein Körper, $f := t_1^3 + t_2^3 + t_3^3 \in k[t_1, t_2, t_3]$, sowie $s_1, s_2, s_3 \in k[t_1, t_2, t_3]$ die elementarsymmetrischen Polynome.

i) Zeigen Sie: Es existiert genau ein $g \in k[X_1, X_2, X_3]$ so, dass $f = g(s_1, s_2, s_3)$ gilt. (2 Punkte)

ii) Bestimmen Sie g aus Teil i) explizit. (4 Punkte)

Aufgabe 2 Für eine natürliche Zahl $n \geq 2$ zeigen Sie:

i) $\varphi(n) = n \cdot \prod_{0<p|n \text{ Primzahl}}(1 - p^{-1})$. (2 Punkte)

ii) $n = \sum\limits_{0<d|n} \varphi(d)$. (4 Punkte)

Aufgabe 3 Seien k ein Körper, $f \in k[X]$ irreduzibel und separabel, E/k ein Zerfällungskörper von f, und es gelte, dass $Gal(E/k)$ abelsch ist. Zeigen Sie: Für jede Nullstelle $\alpha \in E$ von f gilt $E = k(\alpha)$. Zeigen Sie durch ein Beispiel, dass man auf die Kommutativität der Galoisgruppe hier nicht verzichten kann. (5+1 Punkte)

Aufgabe 4 Sei $\alpha \in \mathbb{C}$ mit $\alpha^6 + 3 = 0$ gewählt. Zeigen Sie, dass $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ galoissch ist, und bestimmen Sie die Galoisgruppe sowie alle Zwischenkörper. (6 Punkte)
Hinweis: $\zeta_6 \in \mathbb{Q}(\alpha)$.

Zusatzaufgabe.
Seien E ein algebraisch abgeschlossener Körper, $\sigma \in Aut(E)$, und die Körpererweiterung $k := E^{\langle\sigma\rangle} \subseteq E$ sei algebraisch.
Zeigen Sie, dass jede endliche algebraische Erweiterung von k zyklisch ist.(6 Punkte)

UNIVERSITÄT REGENSBURG — WS2011/2012
FAKULTÄT FÜR MATHEMATIK — Blatt 12
Prof. Dr. N. Naumann

Übungen zur Vorlesung
Algebra
Abgabe: 25.1. 2012, 11.30 Uhr

Aufgabe 1 Die Gruppe G operiere auf der Menge X, und $\mathcal{P}(X)$ bezeichne die Potenzmenge von X, d.h. die Menge aller Teilmengen von X. Zeigen Sie, dass die Abbildung

$$G \times \mathcal{P}(X) \longrightarrow \mathcal{P}(X)\,,\ (g, Y) \mapsto gY := \{g \cdot x \mid x \in Y\}$$

wohldefiniert und eine Operation von G auf $\mathcal{P}(X)$ ist.

Aufgabe 2 Seien G eine endliche, nicht-triviale Gruppe und p der kleinste Primteiler der Ordnung von G.

i) Zeigen Sie, dass jeder Normalteiler $N \subseteq G$ von Ordnung p im Zentrum von G liegt. Zeigen Sie durch zwei Beispiele, dass man hier weder auf die Vorraussetung, dass N Normalteiler ist, noch auf die Minimalität von p verzichten kann.

ii) Zeigen Sie, dass jede Untergruppe von G vom Index p ein Normalteiler ist. Zeigen Sie durch ein Beispiel, dass man hier auf die Minimalität von p nicht verzichten kann.

Hinweis: Für i) lassen Sie G durch Konjugation auf N operieren, für ii) auf der Menge aller zur gegebenen Untergruppe konjugierten Untergruppen.

Aufgabe 3 Für gegebene natürliche Zahlen $n, m \geq 1$ zeiegn Sie die Äquivalenz der folgenden Aussagen:

i) $(n, m) = 1$.

ii) Das Kreisteilungspolynom $\Phi_m(X) \in \mathbb{Q}(\zeta_n)[X]$ ist irreduzibel.

Aufgabe 4 Seien p eine Primzahl so, dass $p-1$ Produkt von paarweise verschiedenen Primzahlen ist, und bezeichne n die Anzahl dieser Primfaktoren. Zeigen Sie, dass $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ eine zyklische Galoiserweiterung ist, die 2^n Zwischenkörper besitzt. Bestimmen Sie die fünf kleinsten Primzahlen p, die die obige Bedingung erfüllen.

Zusatzaufgabe.
Seien $p \neq q$ positive Primzahlen. Zeigen Sie, dass alle von Null verschiedenen Koeffizienten des Kreisteilingspolynoms $\Phi_{pq}(X) \in \mathbb{Z}[X]$ Betrag 1 haben.
Hinweis: Zeigen Sie zunächst $\Phi_{pq}(X) = (1-X)\Phi_q(X^p)(1-X^q)^{-1}$, und überlegen Sie dann, wie man hier die geometrische Reihe anwenden kann.

Übungen zur Vorlesung
Algebra
Abgabe: 1.2. 2012, 11.30 Uhr

Aufgabe 1

i) Die Gruppe G operiere auf der Menge X. Zeigen Sie, dass durch $(g \mapsto (x \mapsto g \cdot x))$ ein Gruppenhomomorphismus $G \to \Sigma(X)$ definiert wird.

ii) Eine Gruppe der Ordnung 27 operiere auf einer Menge der Ordnung 50. Zeigen Sie, dass es mindestens 2 Fixpunkte geben muss.

iii) Sei N ein abelscher Normalteiler einer Gruppe G. Zeigen Sie, dass durch $(gN, n) \mapsto gng^{-1}$ eine Operation von G/N auf N definiert ist.

Aufgabe 2

i) Sei p prim. Zeigen Sie, dass die Untergruppe der strikt oberen Dreiecksmatrizen in $\mathrm{GL}_n(\mathbb{F}_p)$ eine p-Sylowgruppe ist. Geben Sie explizit ein Element an, welches die strikt oberen Dreiecksmatrizen in die strikt unteren Dreiecksmatrizen konjugiert.

ii) Sei G eine endliche Gruppe, und für jede Primzahl p sei S_p eine p-Sylowgruppe von G. Zeigen Sie, dass G genau dann isomorph ist zum Produkt der S_p, wenn G für jede Primzahl p genau eine p-Sylowgruppe hat.

iii) Seien p, q zwei (nicht notwendigerweise verschiedene) Primzahlen. Welche Gruppen der Ordnung pq gibt es bis auf Isomorphie?

iv) Klassifizieren Sie die Gruppen der Ordnung 2012 bis auf Isomorphie. Geben Sie für jede Gruppe die Anzahl der 2-Sylowgruppen, die Anzahl der Elemente der Ordnung 4, die Anzahl der Elemente der Ordnung 2 und das Zentrum an.

Aufgabe 3 Sei G eine endliche Gruppe. Zeigen Sie:

i) Ist G auflösbar, so ist auch jede Untergruppe von G auflösbar.

ii) Ist G auflösbar, so ist auch jede Quotientengruppe von G auflösbar.

iii) Sei $N \lhd G$. Sind N und G/N auflösbar, so auch G.

Aufgabe 4

i) Sei $n > 0$ und K ein Körper der Charakteristik 0, der die n-ten Einheitswurzeln enthält. Sei $a \in K^*$ und E ein Zerfällungskörper des Polynoms $X^n - a$. Zeigen Sie, dass durch $\sigma \mapsto \frac{\sigma(a)}{a}$ ein injektiver Homomorphismus von $\mathrm{Gal}(E/K)$ in die Gruppe der n-ten Einheitswurzeln definiert ist. Insbesondere ist $\mathrm{Gal}(E/K)$ zyklisch.

ii) Bestimmen Sie die Galoisgruppe des Zerfällungskörpers von $X^7 - 5$ über $\mathbb{Q}$.

Zusatzaufgabe.
Sei G eine endliche auflösbare Gruppe. Zeigen Sie, dass es eine Reihe $G = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_m = 1$ mit Normalteilern H_i von G gibt, so dass H_{i-1}/H_i abelsch ist.