Übungsblatt 10

Aufgabe 1. Sei G eine abelsche Gruppe mit Elementen $a, b \in G$ endlicher Ordnung $|a| = m$ und $|b| = n$. Zeigen Sie, dass in G ein Element der Ordnung $\mathrm{kgV}(m,n)$ existiert.

Beweis. Wir nehmen zunächst an, dass $\mathrm{ggT}(m,n) = 1$ gilt und betrachten das Element $z := ab \in G$. Sei nun $k \in \mathbb{N}$ mit $z^k = 1$. Im Folgenden zeigen wir, dass nm ein Teiler von k ist. Aus

$$a^{kn} = a^{kn} b^{kn} = \left(z^k\right)^n = 1$$

folgt $|a| = m \mid kn$. Und wegen $\mathrm{ggT}(m,n) = 1$ gilt $m \mid k$. Analog erhalten wir wegen

$$b^{km} = a^{km} b^{km} = \left(z^k\right)^m = 1$$

$|b| = n \mid km$ und somit $n|k$. Da $\mathrm{ggT}(m,n) = 1$ ist, gilt $mn \mid k$. Insbesondere erhalten wir, dass nm ein Teiler von $|z|$ ist, woraus $|z| = mn$ folgt.
Für den allgemeinen Fall betrachten wir das Element $a' := a^{\mathrm{ggT}(m,n)} \in G$ und stellen fest, dass es Ordnung $\frac{m}{\mathrm{ggT}(m,n)}$ hat. Da $\mathrm{ggT}(|a'|,|b|) = 1$ ist, gilt nach obiger Argumentation, dass $|a'b| = \frac{m}{\mathrm{ggT}(m,n)} \cdot n = \mathrm{kgV}(m,n)$, was die Behauptung beweist. □

Aufgabe 2. Sei K ein Körper und H eine endliche Untergruppe der multiplikativen Gruppe K^*. Zeigen Sie, dass H zyklisch ist. Bestimmen Sie alle endlichen Untergruppen der Gruppen $\mathbb{C}^*$ und $\mathbb{R}^*$.

Beweis. Da H endlich ist, gilt $o_{max} := \max_{h \in H} |h| \in \mathbb{N}$ und betrachte $H_{max} := \{h \in H \mid |h| \text{ teilt } o_{max}\}$. Zunächst rechnen wir nach, dass H_{max} eine Gruppe ist. Offensichtlich gilt $1 \in H_{max}$ und mit $h \in H_{max}$ auch $h^{-1} \in H_{max}$, da $|h| = |h^{-1}|$. Seien nun $h_1, h_2 \in H_{max}$, so erhalten wir

$$(h_1 h_2)^{o_{max}} = h_1^{o_{max}} h_2^{o_{max}} = 1,$$

woraus $|h_1 h_2| \mid o_{max}$ folgt. Also ist H_{max} eine Gruppe.
Jedes Element von H_{max} ist Nullstelle des Polynoms $X^{o_{max}} - 1$, somit gilt $|H_{max}| \leq \deg\left(X^{o_{max}} - 1\right) = o_{max}$. Sei nun $h_{max} \in H_{max}$ mit $|h_{max}| = o_{max}$, so gilt $\langle h_{max} \rangle \subseteq H_{max}$ und $|\langle h_{max} \rangle| = o_{max}$. Also ist $H_{max} = \langle h_{max} \rangle$ zyklisch.
Als nächstes zeigen wir, dass $H = H_{max}$ gilt. Nehmen wir hierfür das Gegenteil an, so existiert ein $h \in H \setminus H_{max}$. Nach Definition gilt $|h| \nmid o_{max}$. Nach Aufgabe 1 existiert ein $g \in H$ mit $|g| = \mathrm{kgV}(|h_{max}|, |h|) = \mathrm{kgV}(o_{max}, |h|)$. Da $|h| \nmid o_{max}$ gilt, ist $|g| = \mathrm{kgV}(o_{max}, |h|) > o_{max}$, ein Widerspruch zur Maximalität von o_{max}. □

Als nächstes berechnen wir die Untergruppen von $\mathbb{C}^*$ und $\mathbb{R}^*$. Sei $H \leq \mathbb{C}^*$ endlich mit $|H| = m$, so gilt nach vorherigem

$$H = \{z \in \mathbb{C}^* \mid z^m - 1 = 0\} = \left\{\exp\left(\frac{2k\pi}{m}\right) \mid 0 \leq k \leq m-1\right\}.$$

Also besteht die Gruppe H aus $m-$te Einheitswurzeln. Bezeichne deshalb H mit μ_m (üblicherweise wird diese Gruppe so bezeichnet).
Ist nun $H \leq \mathbb{R}^* \subseteq \mathbb{C}^*$ endlich mit Ordnung m, so gilt $H = \mu_m \cap \mathbb{R}^*$. Im Folgenden zeigen wir, dass $H = \{\pm 1\}$ für $m \in 2\mathbb{Z}$ und sonst $H = \{1\}$ gilt. Sei $\zeta \in H = \mu_m \cap \mathbb{R}^*$, so gilt $\zeta = \exp\left(\frac{2k\pi i}{m}\right)$ für ein $0 \leq k \leq m-1$. Es gilt genau dann

$$\zeta = \exp\left(\frac{2k\pi i}{m}\right) = \cos\left(\frac{2k\pi}{m}\right) + i \sin\left(\frac{2k\pi}{m}\right) \in \mathbb{R}^*,$$

wenn $\sin\left(\frac{2k\pi}{m}\right) = 0$. Letzteres gilt, wenn $\frac{2k\pi}{m} \in \mathbb{Z}\pi$. Sei also $2k = nm$ für ein $n \in \mathbb{Z}$, so gilt $\cos\left(\frac{2k\pi}{m}\right) = \cos\left(\frac{mn\pi}{m}\right) = \cos(n\pi) \in \{\pm 1\}$. Also ist $H \subseteq \{\pm 1\}$. Für $m \in 2\mathbb{Z}$ gilt offensichtlich $H = \{\pm 1\}$ und sonst $H = \{1\}$.

Aufgabe 3. Seien $K = \mathbb{F}_2$ und L der Körper $K[X]/(X^4 + X + 1)$. Geben Sie an, wie viele der $15 = 2^4 - 1$ Elemente von L^* jeweils welche Ordnung haben. Bestimmen Sie alle primitiven Elemente von $L|K$ explizit.
Zeigen Sie allgemein: Ein endlicher Körper der Ordnung q hat $\phi(q-1)$ primitive Elemente.

Beweis. Das Element der Ordnung 1 ist $\overline{1}$. Die Elemente der Ordnung 3 sind

$$\overline{x^2 + x} \text{ und } \overline{x^2 + x + 1}.$$

Die Elemente der Ordnung 5 sind

$$\overline{x^3},\ \overline{x^3 + x^2},\ \overline{x^3 + x^2 + x + 1} \text{ und } \overline{x^3 + x}$$

und alle übrigen Elemente haben die Ordnung 15.
Sei K ein endlicher Körper mit q Elementen, so ist K^* zyklisch der Ordnung $q-1$. Sei g ein Erzeuger der Gruppe, so gilt $|g^m| = \frac{|g|}{\mathrm{ggT}(m,|g|)} = \frac{q-1}{\mathrm{ggT}(m,q-1)}$. Letzteres sieht man wie folgt ein. Sei $n \in \mathbb{N}$ mit $g^{n \cdot m} = 1$, so gilt $|g| \mid nm$ und dementsprechend auch $\frac{|g|}{\mathrm{ggT}(|g|,m)} \mid n\frac{m}{\mathrm{ggT}(|g|,m)}$. Aus $\mathrm{ggT}\left(\frac{|g|}{\mathrm{ggT}(|g|,m)}, \frac{m}{\mathrm{ggT}(|g|,m)}\right) = 1$ folgt $\frac{|g|}{\mathrm{ggT}(|g|,m)} \mid n$ und somit $|g^m| = \frac{|g|}{\mathrm{ggT}(|g|,m)}$.
Also ist die Menge der primitiven Elemente von K^* gerade $\{g^m \mid 1 \le m \le q-1,\ \mathrm{ggT}(m, q-1) = 1\}$ und somit gibt es genau $\phi(q-1)$ primitive Elemente. □

Aufgabe 4. Sei k ein Körper der Charakteristik $p > 0$. Betrachte $K := k(X, Y) \subset L$, wobei L der Zerfällungskörper des Polynoms

$$(Z^p - X)(Z^p - Y) \in K[Z]$$

ist. In L existieren also p-te Wurzeln von X und Y, d.h. Elemente $x, y \in L$ mit $x^p = X$ und $y^p = Y$.

(1) Zeigen Sie, dass $L = K(x, y)$ und bestimmen Sie die Grade $[L : K]_s$ und $[L : K]$. Schließen Sie, dass $L|K$ nicht separabel ist.

(2) Zeigen Sie, dass $L|K$ nicht einfach ist.

Beweis. (1) Betrachte das Polynom $Z^p - X \in K[Z]$. Offensichtlich gilt mit $g(Z) = Z - X \in K[Z]$ die Gleichheit $Z^p - X = g(Z^p)$. Das Polynom g ist normiert, irreduzibel und separabel über K, sodass wir nach Vorlesung erhalten, dass $x = \sqrt[p]{X}$ eine p-fache Nullstelle von $Z^p - X$ ist. Insbesondere ist x die einzige Nullstelle des Polynoms. Analoges gilt für $Z^p - Y$ und y. Der Zerfällungskörper von $(Z^p - X)(Z^p - Y)$ ist somit $L = K(x, y)$.
Da x die einzige Nullstelle vom irreduziblen Polynom $Z^p - X$ (siehe Blatt 8 Aufgabe 4) ist, gilt

$$[K(x) : K]_s = \left|\left\{b \in \overline{K} \mid b^p - X = 0\right\}\right| = 1$$

und analog, da y die einzige Nullstelle von $Z^p - Y$ und $y \notin K(x)$ gilt, ist

$$[L : K(x)]_s = \left|\left\{b \in \overline{K(x)} = \overline{K} \mid b^p - Y = 0\right\}\right| = 1.$$

Mit der Gradformel des Separabilitätsgrades erhalten wir

$$[L : K]_s = [K(x, y) : K(x)]_s \cdot [K(x) : K]_s = 1 \cdot 1 = 1.$$

Da die Nullstellen x bzw. y mit Vielfachheit p in ihren Minimalpolynomen über K auftreten, erhalten wir nach Vorlesung

$$[L : K] = [L : K(x)] \cdot [K(x) : K] = p[L : K(x)]_s \cdot p[K(x) : K]_s = p^2.$$

Da $[L : K] \neq [L : K]_s$ ist, ist die endliche Erweiterung $L|K$ nicht separabel.

(2) Offensichtlich ist $\left\{x^i y^j \mid 1 \leq i,j \leq p\right\}$ eine K–Basis von L. Sei $z \in L$, so existieren $\lambda_{i,j} \in K$ mit $1 \leq i,j \leq p$ und $z = \sum_{1\leq i,j\leq p} \lambda_{i,j} x^i y^j$. Aus letzterem folgt mit 'Freshman's dream'

$$z^p = \sum_{1\leq i,j\leq p} \lambda_{i,j}^p x^{pi} y^{pj} = \sum_{1\leq i,j\leq p} \lambda_{i,j}^p X^i Y^j \in K.$$

Also erhalten wir, dass $Z^p - z^p \in K[Z]$ und somit ist das Minimalpolynom von z über K ein Teiler von $Z^p - z^p$. Letzteres impliziert, dass $[K(z) : K] \leq p < [L : K]$ gilt. Also ist $L|K$ keine einfache Erweiterung.

□