D-MATH Algebra II FS21
Prof. Marc Burger

Lösung 3

Körpererweiterungen und Zerfällungskörper

1. Es seien $a, b \in \mathbb{Q}$ rationale Zahlen für die $f = X^2 + a$ und $g = X^2 + b$ irreduzibel über $\mathbb{Q}$ sind. Zeigen Sie, dass die Zerfällungskörper von f und g genau dann isomorph sind, wenn $\frac{a}{b}$ ein Quadrat in $\mathbb{Q}$ ist.

2. Sei p eine Primzahl ungleich 2 und 5. Zeigen Sie, dass von den natürlichen Zahlen, die nur Einsen in ihrer Dezimaldarstellung haben, d.h. 1, 11, 111, 1111, ..., mindestens eine durch p teilbar ist.

3. Seien $L_1|K_1$ und $L_2|K_2$ zwei endliche Körpererweiterungen und $\varphi : L_1 \to L_2$ ein Isomorphismus von Körpern mit $\varphi(K_1) = K_2$. Zeigen Sie, dass $[L_1 : K_1] = [L_2 : K_2]$.

4. Sei p eine Primzahl. Zeigen Sie, dass

$$(p-1)! + 1 \equiv 0 \pmod{p},$$

indem Sie $X^{p-1} - 1$ über $\mathbb{F}_p$ faktorisieren.

Lösung: Die obige Gleichheit gilt für $p = 2$. Sei also von nun an p eine ungerade Primzahl. Nach dem kleinen Fermat, gilt für jedes $x \in \mathbb{F}_p^\times$, dass $x^{p-1} = 1$, was nichts anderes heisst, als dass x eine Nullstelle von $X^{p-1} - 1 \in \mathbb{F}_p[X]$ ist, und damit gilt $(X - x)|X^{p-1} - 1$. Da $|\mathbb{F}_p^\times| = p - 1 = \deg(X^{p-1} - 1)$ und $\mathbb{F}_p[X]$ ein faktorieller Ring ist, folgern wir, dass

$$X^{p-1} - 1 = \prod_{x \in \mathbb{F}_p^\times} (X - x).$$

Ausgewertet bei $0 \in \mathbb{F}_p$, erhalten wir, dass $0 = 1 + (-1)^{p-1} \prod_{x \in \mathbb{F}_p^\times} x = 1 + \prod_{x \in \mathbb{F}_p^\times} x$. Da wir $1, 2, \ldots, p-1$ als die Representanten der Elemente in $x \in \mathbb{F}_p^\times$ wählen können, gilt die gewünschte Gleichheit.

5. Sei $f = X^3 - X + 1 \in \mathbb{F}_3[X]$.

   (a) Zeigen Sie, dass f irreduzibel in $\mathbb{F}_3[X]$ ist.

   (b) Zeigen Sie, dass falls E ein Zerfällungskörper von f ist und $\rho \in E$ eine Nullstelle von f, so auch $\rho + 1$ und $\rho - 1$.

   (c) Konstruieren Sie einen Zerfällungskörper von f und berechnen Sie explizit das Produkt zweier beliebiger Elemente in diesem Zerfällungskörper.

(d) Beschreiben Sie explizit die Wirkung von $\mathrm{Gal}(E|\mathbb{F}_3)$ auf die Elemente von E.

Lösung:

(a) Da f Grad drei hat, genügt es zu zeigen, dass f keine Nullstelle in $\mathbb{F}_3[X]$ hat. Es gilt $(0) = f(1) = f(-1) = 1$, und damit ist f irreduzibel in $\mathbb{F}_3[X]$.

(b) Die Abbildung $x \mapsto x^3$ ist ein Körperautomorphismus von K, falls K Charakteristik 3 hat, der die Identität auf $\mathbb{F}_3$ ist. Für $\varepsilon \in \mathbb{F}_3$ erhalten wir daher

$$f(\rho+\varepsilon) = (\rho+\varepsilon)^3 - (\rho+\varepsilon) + 1 = \rho^3 + \varepsilon^3 - \rho - \varepsilon + 1 = f(\rho) + \varepsilon - \varepsilon = 0.$$

Dies impliziert, dass $\rho+1$ und $\rho-1$ Nullstellen von f sind, falls ρ Nullstelle von f ist.

(c) Aus b) folgt, dass jede Körpererweiterung E, die eine Nullstelle ρ von f enthält, alle drei verschiedenen Nullstellen von f enthält, und damit ist E ein Zerfällungskörper von f. Eine solche Körpererweiterung erhalten wir durch

$$E = \mathbb{F}_3[X]/(f) \cong \{a + b\rho + c\rho^2 : a, b, c \in \mathbb{F}_3\},$$

wobei wir Elemente in der rechten Menge koeffizientenweise addieren, und die Multiplikation ist induziert durch die Bijektion $\mathbb{F}_3[X]/(f) \cong \{a + b\rho + c\rho^2 : a, b, c \in \mathbb{F}_3\}$, welche $X \mapsto \rho$ sendet. Dies bedeutet nichts anderes als dass wir zwei Elemente aus der rechten Menge multiplizieren können als wären sie Polynome in ρ und anschliessend vereinfachen wir die Ausdrücke vom Grad drei oder vier mithilfe der Bedingungen $\rho^3 = \rho - 1$ und $\rho^4 = \rho(\rho-1) = \rho^2 - \rho$ zu einem Ausdruck vom Grad zwei. Wir erhalten also für $a + b\rho + c\rho^2, a' + b'\rho + c'\rho^2 \in \{a + b\rho + c\rho^2 : a, b, c \in \mathbb{F}_3\}$ das Produkt

$$\begin{aligned}
&(a + b\rho + c\rho^2)(a' + b'\rho + c'\rho^2) \\
&= aa' + (ab' + a'b)\rho + (ac' + bb' + ca')\rho^2 + (bc' + cb')\rho^3 + cc'\rho^4 \\
&= aa' + (ab' + a'b)\rho + (ac' + bb' + ca')\rho^2 + (bc' + cb')(\rho - 1) + cc'(\rho^2 - \rho) \\
&= aa' - bc' - cb' + (ab' + a'b + bc' + cb' - cc')\rho + (ac' + bb' + ca' + cc')\rho^2.
\end{aligned}$$

6. Sei p eine Primzahl.

(a) Zeigen Sie, dass ein Element der Ordnung p in S_p ein p-Zykel ist.

(b) Zeigen Sie, dass eine Transposition und ein p-Zykel S_p erzeugen.

Lösung:

(a) Jedes $\sigma \in S_p$ kann als Produkt von disjunkten Zykeln $\sigma_1, \ldots, \sigma_n$ der Länge $\ell_1, \ldots, \ell_n$ mit $\sum_{i=1}^n \ell_i = p$ geschrieben werden. Da disjunkte Zykel kommutieren, erhalten wir für jedes $k \in \mathbb{N}$

$$\sigma^k = \sigma_1^k \cdots \sigma_n^k.$$

Die Permutationen $\sigma_1^k, \ldots, \sigma_n^k$ haben disjunkte Träger (die Elemente, die von σ_i permutiert werden und nicht von σ_j für $i \neq j$), so dass folgt, dass $\sigma^k = \mathrm{id}$ genau dann, wenn $\sigma_i^k = \mathrm{id}$ für alle $i = 1, \ldots, n$. Da die Ordnung von σ_i gerade ℓ_i ist (σ_i ist ein Zykel der Länge ℓ_i), folgt, dass $\sigma^k = \mathrm{id}$ genau dann, wenn $\ell_i | k$ für alle i. Dies bedeutet, dass $p = \mathrm{ord}(\sigma) = \mathrm{lcm}(\ell_1, \ldots, \ell_n)$. Da $\ell_i \leqslant p$ für alle i sehen wir, dass $\ell_i \in \{1, p\}$ für alle i (p ist eine Primzahl) und dass eins der ℓ_i gerade gleich p ist. Nun ist $\sum_{i=1}^n \ell_i = p$, woraus folgt, dass die einzige Möglichkeit $n = 1$ mit $\ell_1 = p$ ist, was nichts anderes heisst, als dass σ ein p-Zykel ist.

(b) Ein beliebiger p-Zykel in S_p kann als $(1\,2\,\ldots\,p)$ geschrieben werden (indem wir die Objekte, die permutiert werden, umbenennen), das heisst, um zu zeigen, dass eine beliebige Transposition und ein p-Zykel S_p erzeugen, genügt es zu zeigen, dass jede Transposition und der p-Zykel $\tau = (1\,2\,\ldots\,p)$ S_p erzeugen. Sei $(i\,j)$ eine beliebige Transposition mit $1 \leqslant i < j \leqslant p$. Es gilt $\tau^{j-i}(i) = j$ und da p prim, teilt $j - i$ p nicht, und damit ist $\langle \tau \rangle = \langle \tau^{j-i} \rangle$, also ein p-Zykel, der i auf j schickt, d.h. $\tau^{j-i} = (i\,j\,\ldots)$. Dann gilt

$$\langle (i\,j), \tau \rangle = \langle (i\,j), \tau^{j-i} \rangle = \langle (i\,j), (i\,j\,\ldots) \rangle,$$

und nach Umnummerierung (dies ist nichts anderes als eine Konjugation in S_p) können wir annehmen, dass

$$(i\,j) = (1\,2) \text{ und } (i\,j\,\ldots) = (1\,2\,3\,\ldots\,p).$$

Nun ist es nicht schwierig zu sehen, dass für alle $k = 1, \ldots, p-1$

$$(1\,2\,3\,\ldots\,p)^{k-1}(1\,2)(1\,2\,3\,\ldots\,p)^{-(k-1)} = (k\,k+1).$$

Behauptung: S_n wird von den $n-1$ Transpositionen $(1\,2), (2\,3), \ldots, (n-1\,n)$ erzeugt ($n \in \mathbb{N}$ beliebig).

Beweis: Wir wissen bereits aus Algebra I, Serie 10, Aufgabe 1a), dass S_n von allen Transpositionen erzeugt wird. Es genügt also zu zeigen, dass jede Transposition $(i\,j)$ ein Produkt von Transpositionen der Form $(a\,a+1)$ mit $a < n$ ist. OBdA ist $i < j$. Wir machen eine Induktion über $j - i$. Die Aussage ist klar, falls $j - i = 1$. Sei nun $j - i = k > 1$ und wir nehmen an, die Aussage gilt für alle Transposition von Paaren von natürlichen Zahlen mit Differenz kleiner als k. Betrachte die Gleichheit

$$(i\,j) = (i\,i+1)(i+1\,j)(i\,i+1).$$

Das Element $(i\,i+1)$ ist in unserem Erzeugendensystem und die mittlere Transposition permutiert ein Paar von natürlichen Zahlen mit Differenz $j - (i+1) = k - 1 < k$. Nach Induktionsannahme ist $(i+1\,j)$ ein Produkt von Transpositionen der Form $(a\,a+1)$, und somit auch $(i\,j)$, was zu zeigen war.