Galoistheorie, WS 08/09

Blatt 4

Aufgabe 10 (4+2 Punkte)

(1) Sei R ein Integritätsbereich. Sei $K \subseteq R$ ein Teilkörper von R, d.h. ein Teilring, der ein Körper ist. Sei R als K-Vektorraum endlichdimensional. Zeige, daß R ein Körper ist.

(2) Finde ein $n \geqslant 0$ und eine Basis $(z_1, \ldots, z_n)$ von $\mathbf{C}$ als $\mathbf{R}$-Vektorraum so, daß für alle $i \in [1, n]$ ein $j \in [1, n]$ mit $\bar{z}_i = z_j$ existiert.

Aufgabe 11 ((2+2+2)+4+5 Punkte)

Die Ordnung eines Elements g in einer (multiplikativ geschriebenen) endlichen Gruppe G ist definiert als $\mathrm{o}(g) := \min\{n \in \mathbf{Z}_{\geqslant 1} \ : \ g^n = 1\}$. (Diese existiert, da wegen der Endlichkeit von G es $0 \leqslant k < \ell$ mit $g^k = g^\ell$ geben muß, woraus $g^{\ell - k} = 1$ folgt.)

Schreibe $b\langle a\rangle := \{ba^k \ : \ k \in \mathbf{Z}\}$ für $a,\, b \in G$.

Schreibe $\mathbf{F}_p^\times := \mathbf{F}_p \smallsetminus \{0\}$ für p prim.

(1) Sei $a \in G$ gegeben.

 (a) Zeige, daß für $b,\, b' \in G$ entweder $b\langle a\rangle = b'\langle a\rangle$ oder $b\langle a\rangle \cap b'\langle a\rangle = \emptyset$.

 (b) Zeige, daß $|b\langle a\rangle| = \mathrm{o}(a)$ für alle $b \in G$.

 (c) Folgere, daß $\mathrm{o}(a)$ ein Teiler von $|G|$ ist.

(2) Bestimme alle Elementordnungen in $(\mathbf{F}_7^\times, \cdot)$. Verifiziere (1.c) in diesem Beispiel.

(3) Bestimme alle Elementordnungen in $(\mathbf{F}_{11}^\times, \cdot)$. Verifiziere (1.c) in diesem Beispiel.

Aufgabe 12 (5+3+3+3 Punkte)

Sei p prim.

(1) Sei $a \in \mathbf{F}_p$. Zeige, daß $a^p = a$ (Kleiner Fermatscher Satz; Hinweis: Aufgabe 11.(1.c)).

(2) Zeige, daß $X^p - X = \prod_{i \in \mathbf{F}_p} (X - i)$ in $\mathbf{F}_p[X]$. (Hinweis: (1).)
Berechne $\prod_{i \in [0, 3-1]} (X - i)$ in $\mathbf{Z}[X]$ und vergleiche.

(3) Zeige, daß $(p-1)! \equiv_p -1$ (Satz von Wilson; Hinweis: Koeffizientenvergleich in (2)).
Ist $(n-1)! \equiv_n -1$ für alle $n \in \mathbf{Z}_{\geqslant 1}$?

(4) Sei $p \geqslant 3$. Sei $s(p) := \sum_{i \in [1, p-1]} \frac{1}{i}$. Zeige, daß der Zähler von $s(p)$ in gekürzter Bruchschreibweise durch p teilbar ist.
(Hinweis: Koeffizientenvergleich bei X^2 in (2)).