Probeklausur - eine Lösung

Aufgabe 1
Sei p eine Primzahl, $n \in \mathbb{N}$, $q = p^n$ und $\mathbb{F}_q$ der Körper mit q Elementen. Sei $G = \mathrm{GL}_2(\mathbb{F}_q)$.

a) Bestimmen Sie $\#G$.

b) Zeigen Sie, dass $P = \{\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbb{F}_q\}$ eine p-Sylowgruppe ist.

c) Bestimmen Sie den Normalisator $N := \{g \in G : gPg^{-1} = P\}$ von P.
(*Hinweis:* Es reicht, diejenigen $g \in G$ zu finden, so dass $ghg^{-1} \in P$ für alle $h \in P$ gilt.)

d) Bestimmen Sie die Anzahl der p-Sylowgruppen in G.

Lösung Aufgabe 1

a) Die erste Spalte ist ein Vektor aus $\mathbb{F}_q^2$, aber – da die Determinante nicht 0 ist – nicht der Nullvektor, also gibt es $q^2 - 1$ Möglichkeiten für die erste Spalte. Die Determinante ist genau dann 0, wenn die Spalten linear abhängig sind, wenn also die zweite Spalte aus dem Erzeugnis der ersten Spalte gewählt wird: Dieses Erzeugnis hat die Mächtigkeit q, schließlich ist es ein eindimensionaler $\mathbb{F}_q$-Vektorraum.
Für jede Wahl der ersten Spalte haben wir also q Vektoren, die wir nicht als zweite Spalte wählen dürfen, also $q^2 - q$ mögliche zweite Spalten.
Insgesamt gibt das $(q^2 - 1)(q^2 - q)$ invertierbare Matrizen, dies ist die gesuchte Mächtigkeit.

b) Wegen $\#G = q(q-1)(q^2-1)$ und da $p|q$, aber $p \nmid 1$ ist $q = p^n$ die maximale p-Potenz, die $\#G$ teilt, und als solche die Mächtigkeit der p-Sylowgruppen.
Wir müssen also zeigen, dass P eine Untergruppe der Ordnung q ist, wobei letzteres offensichtlich ist.
P ist aber auch eine Untergruppe, denn $P \neq \emptyset$ (etwa $I_2 \in P$) und für $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \in P$ beliebig ist $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix} \in P$ und $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix} \in P$.

c) Für ein $g \in G$ ist die Bedingung $ghg^{-1} \in P$ für alle $h \in P$ äquivalent zu $gPg^{-1} \subseteq P$. Da Konjugieren mit g injektiv ist, gilt $\#gPg^{-1} = \#P$, was mit „$\subseteq$“ und der Endlichkeit der Mengen die Gleichheit erzwingt, also gilt tatsächlich $N = \{g \in G : ghg^{-1} \in P \text{ für alle } h \in P\}$.
Seien $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in P$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ mit inverser Matrix $\frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, so ist
$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \cdot \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{ad-bc}\begin{pmatrix} ad-bc-acx & * \\ -c^2x & ad-bc+acx \end{pmatrix}$.
Es ist $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in N$, wenn die letzte Matrix für beliebiges $x \in \mathbb{F}_q$ (also für alle $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in P$) Element aus P ist, das ist genau dann der Fall, wenn $-c^2x = -acx = 0$ für alle x gilt, was offensichtlich genau für $c = 0$ der Fall ist.

Also ist $N = \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, d \in \mathbb{F}_q^\times, b \in \mathbb{F}_q\}$ der Normalisator, wobei die Einschränkung an a, d folgt, weil die Determinante ungleich 0 sein muss.

d) Es ist $\#N = q(q-1)(q-1) = (q^2-q)(q-1)$, was direkt aus c) folgt.
G operiert auf der Menge M der p-Sylowgruppen durch Konjugation. Die Operation ist transitiv nach Sylow, insbesondere ist also $GP = M$, der Stabilisator von P ist N nach Definition. Im Beweis der Bahnbilanzformel haben wir gelernt, wie wir dann $\#M$ ausrechnen können, denn es gilt:
$\#M = \#GP = [G : \mathrm{Stab}_P] = \frac{\#G}{\#\mathrm{Stab}_P} = \frac{(q^2-1)(q^2-q)}{(q^2-q)(q-1)} = q + 1$.

Aufgabe 2
Sei N eine natürliche Zahl, die $2^N - 1$ teilt. Zeigen Sie die folgenden Aussagen:

a) N ist ungerade.

b) Sei p ein Primteiler von N und $a := \mathrm{ggT}(p-1, N)$. Dann ist p ein Teiler von $2^a - 1$.

c) $N = 1$.

Lösung Aufgabe 2

a) Sicher ist $2^N - 1$ ungerade, also auch jeder Teiler, insbesondere N.

b) Nach dem kleinen Satz von Fermat gilt $p|(2^{p-1} - 1)$ und nach der Aufgabenstellung gilt $p|(2^N - 1)$. $(*)$
Es reicht zu zeigen, dass dann $p|(2^{k(p-1)+lN} - 1)$ für alle $k, l \in \mathbb{Z}$ gilt (**Behauptung**), dann folgt die Aussage, da wir den ggT a als solche Linearkombination schreiben können.
Die Behauptung rechnen wir direkt nach, denn es ist wegen der Vorüberlegung $(*)$ $2^{p-1} \equiv 1\ (p), 2^N \equiv 1\ (p)$, also $2^{k(p-1)+lN} = (2^{p-1})^k \cdot (2^N)^l \equiv 1^k \cdot 1^l \equiv 1\ (p)$, was die Behauptung zeigt.

c) Wäre nun $N \neq 1$, so hätte N einen kleinsten Primteiler p_0. Für diesen gilt $\mathrm{ggT}(p_0 - 1, N) = 1$. Dann aber teilt p_0 wegen b) $2^1 - 1 = 1$, was für eine Primzahl p_0 sicher nicht sein kann.
WIDERSPRUCH
Es folgt $N = 1$.

Aufgabe 3
Sei $I = (2, X) \trianglelefteq \mathbb{Z}[X]$ das von 2 und X erzeugte Ideal. Zeigen Sie die nachfolgenden Aussagen:

a) Für alle n ist I^n das Erzeugnis von $2^n, 2^{n-1}X, ..., 2X^{n-1}, X^n$.

b) Für $n \geq 1$ ist I^n kein Hauptideal.

Lösung Aufgabe 3

a) Allgemein gilt: Wird ein Ideal I von einem System $\{b_i\}_{i \in A}$ und ein Ideal J von einem System $\{c_j\}_{j \in B}$ erzeugt (wobei A, B beliebige Indexmengen sind), so wird $I \cdot J$ vom System aller Produkte $\{b_i c_j\}_{i \in A, j \in B}$ erzeugt. Dies sieht man leicht ein, wenn man die Elemente aus $I \cdot J$ (womit das Ideal, das von den Produkten ij erzeugt wird, gemeint ist) hinschreibt.
Damit folgt die Behauptung per Induktion:
Sicher ist sie wahr für $n = 1$, das ist ja gerade die Definition von I.
Sei die Aussage richtig für n, also I^n erzeugt von $\{2^n, 2^{n-1}X, ..., X^n\}$. Nach der Vorüberlegung wird $I^{n+1} = I \cdot I^n$ von allen Produkten aus $\{2^n, 2^{n-1}X, ..., X^n\}$ und $\{2, X\}$, was gerade $\{2^{n+1}, ..., X^{n+1}\}$ entspricht, erzeugt.

b) In I^n liegen die Elemente 2^n und X^n. Wäre I^n ein Hauptideal, so gäbe es einen Erzeuger k, der 2^n und X^n teilt, aber da 2^n Grad 0 hat, muss k ebenfalls Grad 0 haben, also $k \in \mathbb{Z}$. Da weiterhin $k|X^n$ gilt, muss k den Leitkoeffizienten 1 teilen, also ist $k \in \{\pm 1\}$ eine Einheit, es folgt $J = \mathbb{Z}[X]$. Aber alle Polynome aus J haben als konstantes Glied eine gerade Zahl, also $J \neq \mathbb{Z}[X]$.
WIDERSPRUCH

Aufgabe 4
Berechnen Sie alle $z \in \mathbb{Z}$, die die nachfolgenden Kongruenzen erfüllen:
$z \equiv 4$ (19)
$z \equiv 12$ (37)
$z \equiv 14$ (43)
(*Hinweis:* Inverse modulo natürlicher Zahlen lassen sich mit Hilfe des euklidischen Algorithmus bestimmen.)

Lösung Aufgabe 4

Wir fangen mit den ersten beiden Kongruenzbedingungen an. Es ist also

$$z = 4 + 19k \equiv 12 \pmod{37},$$

was $19k \equiv 8 \pmod{37}$ bedeutet und nach Multiplikation mit 2 schließlich

$$k \equiv 16 \pmod{37}.$$

Demnach können wir wegen $19 \cdot 37 = 703$ weitermachen mit

$$z = \underbrace{4 + 16 \cdot 19}_{=308} + 703m \equiv 14 \pmod{43},$$

was wegen $308 = 7 + 7 \cdot 43$ und $703 = 16 \cdot 43 + 15$ auf

$$15m \equiv 7 \pmod{43}$$

führt.

Da wir weiterhin $20 \cdot 15 = 300 = 7 \cdot 43 - 1$ schon gesehen haben, ist modulo 43 die Inverse von 15 gleich -20. Es folgt

$$m \equiv -140 \equiv -11 \pmod{43}.$$

Dies wiederum führt auf

$$z = 308 - 7733 + n \cdot 30229 = -7425 + n \cdot 30229$$

als allgemeine Lösung der angegebenen simultanen Kongruenzbedingungen.

Aufgabe 5
Es sei $A \leq \mathbb{C}$ eine Untergruppe (bezüglich $+$) und

$$R := \{z \in \mathbb{C} : zA \subseteq A\}.$$

Zeigen Sie die folgenden Aussagen:

a) R ist ein Teilring von $\mathbb{C}$ und A ein R-Untermodul von $\mathbb{C}$.

b) Aus $1 \in A$ folgt $R \subseteq A$.

c) Ist $A \neq \{0\}$ endlich erzeugt, so sind R und A frei abelsch. Der Rang von $(R, +)$ ist dabei kleinergleich dem Rang von $(A, +)$.

d) Finden Sie ein Beispiel für $A \leq \mathbb{C}$ mit $1 \in A, A \not\subseteq \mathbb{Z}, R = \mathbb{Z}$.

Lösung Aufgabe 5

a) Offensichtlich gilt $1 \in R$. Für $r, s \in R$ und $a \in A$ ist weiterhin $(r - s) \cdot a = ra - sa \in A$, da A eine Gruppe bezüglich der Addition ist, und auch $(rs)a = r(sa) \in A$, da laut Definition $sa \in A$ gilt und damit auch $r(sa) \in A$.

Damit ist R ein Teilring von $\mathbb{C}$, was $\mathbb{C}$ zu einem R-Modul macht, und A ist ein R-Untermodul von $\mathbb{C}$, da es eine Untergruppe ist und unter der Multiplikation mit Elementen aus R invariant.

b) Mit $1 \in A$ gilt für alle $r \in R$ auch $r = r \cdot 1 \in A$.

c) Wenn A endlich erzeugt ist, so kann man den Struktursatz für endlich erzeugte abelsche Gruppen anwenden, und A ist eine direkte Summe von zyklischen Gruppen. Da es in A aber außer 0 keine Elemente endlicher Ordnung gibt, denn wir sind in einem $\mathbb{R}$-Vektorraum, ist A torsionsfrei, also sind alle direkten Summanden von A unendliche zyklische Gruppen, also ist A frei abelsch.

Sei nun $a \in A$ von Null verschieden. Dann ist R als abelsche Gruppe isomorph zu $Ra \subset A$, denn die Multiplikation mit a ist injektiv. Als Untergruppe einer frei abelschen Gruppe ist auch Ra frei abelsch, und der Rang ist nicht größer als der von A (laut einem Vorlesungssatz, wo dies für $\mathbb{Z}^n$ formuliert wurde). Dies gilt dann auch für R.

d) Zum Beispiel $\frac{1}{2}\mathbb{Z}$ würde das erfüllen, denn wegen b) muss ja $R \subset A$ gelten, und für $s \in A \setminus \mathbb{Z}$ ist $s^2 \notin A$, also liegt R in $\mathbb{Z}$.

Auch $A = \mathbb{Z} + \mathbb{Z}\sqrt[3]{2}$ wäre ein nettes Beispiel, wo sogar der Rang größer ist.

Aufgabe 6

Gegeben sei die Matrix $A = \begin{pmatrix} 2 & 1 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \in \mathbb{Z}^{3\times 3}$.

Bestimmen Sie unimodulare Matrizen S, T, so dass SAT in Elementarteilernormalform vorliegt. Geben Sie die Elementarteil $a_1|a_2|a_3$ an.

Finden Sie anschließend $\mathbb{Z}$-Basen $B = \{b_1, b_2, b_3\}$ von $H = \langle \begin{pmatrix} 2 \\ 4 \\ 7 \end{pmatrix}, \begin{pmatrix} 1 \\ 5 \\ 8 \end{pmatrix}, \begin{pmatrix} 3 \\ 6 \\ 9 \end{pmatrix} \rangle$ und $C = \{c_1, c_2, c_3\}$ von $\mathbb{Z}^3$, so dass $b_i = a_i c_i$ für $i = 1, 2, 3$ gilt.

Lösung Aufgabe 6 Ach du je...

Wir ziehen erst die erste Spalte von der dritten ab, dann die zweite von der ersten und schließlich die neue erste von den beiden anderen, multiplizieren also A mit

$$\begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 & -2 \\ -1 & 2 & 1 \\ 0 & 0 & 1 \end{pmatrix} = T_1,$$

was

$$A \cdot T_1 := A_1 = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 6 & 3 \\ -1 & 9 & 3 \end{pmatrix}$$

liefert. Nun radieren wir durch Multiplikation mit

$$S_1 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

von links die erste Spalte etwas sauberer und erhalten

$$A_2 = S_1 A T_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 6 & 3 \\ 0 & 9 & 3 \end{pmatrix}.$$

Nun vertauschen wir die letzten beiden Spalten und ziehen das Doppelte der zweiten von der dritten ab. Wir multiplizieren also von rechts mit der Matrix

$$T_2 := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & -2 \end{pmatrix} \text{ und erhalten } A_3 = S_1 A T_1 T_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 3 & 3 \end{pmatrix},$$

und Subtrahieren nun die zweite Zeile von der dritten durch Linksmultiplikation mit $S_2 := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix}$.

Mit $S := S_2 S_1 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix}$ und $T := T_1 T_2 = \begin{pmatrix} 1 & -2 & 3 \\ -1 & 1 & 0 \\ 0 & 1 & -2 \end{pmatrix}$ bekommen wir

$$\tilde{A} = SAT = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

Die Elementarteiler sind demnach 1, 3, 3, und wegen $AT\mathbb{Z}^3 = S^{-1}\tilde{A}\mathbb{Z}^3$ sind die Spalten von AT eine mögliche Wahl für B, also

$$B = \{\begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix}\} \text{ und damit } C = \{\begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}\}.$$