Martin Goldstern

Prüfung ALGEBRA, 2013-06-27

Mit „Beschreiben Sie alle X“ ist im folgenden gemeint:

- Geben Sie an, ob es X gibt. Gibt es endlich oder unendlich viele, abzählbar oder überabzählbar viele? Wenn nach algebraischen (oder topologischen, etc) Strukturen gefragt ist, sind wir nicht an der tatsächlichen Anzahl der Strukturen interessiert, sondern nur „bis auf Isomorphismus“; gesucht ist also eine Liste von paarwise nichtisomorphen X, sodass jedes X zu einem X auf der Liste isomorph ist.
- Wenn es endlich viele gibt, geben Sie an, wie viele (zumindest eine obere Schranke). Wenn möglich und sinnvoll, zählen Sie sie alle auf. (Zählen Sie die X systematisch auf — etwa geordnet nach der Größe, nach der Anzahl der Primelemente, nach der größten auftretenden Ordnung, etc, um sicher zu sein, nichts übersehen zu haben.)
- Wenn es abzählbar unendlich viele, überlegen Sie, ob es eine sinnvolle systematische Anordnung gibt; vielleicht kann man alle X mit den natürlichen Zahlen indizieren, oder mit Paaren natürlicher Zahlen, etc.

1. Wir betrachten in dieser Aufgabe Integritätsbereiche. Definieren Sie die folgenden Begriffe:

   (a) Integritätsbereich, euklidischer Ring, faktorieller Ring, Hauptidealring. Welche Implikationen gelten zwischen diesen Begriffen? (Ohne Beweis.)
   Geben Sie (ohne Beweis) an, welche der folgenden Ringe welche der 4 Eigenschaften erfüllen: $\mathbb{Z}$, $\mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}[x]$, $\mathbb{Z}[x,y]$, $\mathbb{Q}[x]$, $\mathbb{Q}[x,y]$.

   (b) teilbar, Einheit, ggT, Hauptideal.

   (c) prim, irreduzibel. Welche Implikation bzw Äquivalenzen gelten zwischen diesen Begriffen

      i. in allen Integritätsbereichen?

      ii. in allen euklidischen Ringen?

      iii. in allen faktoriellen Ringen?

      (Implikationen nur angeben, nicht beweisen.)

   Achten Sie darauf, logische Symbole (oder die entsprechenden Worte, wie „und“, „wenn–dann“, „es gibt“, „für alle“) korrekt zu verwenden. Wenn Sie etwa eine Aussage formulieren, die für alle x gilt, dann schreiben Sie auch „für alle x“ oder „$\forall x$“, etc.)

2. Sei K die Klasse aller abelschen Gruppen $(G, \cdot, 1, ^{-1})$, die $\forall x \in G : x^{2013} = 1$ erfüllen.

   (a) Geben Sie eine Beschreibung aller endlichen Gruppen in K an, und beantworten Sie mit Hilfe dieser Beschreibung die folgenden Fragen.

   (b) Beschreiben Sie alle Strukturen in K mit höchstens 10 Elementen.

   (c) Wie viele Gruppen in K werden von der leeren Menge erzeugt?

   (d) Wie viele Gruppen in K werden von einer höchstens einelementigen Teilmenge erzeugt?

   (e) Wie viele Gruppen in K werden von einer höchstens zweielementigen Teilmenge erzeugt?

   (f) Zeigen Sie, dass C_{2013} in K frei ist. (Frei von welcher Menge erzeugt?)

   (g) Beschreiben Sie die in K von zwei Elementen frei erzeugte Struktur.

   Begründen Sie Ihre Antworten.
   Hinweise: Mit C_{2013} bezeichnen wir die zyklische Gruppe mit 2013 Elementen. Verwenden Sie den Darstellungssatz für endliche abelsche Gruppen. $2013 = 3 * 11 * 61$.

3. Sei p eine Primzahl, $P = GF(p)$ der Körper mit p Elementen, L ein endlicher Körper mit $P \leq L$. Für $k = 1, 2, \ldots$ sei $\varphi_k : L \to L$ die durch $\alpha \mapsto \alpha^k$ definierte Abbildung. Mit $\varphi_k \restriction P$ bezeichnen wir die Einschränkung von φ_k auf P.

   (a) Zeigen Sie, dass die Abbildung φ_p ein Automorphismus von L ist. Schließen Sie, dass auch die Abbildungen φ_{p^2}, φ_{p^3} etc. Automorphismen von L sind.

   (b) Zeigen Sie, dass es außer der Identität keine Automorphismen von P gibt. Schließen Sie, dass für $1 < k < p$ die Abbildung φ_k kein Automorphismus von P ist. (Hinweis: Zählen Sie die Nullstellen des Polynoms $x^k - x$.)

   (c) Zeigen Sie: Wenn $1 < k < |L|$, und φ_k ein Automorphismus von L ist, dann muss p ein Teiler von k sein. Mit anderen Worten: φ_k kann nur dann Automorphismus von L sein wenn $k = 1$ oder wenn es ein k_1 mit $k = p \cdot k_1$ gibt.
   Hinweis: Wenn p kein Teiler von $k > 1$ ist, finden Sie den Grad des Polynoms $(x + 1)^k - x^k - 1$, und vergleichen Sie ihn mit der Anzahl der Nullstellen.

   (d) Zeigen Sie $\varphi_{k_1} = \varphi_p^{-1} \circ \varphi_{p \cdot k_1}$. Schließen Sie, dass für $k < |L|$ die Abbildung φ_k nur dann Automorphismus von L sein kann, wenn $k \in \{1, p, p^2, \ldots\}$.

   (e) Sei $\psi : L \to L$ ein Automorphismus. Zeigen Sie, dass es ein $k \geq 1$, $k < |L|$ geben muss, sodass $\psi = \varphi_k$. Hinweis: Sei γ erzeugendes Element der multiplikativen Gruppe von L. (Was heißt das? Formulieren, nicht beweisen.) Dann muss es ein k geben, sodass $\psi(\gamma) = \gamma^k$. (Warum?) Zeigen Sie nun $\psi = \varphi_k$ für dieses k.

   (f) Beschreiben Sie alle Automorphismen von L. (Überlegen Sie insbesondere, ob φ_1, φ_p, φ_{p^2}, ... verschieden sind.)

   Begründen Sie Ihre Antworten. In jedem Unterpunkt dieser Aufgabe dürfen sie alle vorigen Unterpunkte verwenden (auch wenn es Ihnen nicht gelungen ist, diese zu beweisen). Wenn Sie frühere Unterpunkte verwenden, weisen Sie explizit auf diese hin. (Also nicht „daher ist $\psi^2 = id$“, sondern „aus (2) und (4) folgt $\psi^2 = id$“.)