Technische Universität München
Zentrum Mathematik
PD Dr. Ch. Karpfinger

Repetitorium zur Algebra

Herbst 2003, Thema Nr. 2

Aufgabe 1 (*Herbst 2003*)

(a) Definieren Sie die alternierende Gruppe A_n.

(b) Warum ist A_n für $n \geq 2$ eine Untergruppe vom Index 2 in S_n.

(c) Zeigen Sie, daß die Gruppe S_4 auflösbar ist.

Lösung. Z.B.: Die Elemente von A_n sind diejenigen Permutationen mit positivem Vorzeichen, d. h.

$$A_n = \{\sigma \in S_n \,|\, \operatorname{sgn}(\sigma) = 1\}\,.$$

(b) Es ist A_n der Kern des Homomorphismus sgn: $S_n \to \{\pm 1\}$. Für $n \geq 2$ ist dieser Homomorphismus surjektiv. Nach dem Homomorphiesatz gilt also $S_n/A_n \cong \{\pm 1\}$. Somit ist A_n eine Untergruppe vom Index 2.
(c) Eine endliche Gruppe ist genau dann auflösbar, wenn sie eine abelsche Normalreihe besitzt. Wir betrachten die folgende Normalreihe in der S_4:

$$\{(1)\} \trianglelefteq \{(1), (12)(34), (13)(24), (14)(23)\} \trianglelefteq A_4 \trianglelefteq S_4\,.$$

Da die Faktoren alle abelsch sind, ist dies eine abelsche Normalreihe, die Gruppe S_4 also auflösbar.

Aufgabe 2 (*Herbst 2003*) Es sei K ein Teilkörper von $\mathbb{C}$, der über $\mathbb{Q}$ von endlichem Grad ist. Zeigen Sie: Ist n ungerade und K normal über $\mathbb{Q}$, so gilt $K \subseteq \mathbb{R}$.

Aufgabe 3 (*Herbst 2003*) Es seien p und q Primzahlen. Warum zerfällt das Polynom

$$f = X^{p^q} - X$$

über dem Körper $\mathbb{F}_p$ mit p Elementen in p verschiedene Faktoren vom Grad 1 und in $\frac{p^q - p}{q}$ verschiedene irreduzible Faktoren vom Grad q?
Hinweis: Die Faktoren müssen nicht angegeben werden! Zum Einstieg in die Aufgabe überlege man, daß die Nullstellen von f einen Körper bilden.

Lösung. Wir betrachten das Polynom $f = X^{p^q} - X \in \mathbb{Z}_p[X]$, dabei setzen wir $\mathbb{F}_p = \mathbb{Z}_p$. Bekanntlich bildet die Menge der Nullstellen von f (in einem algebraischen Abschluß von $\mathbb{Z}_p$) einen Körper mit p^q Elementen; das ist der Körper $\mathbb{F}_{p^q}$. Unter den p^q Nullstellen befinden sich die Nullstellen $\overline{0}, \overline{1}, \ldots, \overline{p-1} \in \mathbb{Z}_p$. Damit können wir f zerlegen:

$$f = X\,(X - \overline{1}) \cdots (X - \overline{p-1})\, g_1 \cdots g_r\,.$$

Die Polynome $g_1, \ldots, g_r$ seien hierbei irreduzibel; aus Gradgründen gilt $\deg(g_1 \cdots g_r) = p^q - p$. Zu zeigen bleibt:

$$\deg(g_i) = q \text{ für alle } i = 1, \ldots, r \text{ und } r = \frac{p^q - p}{q}.$$

Ist α eine Nullstelle von g_i für ein $i \in \{1, \ldots, r\}$, so gilt

$$\mathbb{Z}_p \subseteq \mathbb{Z}_p(\alpha) \subseteq \mathbb{F}_{p^q}.$$

Es gilt $\mathbb{Z}_p(\alpha) = \mathbb{F}_{p^s}$ mit einem s, das bekanntlich ein Teiler von q ist. Da q eine Primzahl ist, bleiben nur die Möglichkeiten $s = 1$ oder $s = q$. Da $\alpha \notin \mathbb{Z}_p$, gilt $s = q$, d. h.

$$\mathbb{Z}_p(\alpha) = \mathbb{F}_{p^q} \text{ für jede Wurzel } \alpha \text{ von } g_1, \ldots, g_r.$$

Das begründet $\deg(g_i) = q$ für jedes $i = 1 \ldots, r$. Und folglich gilt auch $r = \frac{p^q - p}{q}$.

Aufgabe 4 (*Herbst 2003*) Es sei $R = \mathbb{Z} + \mathbb{Z}\mathrm{i}$ der Hauptidealring der ganzen Gaußschen Zahlen mit $\mathrm{i}^2 = -1$. Weiter sei $N : R \to \mathbb{Z}$ die komplexe Norm $N(a + b\mathrm{i}) = a^2 + b^2$.

(a) Zeigen Sie, daß 11 ein Primelement und 13 kein Primelement in R ist.

(b) Zeigen Sie, daß $11R$ ein maximales Ideal in R ist, und zerlegen Sie $13R$ in ein Produkt von zwei maximalen Idealen.

(c) Welche Ordnung und welche Struktur hat die Gruppe $(R/11R)^\times$ der teilerfremden Restklassen modulo 11 in R?

(d) Welche Ordnung und welche Struktur hat die Gruppe $(R/13R)^\times$ der teilerfremden Restklassen modulo 13 in R?

Hinweis: Der Chinesische Restsatz kann nützlich sein.

Lösung. (a) Die Einheiten von R sind $1, -1, \mathrm{i}, -\mathrm{i}$. Der Ring R ist euklidisch, somit sind Primelemente und unzerlegbare Elemente ein und dasselbe. Ein Element ist also genau dann ein Primelement, wenn es sich nicht als Produkt von zwei Nichteinheiten schreiben läßt.
Für das Element $13 \in R$ gilt

$$13 = 3^2 + 2^2 = (3 + 2\mathrm{i})(3 - 2\mathrm{i}).$$

Da $3 \pm 2\mathrm{i}$ keine Einheiten sind, ist 13 kein Primelement.
Für das Element $11 \in R$ gelte

$$11 = (a + b\mathrm{i})(c + d\mathrm{i}).$$

Dann gälte

$$121 = 11 \cdot 11 = N(11) = (a^2 + b^2)(c^2 + d^2),$$

so daß 11 ein Teiler von $a^2 + b^2$ bzw. von $c^2 + d^2$ wäre, was offenbar nicht möglich ist.

(b) Da 11 ein Primelement ist, ist 11 unzerlegbar. Als unzerlegbares Element erzeugt 11 ein maximales Ideal $(11) = 11R$.
Wegen $13 = (3 + 2\mathrm{i})(3 - 2\mathrm{i})$ liegt die Vermutung nahe, daß

$$(13) = (3 + 2\mathrm{i})(3 - 2\mathrm{i})$$

eine Zerlegung des Ideals (13) in ein Produkt von maximalen Idealen ist. Begründung:
Die Ideale, die von $3 \pm 2\mathrm{i}$ erzeugt werden, sind maximal: Die Elemente $3 \pm 2\mathrm{i}$ sind wegen $N(3 \pm 2\mathrm{i}) = 13$ prim (eine echte Zerlegung hätte Faktoren, deren Normen echte Teiler von 13 wären).

Die Gleichheit $(13) = (3+2\mathrm{i})\,(3-2\mathrm{i})$ gilt bekanntlich (in einem kommutativen Ring R mit 1 gilt $(a)\,(b) = (a\,b)$ für alle $a, b \in R$).

(c) Endliche Untergruppen einer multiplikativen Gruppe eines Körpers sind bekanntlich zyklisch. Demnach ist $R/(11)^\times$ zyklisch. Da der Körper $F = R/(11)$ offenbar 121 Elemente hat, ist die Ordnung von $R/(11)^\times$ gleich 120.

(d) Wir betrachten die multiplikative Gruppe $R/(13)^\times$ aller Einheiten in dem unitären Ring $R/(13)$ mit $13^2 = 169$ Elementen. Es sind $(3+2\mathrm{i})$ und $(3-2\mathrm{i})$ zwei teilerfremde Ideale in $R/(13)$, d. h.

$$R/(13) = (3+2\mathrm{i}) + (3-2\mathrm{i})\,,$$

da die beiden Ideale maximal sind und die Summe von Idealen wieder ein Ideal ist. Für den Schnitt dieser Ideale gilt

$$(3+2\mathrm{i}) \cap (3-2\mathrm{i}) = (3+2\mathrm{i}) \cdot (3-2\mathrm{i}) = (13)\,,$$

da bekanntlich $(3+2\mathrm{i}) \cdot (3-2\mathrm{i}) \subseteq (3+2\mathrm{i}) \cap (3-2\mathrm{i})$ und jedes Element aus $(3+2\mathrm{i}) \cdot (3-2\mathrm{i})$ ein Vielfaches von 13 ist, da es die Primteiler $(3+2\mathrm{i})$ und $(3-2\mathrm{i})$ hat.
Nach dem allgemeinen chinesischen Restsatz gilt nun $R/(13) \cong R/(3+2\mathrm{i}) \times R/(3-2\mathrm{i})$. Damit gilt

$$R/(13)^\times \cong R/(3+2\mathrm{i})^\times \times R/(3-2\mathrm{i})^\times\,.$$

Da $R/(3 \pm 2\mathrm{i})^\times$ wieder multiplikative Gruppen endlicher Körper sind erhalten wir, daß $R/(13)^\times$ direktes Produkt zweier zyklischer Gruppen ist, deren Ordnungen 12 sind. Weiter gilt $|R/(13)^\times| = 144$.

Aufgabe 5 (*Herbst 2003*)
Zeigen Sie die Irreduzibilität der folgenden Polynome f über $\mathbb{Z}$:

(a) $f = X^p + pX - 1$ für jede Primzahl p.

(b) $f = X^4 - 42X^2 + 1$.

Lösung. (a) Der Reduktionssatz ist hier nicht anwendbar, da bei Reduktion bzgl. jeder Primzahl p das reduzible Polynom $X^p - 1$ entsteht. Da auch Eisenstein nicht anwendbar ist, bleiben nur die üblichen Tricks: Betrachte

$$\begin{aligned} f(X+1) &= (X+1)^p + p(X+1) - 1 = \sum_{k=0}^{p} \binom{p}{k} X^{p-k} + pX + p - 1 \\ &= X^p + \binom{p}{1} X^{p-1} + \cdots + \left(\binom{p}{p-1} + p \right) X + p\,. \end{aligned}$$

Nun kann man Eisenstein anwenden und erhält die Irreduzibilität von f.
(b) Das Polynom hat offenbar keine Nullstelle in $\mathbb{Z}$, die Frage ist, warum es keine Zerlegung in zwei quadratische Faktoren gibt. Eisenstein ist nicht anwendbar, der Reduktionssatz hilft nicht viel, also probiert man es mit der Brechstange:

$$X^4 - 42X^2 + 1 = (X^2 + aX + b)(X^2 + cX + d) = X^4 + (a+c)X^3 + (ac + b + d)X^2 + (ad + bc)X + bd\,.$$

Ein Koeffizientenvergleich liefert das Gleichungssystem

$$\begin{aligned} a + c &= 0 \\ ac + b + d &= -42 \\ ad + bc &= 0 \\ bd &= 1\,. \end{aligned}$$

Es folgt $b = 1 = d$ oder $b = -1 = d$. In beiden Fällen erhält man die Unlösbarkeit des Systems, im ersten Fall folgte nämlich $a^2 = 44$ und im zweiten $a^2 = 40$, beide Gleichungen sind in $\mathbb{Z}$ nicht lösbar.