Universität Konstanz Fachbereich Mathematik und Statistik
Vordiploms- und Zwischenprüfung in Algebra
20. April 2007

Lösungsvorschlag zur Aufgabe 1: Für jedes $k \in \mathbb{Z}$ bezeichne $[k]$ die Restklasse von k in $\mathbb{Z}/(4)$. Es gilt $\mathbb{Z}/(4) = \{[0], [1], [2], [3]\}$ und $[0]^2 = [0]$, $[1]^2 = [1]$, $[2]^2 = [2^2] = [4] = [0]$ und $[3]^2 = [9] = [1]$. Die einzigen Quadrate im Ring $\mathbb{Z}/(4)$ sind daher $[0]$ und $[1]$. Wäre jetzt $n \in \mathbb{N}$ durch 4 teilbar und $n + 3$ das Quadrat einer ganzen Zahl, so wäre $[3] = [n + 3]$ ein Quadrat in $\mathbb{Z}/(4)$. Widerspruch!

Lösungsvorschlag zur Aufgabe 2: Die Gruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ist nicht zyklisch, denn außer dem neutralen Element haben alle Elemente die Ordnung 2 (und erzeugen daher nur eine zwei-, nicht aber eine vierelementige Untergruppe). Echte Untergruppen dieser Gruppe haben natürlich die Ordnung 2 oder 1 (denn die Ordnung muß ja ein Teiler von 4 sein), sind also zyklisch.

Lösungsvorschlag zur Aufgabe 3: Für jede Primzahl p bezeichnen wir mit n_p die Anzahl der p-Sylowuntergruppen. Für jede Primzahl, die 30 teilt, gilt nach den Sylowsätzen aus der Vorlesung $n_p \equiv 1$ modulo p und $n_p \mid 30$. Wegen $30 = 2 \cdot 3 \cdot 5$ gilt daher $n_2 \in \{1, 3, 5, 15\}$, $n_3 \in \{1, 10\}$ und $n_5 \in \{1, 6\}$. Da in der Primfaktorzerlegung von 30 jede Primzahl höchstens einmal auftaucht, haben alle Sylowuntergruppen jeweils Primzahlordnung. Je zwei Sylowuntergruppen schneiden sich daher nur im neutralen Element, denn jedes andere gemeinsame Element müßte nach dem kleinen Satz von Fermat schon die beiden Sylowuntergruppen erzeugen (womit sie gleich wären). Wäre $n_2 \geq 3$, $n_3 \geq 10$ und $n_5 \geq 6$, so hätte man daher mindestens $1 + 3 \cdot 1 + 10 \cdot 2 + 6 \cdot 4 = 48$ Elemente. Widerspruch!

Lösungsvorschlag zur Aufgabe 4: (a) Sei G eine Gruppe mit $\#G = 6$. Nach den Sylowsätzen muß die Anzahl der 3-Sylowuntergruppen einerseits kongruent 1 modulo 3 und andererseits ein Teiler von 2 sein. Also gibt es nur eine 3-Sylowuntergruppe N, die damit ein Normalteiler sein muß (denn sie kann ja von keinem Automorphismus bewegt werden, insbesondere nicht von einem inneren Automorphismus). Nun ist $G \rhd N \rhd \{1\}$ eine Normalreihe mit Faktoren G/N und $N \cong N/\{1\}$. Es bleibt zu zeigen, daß diese Faktoren abelsch sind. Sie sind aber sogar zyklisch, ja sogar von Primzahlordnung, denn N hat 3 und G/N hat $6/3 = 2$ Elemente.

(b) Sei G eine Gruppe mit $\#G = 42 = 6 \cdot 7$. Nach den Sylowsätzen muß die Anzahl der 7-Sylowuntergruppen einerseits kongruent 1 modulo 7 und andererseits ein Teiler von 6 sein. Also gibt es nur eine 7-Sylowuntergruppe N, die damit ein Normalteiler sein muß (vergleiche (a)). Nun ist N eine Gruppe, die abelsch (sogar zyklisch, da von Primzahlordnung) und damit natürlich auflösbar ist. Außerdem ist die

Gruppe G/N nach Aufgabe (a) auflösbar, denn sie ist von der Ordnung 6. Nach Vorlesung ist mit N und G/N auch G auflösbar.

Lösungsvorschlag zur Aufgabe 5: (a) $2 = 2^2 = 2 + 2$ und damit $0 = 2$ in A

(b) Sind $x, y \in A$, so gilt $x + y = (x + y)^2 = (x + y)(x + y) = x^2 + xy + yx + y^2 = x + y + xy + yx$ und damit $0 = xy + yx$. Aus (a) folgt aber $-1 = 1$, also $xy = -yx = (-1)(yx) = yx$ für alle $x, y \in A$.

(c) Sei I ein Ideal in A. Für jedes $x \in A$ bezeichne $[x]$ die Restklasse von x in A/I. Dann gilt $[x]^2 = [x^2] = [x]$.

(d) Sei A ein Integritätsbereich und $0 \neq x \in A$. Dann gilt $x^2 = x$, da A boolesch ist. Daraus folgt aber nun $x = 1$. Insgesamt sieht man so $A = \{0, 1\}$. Andererseits ist nach der Definition eines Integritätsbereichs $0 \neq 1$, also hat A genau zwei Elemente 0 und 1. Daher ist A isomorph zum Körper $\mathbb{Z}/(2)$.

(e) Sei I ein Primideal in A. Dann ist A/I nach Vorlesung ein Integritätsbereich und nach (c) boolesch, also nach (d) isomorph zu einem Körper. Daher ist A/I selbst ein Körper, was nach Vorlesung heißt, daß I ein maximales Ideal in A ist.

Lösungsvorschlag zur Aufgabe 6: (a) Die Zahl $198374 = 110000 + 88000 + 330 + 44$ ist offenbar durch 11 teilbar. Der konstante Koeffizient des Polynoms ist auch durch 11, aber nicht durch 11^2 teilbar. Außerdem ist das Polynom primitiv über $\mathbb{Z}$. Da 11 eine Primzahl ist, können wir also das Kriterium von Eisenstein aus der Vorlesung anwenden und erhalten, daß das Polynom irreduzibel in $\mathbb{Z}[X]$ ist. Damit ist es nach Vorlesung erst recht irreduzibel in $\mathbb{Q}[X]$ (denn sein Grad ist ≥ 1).

(b) Das gegebene Polynom

$$(X + a)^p + ap - a^p = X^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i X^{p-i} + ap$$

ist normiert (insbesondere primitiv über $\mathbb{Z}$), der konstante Koeffizient ap läßt sich durch p, aber nicht durch p^2 teilen, und alle anderen Koeffizienten

$$\binom{p}{i} = \frac{p!}{(p-i)!i!} = \frac{(p-1)!p}{(p-i)!i!} \qquad (1 \leq i \leq p-1)$$

lassen sich in $\mathbb{Z}$ durch p teilen, denn in der Primfaktorzerlegung von $i!(p-1)!$ kann für kein $i \in \{1, \ldots, p-1\}$ die Primzahl p auftauchen (sonst wäre p ein Teiler von i für ein $i \in \{1, \ldots, p-1\}$). Nun wendet man wie in (a) Eisenstein an, jedoch mit dem Primelement $p \in \mathbb{Z}$.

Lösungsvorschlag zur Aufgabe 7: Wir behaupten, daß die gesuchte Menge gleich $\mathbb{C} \setminus \{0\}$ ist. Dies folgt aus folgenden beiden Tatsachen:

Die Ringe $\mathbb{C}[X]/(X^2)$ und $\mathbb{C} \times \mathbb{C}$ sind nicht isomorph, da es in $\mathbb{C}[X]$ ein nilpotentes Element $\neq 0$ gibt (nämlich die Restklasse von X), aber nicht in $\mathbb{C} \times \mathbb{C}$.

Sei $a \in \mathbb{C} \setminus \{0\}$. Dann sind die Ringe $\mathbb{C}[X]/(X^2+a)$ und $\mathbb{C} \times \mathbb{C}$ isomorph. Wähle nämlich $b \in \mathbb{C}$ mit $b^2 = -a$. Dann gilt

$$X^2 + a = (X+b)(X-b)$$

und wegen $b \neq 0$ sind $X+b$ und $X-b$ verschieden und damit zueinander teilerfremd. Nach dem Chinesischen Restsatz erhält man daher die Ringisomorphie $\mathbb{C}[X]/(X^2+a) \cong (\mathbb{C}[X]/(X+b)) \times (\mathbb{C}[X]/(X-b))$. Nach dem Homomorphiesatz sind außerdem

$$\mathbb{C}[X]/(X-b) \to \mathbb{C},\ f \mapsto f(b) \quad \text{und} \quad \mathbb{C}[X]/(X+b) \to \mathbb{C},\ f \mapsto f(-b)$$

Ringsiomorphismen. Insgesamt erhält man daher leicht

$$\mathbb{C}[X]/(X^2+a) \cong \mathbb{C} \times \mathbb{C}.$$

Lösungsvorschlag zur Aufgabe 8: Setze $f := X^2+2X+2 \in \mathbb{F}_3[X]$. Dann gilt $f(0) = 2 \neq 0$, $f(1) = 5 = 2 \neq 0$, $f(2) = 4+4+2 = 1 \neq 0$ in $\mathbb{F}_3$. Da f ein Polynom vom Grad 2 und $\mathbb{F}_3$ ein Körper ist, muß f daher irreduzibel im Ring $\mathbb{F}_3[X]$ sein. Da $\mathbb{F}_3[X]$ ein faktorieller Ring ist (sogar ein Hauptidealring), ist damit f sogar ein Primelement. Also ist das von f erzeugte Ideal in $\mathbb{F}_3[X]$ ein Primideal. Da $\mathbb{F}_3[X]$ ein Hauptidealbereich ist, ist jedes Primideal $\neq \{0\}$ sogar maximal. Daher ist das von f erzeugte Ideal in $\mathbb{F}_3[X]$ maximal und daher $\mathbb{F}_3[X]/(f)$ ein Körper. Nach Vorlesung bilden die Restklassen von 1 und X eine zweielementige Basis des $\mathbb{F}_3$-Vektorraums $\mathbb{F}_3[X]/(f)$ (da f den Grad 2 hat). Daher ist $\mathbb{F}_3[X]/(f)$ als $\mathbb{F}_3$-Vektorraum zweidimensional und hat daher 9 Elemente. Da es bis auf Isomorphie nur einen neunelementigen Körper $\mathbb{F}_9$ gilt, muß zwangsläufig $\mathbb{F}_3[X]/(f) \cong \mathbb{F}_9$ gelten.

Lösungsvorschlag zur Aufgabe 9: (a) Es gilt $a^2 = 2+\sqrt{2}$, also $a^2 - 2 = \sqrt{2}$ und somit $(a^2-2)^2 = 2$, d.h. $a^4 - 4a^2 + 2 = 0$. Wir behaupten nun, daß

$$p := X^4 - 4X^2 + 2 \in \mathbb{Q}[X]$$

das Minimalpolynom von a über $\mathbb{Q}$ ist. Da a bereits eine Nullstelle des normierten Polynoms p ist, muß nur noch nachgewiesen werden, daß p irreduzibel im Ring $\mathbb{Q}[X]$ ist. Nach dem Kriterium von Eisenstein angewandt auf das Primelement $2 \in \mathbb{Z}$, folgt aber sofort, daß p irreduzibel in $\mathbb{Z}[X]$ ist. Da p ein Polynom vom Grad ≥ 1 ist, folgt aus der Vorlesung, daß p auch in $\mathbb{Q}[X]$ irreduzibel ist.

(b) Genauso wie man in (a) nachgerechnet hat, daß a eine Nullstelle von p ist, kann man nachrechnen, daß die vier reellen Zahlen

$$\pm\sqrt{2 \pm \sqrt{2}}$$

Nullstellen von p sind. Diese vier Zahlen sind auch paarweise verschieden: Zwei sind negativ, zwei sind positiv. Die zwei negativen haben verschiedene Beträge genauso wie die beiden positiven. Da p den Grad 4 hat, müssen diese vier reellen Zahlen schon alle Nullstellen von p sein.

(c) Zu zeigen ist, daß die vier Nullstellen von p alle in $\mathbb{Q}(a)$ liegen. Es reicht dazu natürlich $\sqrt{2-\sqrt{2}} \in \mathbb{Q}(a)$ zu zeigen. Dies folgt aber aus

$$\sqrt{2-\sqrt{2}} = \frac{a\sqrt{2-\sqrt{2}}}{a} = \frac{\sqrt{4-2}}{a} = \frac{\sqrt{2}}{a} \in \mathbb{Q}(a).$$

(d) Nach (c) ist $\mathbb{Q}(a)$ der Zerfällungskörper eines Polynoms über $\mathbb{Q}$. Damit ist die Körpererweiterung $\mathbb{Q}(a)|\mathbb{Q}$ normal. Da $\mathbb{Q}$ vollkommen ist, ist sie auch separabel. Somit ist $\mathbb{Q}(a)|\mathbb{Q}$ eine Galoiserweiterung.

(e) Wegen $\deg p = 4$ gilt $[\mathbb{Q}(a) : \mathbb{Q}] = 4$. Nach dem Hauptsatz der Galoistheorie hat daher die Galoisgruppe von $\mathbb{Q}(a)|\mathbb{Q}$ vier Elemente. Mit anderen Worten gibt es vier Automorphismen der Körpererweiterung $\mathbb{Q}(a)|\mathbb{Q}$. Jeder solche Automorphismus ist aber schon dadurch festgelegt, worauf er a abbildet. Er kann aber a nur auf eine der vier Nullstellen $\pm\sqrt{2 \pm \sqrt{2}}$ von p abbilden. Die vier Elemente der Galoisgruppe von $\mathbb{Q}(a)|\mathbb{Q}$ sind daher wie folgt gegeben:

$$a \mapsto \sqrt{2+\sqrt{2}},\ a \mapsto \sqrt{2-\sqrt{2}},\ a \mapsto -\sqrt{2+\sqrt{2}},\ a \mapsto -\sqrt{2-\sqrt{2}}.$$

Wir behaupten, daß das zweite Element $\sigma : a \mapsto \sqrt{2-\sqrt{2}}$ schon die Galoisgruppe erzeugt. Dazu reicht es zu zeigen, daß σ^2 nicht die Identität ist (denn dann kommt für die Ordnung von σ in der Galoisgruppe, die ja ein Teiler von 4 sein muß, nur noch 4 in Frage). Es gilt aber

$$\sigma(\sqrt{2}) = \sigma(a^2-2) = \sigma(a)^2 - 2 = 2 - \sqrt{2} - 2 = -\sqrt{2}$$

und daher

$$\begin{aligned}\sigma^2(a) = \sigma\left(\sqrt{2-\sqrt{2}}\right) &= \sigma\left(\frac{\sqrt{2}}{a}\right) \qquad \text{(vergleiche (c))} \\ &= \frac{-\sqrt{2}}{\sigma(a)} = \frac{-\sqrt{2}}{\sqrt{2-\sqrt{2}}} = \frac{-\sqrt{2}\left(\sqrt{2+\sqrt{2}}\right)}{\sqrt{4-2}} = -a \neq a.\end{aligned}$$

Lösungsvorschlag zur Aufgabe 10: Offensichtlich gilt $[K(a) : K(a^2)] \leq 2$. Gälte $[K(a) : K(a^2)] = 2$, so wäre nach der Gradformel

$$[L : K] = [L : K(a)][K(a) : K(a^2)]$$

gerade. Also gilt $[K(a) : K(a^2)] = 1$ und damit $K(a) = K(a^2)$.