Mathematisches Institut
der Universität München
Andreas Fackler

Sommersemester 2009
Lösungsvorschlag zu Übungsblatt 1

Klausurenkurs Algebra

Aufgabe 1 (Herbst 2007, Thema 1, Aufgabe 1)

(a) Wir zeigen, dass $4^{2n+1} + 3^{n+2}$ kongruent 0 modulo 13 ist, also durch 13 teilbar:

$$4^{2n+1} + 3^{n+2} \equiv 4 \cdot 4^{2n} + 9 \cdot 3^n \equiv 4 \cdot 16^n - 4 \cdot 3^n \equiv 4 \cdot 3^n - 4 \cdot 3^n \equiv 0 \mod 13$$

(b) Sei $m = a^2 + b^2$ und $n = c^2 + d^2$. Dann ist $m = |a + ib|^2$ und $n = |c + id|^2$, wobei $a + ib, c + id \in \mathbb{Z}[i]$ gaußsche Zahlen sind. Es folgt:

$$mn = |a+ib|^2|c+id|^2 = |(a+ib)(c+id)|^2 = |ac-bd+i(ad+bc)|^2 = (ac-bd)^2+(ad+bc)^2$$

Also ist auch das Produkt von m und n wieder eine Summe von Quadraten.

(c) Diese Aussage ist falsch. Ein Gegenbeispiel ist: $(1^2 + 1^2 + 0^2) \cdot (1^2 + 2^2 + 3^2) = 2 \cdot (1 + 4 + 9) = 28$ Angenommen, $28 = a^2 + b^2 + c^2$ für ganze Zahlen $a, b, c \in \mathbb{Z}$. Sei ohne Beschränkung der Allgemeinheit $a \geq b \geq c \geq 0$. Dann ist einerseits $a^2 \leq a^2 + b^2 + c^2 = 28$, und andererseits $3a^2 \geq a^2 + b^2 + c^2 = 28$, also $9 + \frac{1}{3} = \frac{28}{3} \leq a^2 \leq 28$. Für a kommen also nur die Werte 4 und 5 in Frage. Es ist $b^2 + c^2 = 28 - a^2$ entweder $28 - 16 = 12$ oder $28 - 25 = 3$. Im letzteren Fall kommen für b nur 0 und 1 in Frage. Dann ist aber $3 - b^2$ keine Quadratzahl. Es muss also $a = 4$ und damit $28 - a^2 = 12$ sein. In diesem Fall kommen für b die Werte 0, 1, 2 und 3 in Frage. $12 - b^2$ ist dann 12, 11, 8 bzw. 3. Da keine dieser zahlen eine Quadratzahl ist, lässt sich 28 also nicht in der Form $a^2 + b^2 + c^2$ darstellen.

Aufgabe 2 (Herbst 2007, Thema 1, Aufgabe 2)

(a)⇒ (b) Sei ohne Einschränkung $G = \mathbb{Z}/(p^n)$. Dann ist $\langle \overline{p} \rangle$ eine echte Untergruppe. Ist $\overline{x} \notin \langle \overline{p} \rangle$, so sind x und p Teilerfremd, also ist dann $\langle \overline{x} \rangle = G$. Dies zeigt, dass jede Untergruppe, die ein Element von $G \setminus \langle \overline{p} \rangle$ enthält (die also nicht Teilmenge von $\langle \overline{p} \rangle$ ist), bereits ganz G ist. Folglich ist $\langle \overline{p} \rangle$ die einzige maximale Untergruppe.

(b)⇒ (a) Sei M die maximale Untergruppe. Sei $g \in G \setminus M$. Wäre $\langle g \rangle$ nicht ganz G, so gäbe es eine maximale Untergruppe, die $\langle g \rangle$ als Teilmenge enthält. Diese wäre dann ungleich M. Also ist $\langle g \rangle = G$, das heißt, G ist zyklisch.

Aufgabe 3 (Herbst 2007, Thema 1, Aufgabe 3)

Jedes Ideal, das eine Einheit enthält (das also nicht disjunkt zu R^* ist), ist ganz R, also ist R^* disjunkt von M, das heißt, $R^* \subseteq R \setminus M$. Es bleibt zu zeigen, dass $R \supseteq R \setminus M$ ist, dass also jedes $x \notin R \setminus M$ eine Einheit ist. Wäre $(x) \neq R$, so gäbe es ein maximales Ideal $I \supseteq (x)$, also wäre dann $x \in M$. Es ist also $(x) \in R$ und damit gibt es ein $r \in R$, so dass $rx = 1$. Also ist x eine Einheit.

Aufgabe 4 (Herbst 2007, Thema 1, Aufgabe 4)

Um dies zu widerlegen, müssen wir nur eine Galoiserweiterung $M|K$ mit Galoisgruppe $\mathbb{Z}/(4)$ finden. Wir können dann L als Fixkörper des Normalteilers $\langle\overline{2}\rangle \subseteq \mathbb{Z}/(4)$ wählen und erhalten nach dem Hauptsatz der Galoistheorie Galoiserweiterungen $L|K$ und $M|L$ vom Grad 2.

Ein Beispiel für eine solche Erweiterung ist $K = \mathbb{Q}$ und $M = \mathbb{Q}(\zeta_5)$, wobei ζ_5 eine primitive fünfte Einheitswurzel ist. Ihre Galoisgruppe ist isomorph zu $(\mathbb{Z}/(5))^\times$, welche (als Untergruppe der multiplikativen Gruppe des Körpers $\mathbb{Z}/(5)$) zyklisch ist.

Aufgabe 5 (Herbst 2007, Thema 1, Aufgabe 5)

(a)

$$\begin{aligned} f(X^2-2) &\equiv (X^2-2)^3 - 3(X^2-2) + 1 = X^6 - 6X^4 + 12X^2 - 8 - 3X^2 + 6 + 1 \\ &\equiv (3X-1)^2 - 6X(3X-1) + 9X^2 - 1 \equiv 0 \mod f(X) \end{aligned}$$

(b) Da sowohl $\alpha \in \mathbb{Q}(\alpha)$ als auch $\alpha^2 + 2 \in \mathbb{Q}(\alpha)$ Nullstellen von $f(X)$ sind, zerfällt $f(X)$ in $\mathbb{Q}(\alpha)$ in Linearfaktoren. $\mathbb{Q}(\alpha)$ ist also der Zerfällungskörper von $f(X)$ und somit galoissch. ($\mathbb{Q}$ ist ein perfekter Körper, das heißt, jedes irreduzible Polynom ist separabel.)

(c) Hierzu ist noch zu zeigen, dass $f(X)$ irreduzibel, $\mathbb{Q}(\alpha)|\mathbb{Q}$ also wirklich vom Grad 3 (und nicht etwa $\mathbb{Q}(\alpha) = \mathbb{Q}$) ist. Da f Grad 3 hat, genügt es hierzu zu zeigen, dass f keine Nullstelle in $\mathbb{Q}$ hat.

Hätte $f(X)$ eine Nullstelle in $\mathbb{Q}$, so läge diese in $\mathbb{Z}$ und würde den konstanten Koeffizienten 1 teilen, wäre also 1 oder -1. Es ist aber $f(1) \neq 0 \neq f(-1)$.