Algebraische Zahlentheorie: [MTH-1483]

Ilia Pirashvili

Arbeitsblatt 3

1 Aufgaben

Aufgabe 1 (1 Punkt). Sei $K \to L$ eine Körpererweiterung und $\alpha \in L$. Beweise, dass es genau dann eine Isomorphie

$$K[X] \to K[\alpha]$$

von Ringen gibt, wenn α *nicht* algebraisch über K ist.

Lösung. Diese Abbildung, definiert durch $f(x) \mapsto f(\alpha)$ ist immer surjektiv.

Wir behaupten, dass es genau dann injektiv ist, wenn α nicht algebraisch ist. Dies ist klar, da Injektivität in Ringen mit dem Kern bestimmt werden kann: Der Kern dieser Abbildung ist genau dann $\{0\}$, wenn es kein Polynom $f(x) \in K[X]$ gibt, sodass $f(x) \mapsto 0$, i.e., sodass $f(\alpha) = 0$. □

Aufgabe 2. [1 Punkt] Sei K ein Körper. Beweise, dass $\{1, X, X^2, \dots, X^{d-1}\}$ eine K-Basis von $K[X]/f(x)$, für jeden irreduziblen Polynom $f(x) \in K[X]$ von Grad d definiert.

Lösung. Am einfachsten kann man mit der Dimension des Vektorraums argumentieren: Wir wissen, dass $[K[X]/f(x) : K] = d$, daher muss eine Basis darüber genau d Elemente haben.

Da $f(x)$ von Grad d ist, können $\{1, X, X^2, \dots, X^{d-1}\}$ nicht linear Abhängig voneinander sein, da es sonst möglich wäre

$$\overline{X}^i = a_0 + a_1\overline{X} + \cdots + a_{i-1}\overline{X}^{i-1} + a_{i+1}\overline{X}^{i+1} + \cdots + a_{d-1}\overline{X}^{d-1}$$

in $K[X]/f(x)$ zu schreiben, für irgendein $1 \le i \le d-1$, wobei nicht jedes der a_i null wäre.

Dies würde dann umformen zu einem Polynom vom Grad $\le d-1$ was Null in $K[X]/f(x)$ wäre, also, im Ideal $(f) \subseteq K[X]$ liegen würde. Daher müsste es ein Vielfaches von $f(x)$ sein, was ein Widerspruch ist, da $\mathsf{grad}(f) = d > d-1$.

Also sind $\{1, X, X^2, \dots, X^{d-1}\}$ linear Unabhängig und ihre Anzahl stimmt mit der Dimension überein ⇒ Basis. □

Aufgabe 3 (4 Punkte insgesamt). Sei $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ das Körper mit 2 Elementen.

1. (1 Teilpunkt) Beweise, dass $f(x) = x^2 + x + 1$ irreduzibel ist über $\mathbb{F}_2$ und schlussfolgere, dass es einen Körper mit 4 Elementen gibt.

2. (1 Teilpunkt) Wenn wir diesen Körper mit Elementen der Form $(a, b), a, b \in \mathbb{F}_2$ gleichsetzen, gebt die Formel für
$$(a, b) + (c, d)$$
und
$$(a, b)(c, d).$$

3. (2 Teilpunkt) Beweise, dass $x^3 + x + 1$ und $x^3 + x^2 + 1$ irreduzibel sind über $\mathbb{F}_2$. Sind die korrespondierenden Körper mit 8 Elementen isomorph?

Lösung. 1. Da f quadratisch ist, ist es irreduzibel genau dann, wenn es keine Wurzel hat. Da $f(0) = f(1) = 1 \neq 0$ ist f irreduzibel über $\mathbb{F}_2$.

Da es irreduzibel ist, ist $\mathbb{F}_2[X]/x^2 + x + 1$ ein Integritätsbereich. Bei Aufgabe 4 ist es ein Körper.

2. Wir können $x^2 + x + 1$ umformen zu

$$x^2 = -(x + 1) = x + 1$$

über $\mathbb{F}_2$. Sei α eine Wurzel dieses Polynoms. Als solches können wir die Elemente von $\mathbb{F}_2[X]/x^2 + x + 1$ gleichsetzen mit $\{a + b\alpha\}$, wobei $\alpha^2 = \alpha + 1$. Dies können wir mit paaren von Elementen $(a, b) \in \mathbb{F}_2$ gleichsetzen.

Um die Ringstruktur zu beschreiben, bemerken wir, dass

$$(a + b\alpha) + (c + d\alpha) = (a + c) + (b + d)\alpha$$

und

$$\begin{aligned}(a + b\alpha)(c + d\alpha) &= ac + (ad + bc)\alpha + bd\alpha^2 \\ &= ac + (ad + bs)\alpha + bd(1 + \alpha) \\ &= (ac + bd) + (ad + bc + bd)\alpha.\end{aligned}$$

Daher gilt

$$(a, b) + (c, d) = (a + c, b + d)$$

und

$$(a, b)(c, d) = (ac + bd, ad + bc + bd).$$

3. Auch bei Grad 3 reicht es aus zu zeigen, dass ein Polynom keine Wurzeln hat. Bei beiden kann man das direkt sehen.

Lass α eine Wurzel von $x^3 + x + 1$ und β eine Wurzel von $x^3 + x^2 + 1$ sein, so dass

$$K[X]/x^3 + x + 1 = \{a + b\alpha + c\alpha^2 \mid a, b, c \in K\}$$

und

$$K[X]/x^3 + x^2 + 1 = \{a + b\beta + c\beta^2 \mid a, b, c \in K.\}$$

Um zu sehen, dass diese Körper Isomorph sind, definieren wir die Abbildung

$$\varphi : K[X]/x^3 + x + 1 \to K[X]/x^3 + x^2 + 1$$

mit

$$\alpha \mapsto \beta + 1.$$

Es gilt $\alpha^3 = -(\alpha + 1) = \alpha + 1$. Um zu zeigen, dass φ Wohldefiniert ist, reicht es aus zu zeigen, dass

$$\varphi(\alpha^3) = \varphi(\alpha + 1).$$

Also, dass

$$(\beta + 1)^3 = (\beta + 1) + 1.$$

Dies gilt, da

$$\begin{aligned}(\beta + 1)^3 &= \beta^3 + \overline{3}\beta^2 + \overline{3}\beta + 1 \\ &= \beta^3 + \beta^2 + \beta + 1 \\ &= (\beta^2 + 1) + \beta^2 + \beta + 1 \\ &= \overline{2}\beta^2 + \beta + \overline{2} \\ &= \beta + \overline{2} \\ &= (\beta + 1) + 1,\end{aligned}$$

wie gewollt. Hier haben wir die Tatsache benutzt, dass $\beta^3 = -(\beta^2+1) = \beta^2+1$.

□

Aufgabe 4 (2 Punkte). Sei $0 \neq R$ ein endlicher Integritätsbereich, ungleich dem Nullring. Das heißt, $|R| < \infty$. Beweise, dass R ein Körper ist.

Lösung. Sei $r \in R$ ungleich Null. Zu zeigen, $r \in R^\times$. Wir definieren die Abbildung

$$f_r : R \to R, \quad x \mapsto rx.$$

Hier muss man sagen, dass f *kein* Ringhomomorphismus ist, da $1 \not\mapsto 1$, es ist aber ein R-Modulen Homomorphismus. Dies ist nicht wichtig, den es geht nur darum, dass f_r ein Isomorphismus ist, woraus die Aussage folgen wird, da es ein Element $s \in R$ geben wird, so dass $f_r(s) = 1$. Es ist einfach zu Überprüfen, dass $s = r^{-1}$ sein wird.

Um zu sehen, dass f_r ein Isomorphismus ist, sein $x, y \in R$, so dass

$$f_r(x) = f_r(x).$$

Daher $rx = ry$ was äquivalent zu $r(x-y) = 0$ ist. Da R ein Integritätsbereich ist und $r \neq 0$, folgt $x = y$. Daher ist f_r injektiv. Da R endlich ist, ist es nun auch surjektiv und als solches bijektiv. Damit sind wir fertig. □

Aufgabe 5 (2 Punkte insgesamt). Sei $\mathbb{Q} \to \mathbb{C}$ eine Körpererweiterung. Finde die Minimalpolynome (über $\mathbb{Q}$) zu den folgenden Elementen (in $\mathbb{C}$).

1. (1 Teilpunkt) $\frac{1+\sqrt{5}}{2}$.
2. (1 Teilpunkt) $\cos(\frac{2\pi}{5})$

Lösung. 1.a. Sei $\alpha = \frac{1+\sqrt{5}}{2}$. Dann gilt

$$\begin{aligned} 2\alpha = 1+\sqrt{5} &\Leftrightarrow 2\alpha - 1 = \sqrt{5} \\ &\Leftrightarrow 4\alpha^2 - 4\alpha + 1 = 5 \\ &\Leftrightarrow \alpha^2 - \alpha - 1 = 0. \end{aligned}$$

Daher ist das Minimalpolynom $\mathfrak{m}_\alpha = x^2 - x - 1$. Das es irreduzibel ist, ist klar, da $\sqrt{5} \notin \mathbb{Q}$, daher muss der Grad der Erweiterung ≥ 2.

2. Dies ist schwerer. Hierzu benutzen wir eine trigonometrische Gleichung

$$\cos(5\theta) = \cos^5(\theta) - 10\cos^3(\theta)\sin^2(\theta) + 5\cos(\theta)\sin^4(\theta) = 16\cos^5(\theta) - 20\cos^3(\theta) + 5\cos(\theta).$$

Sei nun $\theta = \frac{2\pi}{5}$. Dann erhalten wir

$$1 = \cos(2\pi) = 16\cos^5(\frac{2\pi}{5}) - 20\cos^3(\frac{2\pi}{5}) + 5\cos(\frac{2\pi}{5}).$$

Daher ist $\cos(\frac{2\pi}{5})$ eine Wurzel der Gleichung

$$16x^5 - 20x + 5x - 1.$$

(Mit etwas schummeln sieht man sich wieder die Teiler von 1 an.) Da 1 eine Wurzel des Polynoms ist, teilen wir das obige Polynom durch $(x-1)$ und erhalten

$$16x^5 - 20x + 5x - 1 = (x-1)(4x^2 + 2x - 1)^2.$$

Da freilich $\cos(\frac{2\pi}{5}) \neq 1$, ist $\cos(\frac{2\pi}{5})$ eine Wurzel von $(4x^2 + 2x - 1)2$. Dies ist irreduzibel und daher ist

$$\mathfrak{m}_\alpha = x^2 + \frac{1}{2}x - \frac{1}{4}.$$

□

Aufgabe 6 (5 Punkte insgesamt). Sei $\alpha = \sqrt{5} + \sqrt{6}$ und sei $L = \mathbb{Q}(\alpha)$.

1. (2 Teilpunkte) Finde das Minimalpolynom von α über $\mathbb{Q}$.
2. (0,5 Teilpunkt) Beweise, dass $\sqrt{30} \in L$.

Sei $K = \mathbb{Q}(\sqrt{30})$.

3. (0,5 Teilpunkt) Finde die Grade der Erweiterungen
$$[K : \mathbb{Q}], [L : K] \text{ und } [L : \mathbb{Q}].$$
4. (1 Teilpunkt) Finde das Minimalpolynom von α über K.
5. (1 Teilpunkt) Beweise, dass $L \simeq \mathbb{Q}(\sqrt{5}, \sqrt{6})$.

Lösung. 1. Sei $\alpha = \sqrt{5} + \sqrt{6}$. Dies ergibt
$$\begin{aligned} \alpha^2 = 11 + 2\sqrt{30} &\Leftrightarrow \alpha^2 - 11 = 120 \\ &\Leftrightarrow \alpha^4 - 22\alpha^2 + 121 = 120 \\ &\Leftrightarrow \alpha^4 - 22\alpha^2 + 1 = 0. \end{aligned}$$
Auch hier kann man entweder zeigen, dass $\mathfrak{m}_\alpha = x^4 - 22x^2 + 1$ irreduzibel ist, oder dass $\sqrt{5} \notin \mathbb{Q}(\sqrt{6})$ ist.

Wieder kann man sehen, dass ± 1 keine Wurzel ist. Zu sehen, dass es nicht das Produkt von zwei quadratischen Polynomen ist, sei
$$\mathfrak{m}_\alpha = (X^2 + aX + b)(X^2 + cX + d).$$
Da man über einen Körper arbeite, kann man annehmen, dass die Leitkoeffizienten 1 sind. Nach ausrechnen und gleichsetzen sieht man, dass
$$bd = 1, ad + bc = 0, ac + b + d = -22 \text{ und } a + c = 0.$$
Die erste Gleichung ergibt $b = d = \pm 1$. Wenn man die 4te Gleichung in die 3te einsetzt bekommt man
$$-c^2 \pm 2 = -22.$$
Da weder 20 noch 24 eine Quadratzahl ist, führt es zum Widerspruch.

2. $\sqrt{30} = \frac{\alpha^2 - 11}{2} \in \mathbb{Q}(\alpha)$.
3. Dass $[K : \mathbb{Q}] = 4$ und $[L : \mathbb{Q}] = 2$ ist klar. Körperturmsatz sagt nun $[L : K] = 2$.
4. Von $\sqrt{30} = \frac{\alpha^2 - 11}{2} \in \mathbb{Q}(\alpha)$ folgt
$$\alpha^2 = 11 + 2\sqrt{30}.$$
Daher, gilt für
$$\mathfrak{n}_\alpha := x^2 - 11 - 2\sqrt{30}.$$
Aus $\mathfrak{n}_\alpha(\alpha) = 0$ und $\mathsf{grad}(\mathfrak{n}_\alpha) = [L : K]$ folgt, dass $\mathfrak{n}_\alpha$ das Minimalpolynom von α über $K = \mathbb{Q}(\sqrt{30})$ ist.
5. Es ist klar, dass $L \subseteq \mathbb{Q}(\sqrt{5}, \sqrt{6})$ ist, da $\alpha \in \mathbb{Q}(\sqrt{5}, \sqrt{6})$. Die andere Seit kann man machen, indem man zeigt, dass $\sqrt{5} \in L$ (woraus auch $\sqrt{6} \in L$ direkt folgen wird), oder, einfacher, man macht es mit dem Körperturmsatz:

   Dies besagt
$$[\mathbb{Q}(\sqrt{5}, \sqrt{6}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{5}, \sqrt{6}) : \mathbb{Q}(\sqrt{5})][\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] \leq 2 \cdot 2 = [L : Q].$$
   Da $L \subseteq \mathbb{Q}(\sqrt{5}, \sqrt{6})$ und der Grad ihrer Erweiterungen über $\mathbb{Q}$ gleich sind, müssen die Körper Isomorph sein.

□

Aufgabe 7 (2 Punkte). Finde das Minimalpolynom von $\frac{1+i}{\sqrt{2}}$ über $\mathbb{Q}$. Was sind die anderen Wurzeln dieses Polynoms?

Lösung. Sei $\alpha = \frac{1+i}{\sqrt{2}}$. Dann gilt

$$\begin{aligned} \alpha^2 = \frac{(1+i)^2}{2} &\Leftrightarrow 2\alpha^2 = 1 + 2i + i^2 = 2i \\ &\Leftrightarrow \alpha^2 = i \\ &\Leftrightarrow \alpha^4 = -1. \end{aligned}$$

Daher ist ein Kandidat des Minimalpolynoms

$$\mathfrak{m}_\alpha = x^4 + 1.$$

Um dies zu zeigen, müssen wir beweisen, dass $\mathfrak{m}_\alpha$ irreduzibel ist.

(Als erstes bemerken wir, dass modulo 3, es keine Lösung hat. Als solches kann es nur das Produkt von zwei Polynomen $f(x), g(x) \in \mathbb{Z}[X]$ sein, mit $\mathsf{grad}(f) = \mathsf{grad}(g) = 2$. Das Lemma von Gauß sagt nun, dass es auch über $\mathbb{Q}$ irreduzibel ist.

Wir schreiben auf

$$x^4 + 1 = (ax^2 + bx + c)(ux^2 + vx + w).$$

Dies wir letztendlich zum Widerspruch führen.)

Alternativ kann man es beweisen, indem man beweist, dass $\sqrt{2} \notin \mathbb{Q}$ (bekannt) und $i \notin \mathbb{Q}(\sqrt{2})$. Dann können wir durch den Körperturmsatz mit der Grad der Erweiterung argumentieren uns sagen, dass $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, daher muss $\mathfrak{m}_\alpha$ das Minimalpolynom sein.

Um zu sehen, dass $i \notin \mathbb{Q}(\sqrt{2})$, bemerken wir, dass für alle $r = a + b\sqrt{arg} \in \mathbb{Q}(\sqrt{2})$ gilt, $r^2 \geq 0$.

Um die anderen Wurzeln zu finden, bemerken wir, dass wenn $r \in \mathbb{Q}(\alpha)$ eine Wurzel von $\mathfrak{m}_\alpha$ ist, ist auch $-r$ eine Wurzel. Daher ist $-\alpha$ auch eine Wurzel. Des weiteren ist $i \in \mathbb{Q}(\alpha)$ und i erfüllt diese Gleichung, also $i^4 = 1$. Daher ist $\alpha \cdot i$ auch eine Wurzel von $\mathfrak{m}_\alpha$ und so ist auch $-\alpha \cdot i$. Wir haben 4 distinktive Wurzeln gefunden und wegen dem Grad von $\mathfrak{m}_\alpha$ kann es nicht mehr haben. □

Aufgabe 8 (2 Punkte). Sei R ein Ring. Kann es mehr als einen Elementen $x \in R$ geben, so dass

$$2x = 1?$$

Lösung. Die Antwort ist nein. Sein $x, y \in R$ so, dass $2x = 2y = 1$. Setze $a := x - y$. Wir haben

$$2a = 0.$$

Daher

$$\begin{aligned} 0 &= 1 \cdot 0 = (x + x) + (a + a) \\ &= xa + xa + xa + xa \\ &= 2xa + x2a \\ &= 1 \cdot a + x \cdot 0 \\ &= a. \end{aligned}$$

Also, $x = y$. □