Algebraische Zahlentheorie: [MTH-1483]

Ilia Pirashvili

Arbeitsblatt 6

1 Aufgaben

Aufgabe 1 (1 Punkt). Sei K ein algebraisches Zahlenkörper mit

$$[K : \mathbb{Q}] = 2.$$

Beweise, dass $K = \mathbb{Q}(\sqrt{a})$, für irgendeine quadratfreie Zahl $a \in \mathbb{Z}$.

Lösung. Von $[K : \mathbb{Q}] = 2$ wissen wir, dass K als $\mathbb{Q}$-Vektorraum 2-dimensional ist. Also solches gibt es ein $\alpha \in K$, so dass $\mathcal{B} = \{1, \alpha\}$ eine $\mathbb{Q}$-Basis von K ist. Da es eine Basis ist, muss es $p, q \in \mathbb{Q}$ geben, so dass

$$\alpha^2 = p\alpha + q \quad \Leftrightarrow \quad \alpha^2 - p\alpha - q = 0.$$

Es folgt, dass $\alpha = \frac{p \pm \sqrt{p^2-4q}}{2}$. Es ist klar, dass $\alpha \in K$ genau dann wenn $\pm(2\alpha - p) \in K$. Sei $\frac{r}{s} = p^2 - 4q$, $r, s \in \mathbb{Z}, s \neq 0$ und betrachte $\sqrt{\frac{r}{s}}$. Wir haben

$$\sqrt{\frac{r}{s}} = \frac{\sqrt{r}}{\sqrt{s}} = \frac{\sqrt{rs}}{s}.$$

Sei $b := rs$. Es gilt $\sqrt{\frac{r}{S}} \in K$ genau dann wenn $\sqrt{b} \in K$.

Wenn es eine natürliche Zahl $n \geq 2$ gibt, so dass $n^2 \mid b$, also $b = an^2, a \in \mathbb{Z}$, können wir $\sqrt{b} = n\sqrt{a}$ schreiben und natürlich ist $b \in K$ genau dann wenn $a \in K$. Als solches können wir sagen

$$K = \mathbb{Q}(\alpha) = \mathbb{Q}\left(\sqrt{\frac{r}{s}}\right) = \mathbb{Q}(\sqrt{b}) = \mathbb{Q}(\sqrt{a}),$$

wobei a eine quadratfreie ganze Zahl ist. □

Aufgabe 2 (1 Punkt). Sein $\alpha, \beta \in \mathbb{C}$, so dass $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\beta) : \mathbb{Q}] = 2$. Beweise, dass

$$\mathbb{Q}(\alpha, d\beta) = \mathbb{Q}(\alpha + \beta).$$

Lösung. Sei $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 2$. Da $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha, \beta)$, muss deswegen $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = \mathbb{Q}(\alpha + \beta) = \mathbb{Q}(\alpha, \beta)$ gelten und wir sind fertig. Sei also $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 4$. Da $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}[x, y]/(\mathfrak{m}_\alpha(x), \mathfrak{m}_\beta(y))$, $\{1, x, x^2, \ldots, y, xy, x^2y, \ldots, y^2, xy^2, x^2y^2, \ldots\}$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}[x, y]$ ist und laut Annahme wir die Klassen von x^2 und y^2 mit x bzw. y ausdrücken können, muss $\{1, x, y, xy\}$ ein erzeugendes System sein. In anderen Worten, $\{1, \alpha, \beta, \alpha\beta\}$ muss für uns ein erzeugendes System sein. Aus Dimensionsgründen ist es eine Basis.

Da $\mathbb{Q}(\alpha + \beta) \subseteq \mathbb{Q}(\alpha, \beta)$, gilt nur zu beweisen, dass $[\mathbb{Q}(\alpha + \beta) : \mathbb{Q}] = 4$. Wenn nicht, muss es laut dem Körperturmsatz ≤ 2 sein. Daher muss es $r, s \in \mathbb{Q}$ geben, mit

$$(\alpha + \beta)^2 = r + s(\alpha + \beta). \tag{1}$$

Da es bei Annahme $u, v, u', v' \in \mathbb{Q}$ gibt, mit $\alpha^2 = u\alpha + v$ und $\beta^2 = u'\alpha + v'$, folgt, indem wir (1) ausmultiplizieren und unsere Formel darin einsetzen, dass

$$(u - s)\alpha + (u' - s)\beta + 2\alpha\beta = r - v - v' \in \mathbb{Q}.$$

Da aber, wie schon argumentiert, $1, \alpha, \beta, \alpha\beta$ eine $\mathbb{Q}$-Basis bilden, (daher über $\mathbb{Q}$ linear unabhängig sind), müssen alle Koeffizienten null sein, einschließlich 2. Widerspruch. □

Lösung. □

Aufgabe 3 (5 Punkte). Sei $K = \mathbb{Q}(\alpha)$, wobei $\alpha = \sqrt{2} + \sqrt{3}$.

i) Finde die Konjugierten von α.

ii) Liste alle Einbettungen $K \to \mathbb{C}$.

iii) Finde die Norm und die Spur von α.

iv) Zeige, dass
$$\mathcal{B} = \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$$
eine $\mathbb{Q}$-Basis von K ist.

v) Berechne die Diskriminante
$$\Delta(\mathcal{B}).$$

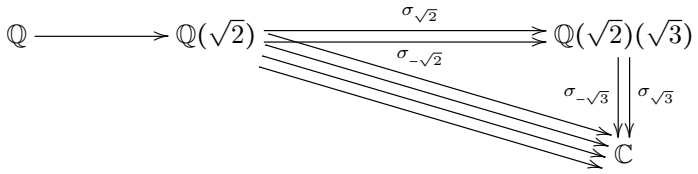
Lösung. i) Wie in Aufgabe 10 von Arbeitsblatt 2 gezeigt, ist das Minimalpolynom von α
$$\mathfrak{m}_\alpha(x) = x^4 - 10x^2 + 1.$$
Wir suchen also nach anderen Lösungen dieses Polynoms. Wir machen eine Variablenwechsel und sagen $y \equiv x^2$. Daher haben wir
$$\mathfrak{m}_\alpha(y) = y^2 - 10y + 1,$$
wessen Nullstellen
$$y = 5 \pm 2\sqrt{6},$$
sind. Daher
$$x^2 = 5 \pm 2\sqrt{6},$$
was zu
$$x = \pm\left(\sqrt{5 \pm 2\sqrt{6}}\right) = \pm\left(\sqrt{(\sqrt{2})^2 + 2\sqrt{6} + (\sqrt{3})^2}\right) = \pm\left(\sqrt{\left(\sqrt{2} \pm \sqrt{3}\right)^2}\right) = \pm\left(\sqrt{2} \pm \sqrt{3}\right)$$
führt. Die Wurzeln, bzw. die Konjugierten von α sind also
$$\alpha_1 = \sqrt{2} + \sqrt{3}, \quad \alpha_2 = \sqrt{2} - \sqrt{3}, \quad \alpha_3 = -\sqrt{2} + \sqrt{3}, \quad \alpha_4 = -\sqrt{2} - \sqrt{3}.$$

Eine andere Möglichkeit dies zu sehen, ist die Isomorphie
$$\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3})$$
zu betrachten. Es ist klar, dass die Konjugierten von $\sqrt{3}$ über $\mathbb{Q}(\sqrt{2})$ gleich
$$\sqrt{3}, \quad -\sqrt{3}$$
sind. Als solches haben wir 2 Einbettungen
$$\sigma_{\sqrt{3}}, \sigma_{-\sqrt{3}} : \mathbb{Q}(\sqrt{2} + \sqrt{3}) \to \mathbb{C},$$
welche $\mathbb{Q}(\sqrt{2})$ fix lässt. Ähnliches gilt auch für $\sqrt{2}$ über $\mathbb{Q}$, wo wir die zwei Abbildungen
$$\sigma_{\sqrt{2}}, \sigma_{-\sqrt{2}} : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})(\sqrt{3}),$$

welche $\mathbb{Q}$ fixiert lässt. Daher fixiert jede mögliche Komposition

$$\sigma_{\pm\sqrt{3}} \circ \sigma_{\pm\sqrt{2}} : \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3}) \to \mathbb{C}$$

$\mathbb{Q}$. Das können wir in Diagrammen wie folgt ausdrücken:



ii) Es ist klar, dass $\{1, \alpha, \alpha^2, \alpha^3\}$ eine $\mathbb{Q}$-Basis von K ist. Um eine Einbettung

$$\sigma_i : K \to \mathbb{C}$$

festzulegen, müssen wir sagen, wo $a + b\alpha + c\alpha^2 + d\alpha^3$ geht. Wir definieren die Abbildungen wie folgt:

$$\sigma_i(a + b\alpha + c\alpha^2 + d\alpha^3) = a + b\alpha_i + c(\alpha_i)^2 + d(\alpha_i)^3.$$

Nun kann man genau ausrechnen, wohin die einzelnen Abbildungen gehen und es durch α darstellen. Dafür muss man nur die Potenten der α_i ausrechnen.

iii)

$$\begin{aligned}
\mathsf{N}(\alpha) &= \prod_{i=1}^{4} \sigma_i(\alpha) = \prod_{i=1}^{4} \alpha_i \\
&= (\sqrt{2}+\sqrt{3})(-\sqrt{2}+\sqrt{3})(\sqrt{2}-\sqrt{3})(-\sqrt{2}-\sqrt{3}) \\
&= (\sqrt{2}+\sqrt{3})^2(\sqrt{2}-\sqrt{3})^2 \\
&= (5+\sqrt{6})(5-\sqrt{6}) \\
&= 25 - 4 * 6 = 1 \\
\mathsf{Sp}(\alpha) &= \sum_{i=1}^{4} \sigma_i(\alpha) = \sum_{i=1}^{4} \alpha_i \\
&= (\sqrt{2}+\sqrt{3}) + (-\sqrt{2}+\sqrt{3}) + (\sqrt{2}-\sqrt{3}) + (-\sqrt{2}-\sqrt{3}) \\
&= 0
\end{aligned}$$

iv) Es ist klar, dass $\sqrt{2}, \sqrt{3}, \sqrt{6} \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) \simeq \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Sein $a, b, c, d \in \mathbb{Q}$, so dass

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0.$$

Wir wollen zeigen, dass $a, b, c, d = 0$. Da wir die Gleichung wie folgt umstellen können

$$(a + \sqrt{2}) + (c + d\sqrt{2})\sqrt{3} = 0,$$

ist dies äquivalent zu sagen, dass $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Wir werden dies durch Widerspruch beweisen. Sei

$$\sqrt{3} = u + v\sqrt{2}, \quad u, v \in \mathbb{Q}$$

Dann gilt

$$3 = u^2 + 2v^2 + 2uv\sqrt{2},$$

woraus

$$\sqrt{2} = \frac{3 - u^2 + 2v^2}{2uv}$$

folgt. Da $\sqrt{2} \notin \mathbb{Q}$, darf die rechte Seite "keinen Sinn machen". Also, $uv = 0$ muss gelten.

Fall 1: $\underline{u = 0}$. Es folgt

$$3 = 2v^2.$$

Sei $v = \frac{v_0}{v_1}, v_i \in \mathbb{Z}$ gekürzt. Dann gilt

$$3v_1^2 = 2v_0^2,$$

woraus folgt, dass $3 \mid v_0^2$. Daher muss auch $3^2 \mid v_0^2$, aber $9 \nmid 3v_1^2$, da v_1 und v_0 teilerfremd sind.

Fall 2: $\underline{v = 0}$. Wir haben

$$3 = u^2$$

was mit dem selben Argument wie oben zu einem Widerspruch führt. Daher folgt, dass

$$a + b\sqrt{2} = 0 = c + d\sqrt{2},$$

woraus $a = b = c = d = 0$ folgt, da $\sqrt{2} \notin \mathbb{Q}$.

v) Es gilt

$$\begin{aligned}
\Delta(\mathcal{B}) &= \det \begin{pmatrix} 1 & \sqrt{2} & \sqrt{3} & \sqrt{6} \\ 1 & -\sqrt{2} & \sqrt{3} & -\sqrt{6} \\ 1 & \sqrt{2} & -\sqrt{3} & -\sqrt{6} \\ 1 & -\sqrt{2} & -\sqrt{3} & \sqrt{6} \end{pmatrix}^2 \\
&= 2 \cdot 3 \cdot 6 \det \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}^2 \\
&= 2 \cdot 3 \cdot 6 \det \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & -2 & 0 & -2 \\ 0 & 0 & -2 & -2 \\ 0 & -2 & -2 & 0 \end{pmatrix}^2 \\
&= 2 \cdot 3 \cdot 6 \det \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & -2 & 0 & -2 \\ 0 & 0 & -2 & -2 \\ 0 & 0 & 0 & 4 \end{pmatrix}^2 \\
&= 2^{10} 3^2.
\end{aligned}$$

□

Aufgabe 4 (1 Punkt). Sei $[L : K] = p$ eine Primzahl. Beweise, dass jedes Element $\alpha \in L \setminus K$ primitiv ist. Das heißt, dass

$$L = K(\alpha).$$

Lösung. Beim Körperturmsatz haben wir

$$p = [L : K] = [L : K(\alpha)][K(\alpha) : K],$$

woraus folgt, dass $[K(\alpha) : K] = 1$ oder p. Es kann nicht 1 sein, da sonst $\alpha \in K$ folgen würde, also ist es p. Daher muss $[L : K(\alpha)] = 1$ sein, woraus folgt, dass $L \simeq K(\alpha)$. □

Aufgabe 5 (4 Punkte). Sei $\alpha = \sqrt[3]{2}$ und $\beta = e^{\frac{2\pi i}{3}} \alpha$. Sei $K = \mathbb{Q}(\alpha, \beta)$.

i) Finde die Konjugierten von α mithilfe des Minimalpolynoms von $\sqrt[3]{2}$.

ii) Zeige, dass $\mathbb{Q}(\alpha) \simeq \mathbb{Q}(\beta)$ indem man das Minimalpolynom von α bestimmt.

iii) Zeige, dass $\alpha \notin \mathbb{Q}(\beta)$ und $\beta \notin \mathbb{Q}(\alpha)$.

iv) Beschreibe alle Einbettungen $K \to \mathbb{C}$.

Lösung. i) Das Minimalpolynom von α ist $\mathfrak{m}_\alpha = x^3 - 2$. Sei $\zeta_3 = \frac{-1+\sqrt{3}i}{2} = e^{\frac{2\pi i}{3}} \in \mathbb{C}$ eine kubische Einheitswurzel. Dann sind

$$\alpha_1 = \alpha, \quad \alpha_2 = \alpha\zeta_3 = \beta, \quad \alpha_1 = \alpha\zeta_3^2 = \beta\zeta_3$$

auch Wurzeln von $\mathfrak{m}_\alpha$, daher die Konjugierten von α.

ii) Da sie das selbe Minimalpolynom $\mathfrak{m}_\alpha$ haben, gilt

$$\mathbb{Q}(\alpha) \simeq \mathbb{Q}[X]/(\mathfrak{m}_\alpha) = \mathbb{Q}[X]/(\mathfrak{m}_\beta) \simeq \mathbb{Q}(\beta).$$

iii) Angenommen $\alpha \in \mathbb{Q}(\beta)$ oder $\beta \in \mathbb{Q}(\alpha)$. Daraus folgt, dass $\zeta_3 = \frac{\beta}{\alpha} \in \mathbb{Q}(\alpha)$ (oder $\mathbb{Q}(\beta)$), also

$$\mathbb{Q}(\zeta_3) \subseteq \mathbb{Q}(\alpha).$$

Dies widerspricht den Körperturmsatz, da x^2+x+1 das Minimalpolynom von ζ_3 ist, wir also

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3 \quad \text{und} \quad [\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$$

haben.

iv) Von unserer obigen Argumentation können wir sehen, dass

$$K = \mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha, \zeta_3).$$

Da $\alpha \mapsto \{\alpha_1, \alpha_2, \alpha_3\}$ und $\zeta_3 \mapsto \{\zeta_3, \zeta_3^2\}$ alle erlaubt sind, haben wir

$$\begin{aligned}
\sigma_1(\alpha) &= \alpha & \sigma_1(\zeta_3) &= \zeta_3 \\
\sigma_2(\alpha) &= \alpha\zeta_3 & \sigma_2(\zeta_3) &= \zeta_3 \\
\sigma_3(\alpha) &= \alpha\zeta_3^2 & \sigma_3(\zeta_3) &= \zeta_3 \\
\sigma_4(\alpha) &= \alpha & \sigma_4(\zeta_3) &= \zeta_3^2 \\
\sigma_5(\alpha) &= \alpha\zeta_3 & \sigma_5(\zeta_3) &= \zeta_3^2 \\
\sigma_6(\alpha) &= \alpha\zeta_3^2 & \sigma_6(\zeta_3) &= \zeta_3^2.
\end{aligned}$$

Dies wäre für die Lösung natürlich ausreichend, wenn wir es aber im Sinne von β ausdrücken wollen, müssen wir uns an die Formeln $\zeta_3 = \frac{\beta}{\alpha}$ und $\sigma_i(\frac{\beta}{\alpha}) = \frac{\sigma_i(\beta)}{\sigma_i(\alpha)}$ wenden. Daraus folgt direkt

$$\sigma_i(\beta) = \sigma_i(\alpha)\sigma_i(\zeta_3).$$

Daher

$$\begin{aligned}
\sigma_1(\alpha) &= \alpha & \sigma_1(\beta) &= \alpha\zeta_3 = \beta \\
\sigma_2(\alpha) &= \alpha\zeta_3 & \sigma_2(\beta) &= \alpha\zeta_3^2 = \frac{\beta^2}{\alpha} \\
\sigma_3(\alpha) &= \alpha\zeta_3^2 & \sigma_3(\beta) &= \alpha \\
\sigma_4(\alpha) &= \alpha & \sigma_4(\beta) &= \alpha\zeta_3^2 = \frac{\beta^2}{\alpha} \\
\sigma_5(\alpha) &= \alpha\zeta_3 & \sigma_5(\beta) &= \alpha \\
\sigma_6(\alpha) &= \alpha\zeta_3^2 & \sigma_6(\beta) &= \alpha\zeta_3 = \alpha.
\end{aligned}$$

□

Aufgabe 6 (3 Punkte). Sein $p, q \in \mathbb{Z}$, so dass $f(x) = X^3 + px + q$ irreduzibel über $\mathbb{Z}[X]$ ist und sei $\alpha \in \mathbb{C}$ eine Wurzel von $f(x)$.

i) Beweise, dass $\mathsf{Sp}(1) = 3, \mathsf{Sp}(\alpha) = 0, \mathsf{Sp}(\alpha^2) = -2p$ und $\mathsf{Sp}(\alpha^3) = -3q$.

ii) Was ist $\mathsf{Sp}(\alpha^4)$?

iii) Beweise, dass
$$\Delta(1, \alpha, \alpha^2) = -4p^3 - 27q^2.$$

Lösung. Wir werden die Symmetrischen Polynome benutzen um diese Aufgabe zu lösen. Die Formeln die wir in der Vorlesung gesehen habe ($s_1 = a_{n-1}$ etc.) sind besser unter dem Namen *Satz von Vieta* bekannt.

Sein $\alpha = \alpha_1, \alpha_2, \alpha_3$ die Konjugierten von α. Ein beliebiges Element kann als $x = a + b\alpha + c\alpha^2$ geschrieben werden. Als solches haben wir, dass

$$\mathsf{Sp}(x) = \sum_{i=1}^{3} \sigma_i(x) = (a + b\alpha + 1 + c\alpha + 1^2) + (a + b\alpha_2 + c\alpha_2^2) + (a + b\alpha_3 + c\alpha_3^2).$$

i) Sei $x = 1$. Wir haben $a = 1, b = 0, c = 0$, daher
$$\mathsf{Sp}(1) = 1 + 1 + 1 = 3.$$
Sei $x = \alpha$. Wir haben $a = 0, b = 1, c = 0$.
$$\mathsf{Sp}(\alpha) = \alpha_1 + \alpha_2 + \alpha_3 = s_1(\alpha) = 0,$$
in unserem Fall, da nichts vor x^2 steht.
Sei $x = \alpha^2$. Wir haben $a = 0, b = 0, c = 1$, also
$$\mathsf{Sp}(\alpha^2) = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 = s_1(\alpha)^2 - 2s_2(\alpha) = -2p.$$
Sei $x = \alpha^3$. Da $f(\alpha) = 0$ bei Definition, haben wir $\alpha^3 = -p\alpha - q$. Wir benutzen nun die Formel
$$\mathsf{Sp}(x + y) = \mathsf{Sp}(x) + \mathsf{Sp}(y).$$
Es ist klar (sieh $x = 1$), dass
$$\mathsf{Sp}(-q) = -3q.$$
Da $p \in \mathbb{Z}$, reduziert sich das multiplizieren mit p aufs addieren. Daher haben wir
$$\mathsf{Sp}(-p\alpha) = -p\mathsf{Sp}(\alpha) = 0$$
bei unserer vorigen Rechnung. Also
$$\mathsf{Sp}(\alpha^3) = \mathsf{Sp}(-p\alpha) - \mathsf{Sp}(q) = -3q.$$

ii) Es gilt
$$\mathsf{Sp}(\alpha^4) = \mathsf{Sp}(\alpha\alpha^3) = \mathsf{Sp}(\alpha(-p\alpha - q)) = \mathsf{Sp}(-p\alpha^2) - \mathsf{Sp}(q\alpha) = -p\mathsf{Sp}(\alpha^2) - q\mathsf{Sp}(\alpha) = 2p^2.$$

iii) Mithilfe von Vandermondes Formel haben wir
$$\begin{aligned} \Delta(1, \alpha, \alpha^2) &= [(\alpha_3 - \alpha_2)(\alpha_3 - \alpha_1)(\alpha_2 - \alpha_1)]^2 \\ &= \cdots \end{aligned}$$
Dies ist eine Symmetrische Gleichung und wir können es mit den elementaren symmetrischen Polynomen darstellen. Wenn man alles richtig gemacht hat, sollte man auf die passende Lösung kommen.

□