Universität Konstanz
Fachbereich Mathematik und Statistik
Sommersemester 2011

Christoph Hanselka
Aaron Kunert
Markus Schweighofer

Lösungsblatt 8 zur Zahlentheorie

Aufgabe 1.
Wir setzen $A := (\mathrm{tr}_{L|K}(x_i x_j))_{1\le i,j\le n}$ und $B := (\mathrm{tr}_{L|K}(x_{\sigma(i)} x_{\sigma(j)}))_{1\le i,j\le n}$. Es genügt zu zeigen, dass $\det(A) = \det(B)$. Es gilt

$$\det(A) = \sum_{\pi\in S_n} \mathrm{sgn}(\pi) \prod_{i=1}^{n} \mathrm{tr}_{L|K}(x_i x_{\pi(i)}),$$
$$\det(B) = \sum_{\pi\in S_n} \mathrm{sgn}(\pi) \prod_{i=1}^{n} \mathrm{tr}_{L|K}(x_{\sigma(i)} x_{(\pi\sigma)(i)}).$$

Da Multiplikation kommutativ ist

$$\prod_{i=1}^{n} \mathrm{tr}_{L|K}(x_i x_{\pi(i)}) = \prod_{i=1}^{n} \mathrm{tr}_{L|K}(x_{\sigma(i)} x_{(\pi\sigma)(i)}),$$

denn das rechte Produkt entsteht aus dem linken Produkt nur doch Permutation der Faktoren. Daraus folgt aber sofort $\det(A) = \det(B)$.

Aufgabe 2.
Zunächst überlegt man sich, dass das Polynom $f(X) = X^3+2X+1$ irreduzibel ist. Dazu betrachtet man es beispielsweise über $\mathbb{Z}/(3)$. Dort hat es keine Nullstellen ist also irreduzibel. Nach dem Reduktionskriterium ist es daher auch über $\mathbb{Q}$ irreduzibel. Inbesondere folgt $[\mathbb{Q}(z) : \mathbb{Q}] = \deg(f) = 3$. Als nächstes ist eine $\mathbb{Z}$–Basis von $\mathbb{Z}[z]$ zu finden. Da $\{1,z,z^2\} \subset \mathbb{Z}[z]$ linear unabhängig über $\mathbb{Q}$ ist, liegt die Vermutung nahe, dass diese Menge eine Basis von $\mathbb{Z}[z]$ ist. Es genügt zu zeigen, dass sie ganz $\mathbb{Z}[z]$ erzeugt. Dies ist der Fall, wenn jede Potenz von z eine $\mathbb{Z}$–Linearkombination von $1,z,z^2$ ist. Es ist aber $z^3 = -2z - 1 \in \mathbb{Z} \oplus z\mathbb{Z} \oplus z^2\mathbb{Z}$, was zeigt, dass $\{1,z,z^2\}$ schon eine Basis von $\mathbb{Z}[z]$ ist. Zuletzt ist noch die Diskriminante von $(1,z,z^2)$ auszurechnen. Dazu bestimmt man die Spuren von $1,z,z^2,z^3$ und z^4. Wir schreiben kurz tr anstatt $\mathrm{tr}_{\mathbb{Q}(z)|\mathbb{Q}}$. Es ist $\mathrm{tr}(1) = 3$. Für die übrigen Spuren bestimmen wir zunächst die Darstellungsmatrizen der Linksmultiplikationen und berechnen deren Spur. Es ist

$$M_{\varphi_z} = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & -2 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{und} \quad M_{\varphi_{z^2}} = \begin{pmatrix} 0 & -1 & 0 \\ 0 & -2 & -1 \\ 1 & 0 & -2 \end{pmatrix},$$

daher ergibt sich $\mathrm{tr}(z) = 0$ und $\mathrm{tr}(z^2) = -4$. Um $\mathrm{tr}(z^3)$ und $\mathrm{tr}(z^4)$ zu bestimmen, verwenden wir die Linearität der Spur. So erhält man $\mathrm{tr}(z^3) = \mathrm{tr}(-2z-1) = -3$ und $\mathrm{tr}(z^4) = \mathrm{tr}(-2z^2 - z) = 8$. Wir erhalten somit

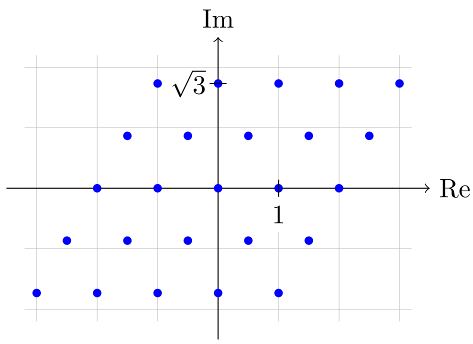
$$\mathrm{d}_{\mathbb{Q}(z)|\mathbb{Q}}(1,z,z^2) = \det \begin{pmatrix} 3 & 0 & -4 \\ 0 & -4 & -3 \\ -4 & -3 & 8 \end{pmatrix} = -59$$

Aufgabe 3.

(a) Die Körpererweiterung $\mathbb{Q} \subset \mathbb{Q}(\pi)$ ist normal und separabel also eine Galoiserweiterung. Weiter ist die komplexe Konjugation ein Automorphismus von $\mathbb{Q}(\pi)$. Daher besteht die Galoisgruppe von $\mathbb{Q}(\pi) \mid \mathbb{Q}$ genau aus der Identität und der komplexen Konjugation. Daher folgt aus Satz 2.4.14 $N(a+b\omega) = (a+b\omega)(a+b\omega)^* = |a+b\omega|^2$. Nachrechnen liefert

$$\begin{aligned}(a+b\omega)(a+b\omega)^* &= \left(a+b\cdot\frac{1+\pi}{2}\right)\left(a+b\cdot\frac{1-\pi}{2}\right)\\ &= a^2+ab\left(\frac{1-\pi}{2}\right)+ab\left(\frac{1+\pi}{2}\right)+\left(\frac{(1+\pi)(1-\pi)}{4}\right)b^2\\ &= a^2+ab+\left(\frac{1-\pi^2}{4}\right)b^2\\ &= a^2+ab+b^2\end{aligned}$$

(b) Folgendes Bild ergibt sich, wenn man den freien $\mathbb{Z}$–Modul, erzeugt von 1 und $\frac{1+\pi}{2}$, in die komplexe Ebene einzeichnet.



(c) Aus dem Bild erkennt man schon, dass es zu jedem $x \in K$ ein $q \in R$ gibt mit $|x-q| < 1$. Dies lässt sich wie folgt formal beweisen. Sei $x = x_1 + x_2\omega \in K$ mit $x_1,x_2 \in \mathbb{Q}$. Wähle $q_1,q_2 \in \mathbb{Z}$ so, dass $|x_1 - q_1| \leq \frac{1}{2}$ und $|x_2 - q_2| \leq \frac{1}{2}$. Dann gilt für $q := q_1 + q_2\omega$ die Abschätzung

$$\begin{aligned}|x-q| &= |(x_1-q_1)+(x_2-q_2)\omega|\\ &\leq |x_1-q_1| + |(x_2-q_2)||\omega|\\ &\leq \frac{1}{4}+\frac{1}{4}|\omega|\\ &= \frac{1}{4}+\frac{\sqrt{3}}{4}\end{aligned}$$

Wegen $\sqrt{3} < 3$ folgt $|x-q| < 1$. Nun lässt sich zeigen, dass R euklidisch bezüglich der Norm ist. Seien $x,f \in R\backslash\{0\}$. Sei $q \in R$ mit $|\frac{x}{f} - q| < 1$. Dann ist $|x - qf| < |f|$. Setzt man $r = x - qf$, dann hat man eine Darstellung $x = qf + r$ mit $|r| < |f|$, was zeigt, dass R euklidisch ist.

(d) Die Gleichung in π und ω lassen sich unmittelbar nachrechnen. Aus der zweiten folgt $R^* \subseteq R$, aus der ersten (oder der zweiten) folgt $K^* \subseteq K$. Da komplexe Konjugation eine Involution ist, folgt die Behauptung.

(e) Zunächst zeigt man, dass $R^\times = \{x \in R \mid |N(x)| = 1\}$ gilt. Hat $x \in R$ die Norm 1, so gilt $\pm 1 = N(x) = xx^*$. Da x^* ebenfalls in R liegt, ist x^* bzw. $-x^*$ invers zu x. Ist umgekehrt

$x \in R^\times$, so gibt es $y \in R$ mit $xy = 1$, also ist $1 = N(x)N(y)$. Da alle Elemente aus R eine ganzzahlige Norm haben, muss $N(x) \in \mathbb{Z}^\times$ gelten. Damit ist nur noch zu zeigen, dass

$$\{x \in R \mid |N(x)| = 1\} = \{\pm\omega, \pm\,\omega^*, \pm\,1\}$$

ist. Angenommen $N(a + b\omega) = \pm 1$ für $a,b \in \mathbb{Z}$. Nach Teilaufgabe (a) ist somit $a^2 + ab + b^2 = \pm 1$. Es ist $N(a + \omega b) = a^2 + ab + b^2 = \frac{1}{2}((a + b)^2 + a^2 + b^2) \geq 0$. Daher genügt es, die Gleichung $(a + b)^2 + a^2 + b^2 = 2$ zu lösen. Offensichtlich ist $|a|,|b| \leq 1$ Für den Fall $ab \geq 0$ (gleiches Vorzeichen) ist $\{\pm 1, \pm\omega\}$ die gesamte Lösungsmenge. Für $ab < 0$ sind die Belegungen $(1,-1)$ und $(-1,1)$ die einzigen Möglichkeiten, die tatsächlich auch die Gleichung lösen. Daraus ergeben sich die übrigen Lösungen zu ω^* und $-\omega^*$.

(f) Es ist $\pi = -1 + 2\omega$. Damit ergibt sich $N(\pi) = (-1)^2 - 2 + 2^2 = 3$. Angenommen $\pi = xy$ mit $x,y \in R$, so ist $3 = N(\pi) = N(x)N(y)$. Da $3 \in \mathbb{Z}$ irreduzibel ist, ist $N(x)$ oder $N(y)$ in $\mathbb{Z}^\times$ und somit $x \in R^\times$ oder $y \in R^\times$. Daher ist $\pi \in R$ irreduzibel und daher (wegen R faktoriell) ein Primelement.

(g) Sei $a \in \mathbb{Z}$. Wir schreiben $a = 3k + r$ mit $k \in \mathbb{Z}$ und $r \in \{0,1,2\}$. Dann ist $a^3 = 27k^3 + 27k^2 r + 9kr^3 + r^3$. Insbesondere ist $a^3 \equiv_{(9)} r^3$. Also ist $a \equiv_{(9)} \pm 1$ oder $a \equiv_{(9)} 0$. Angenommen es wäre $3 \nmid x,y,z$, so ergibt die Gleichung $x^3 + y^3 = z^3$ modulo 9 gelesen, die Gleichungen $\pm 1 \pm 1 = \pm 1$, was ein Widerspruch ist. Daher ist x,y oder z durch 3 teilbar.

(h) Möchte man zeigen, dass $x^3 + y^3 = z^3$ in $\mathbb{Z} \setminus \{0\}$ keine Lösung hat, so kann man im Widerspruch annehmen, dass (x,y,z) ein Lösung ist. Ist $3 \nmid z$ so ist nach Teilaufgabe (g) x oder y durch 3 teilbar. Wir nehmen ohne Einschränkung an, dass $3 \mid x$. Dann erhalten wir die Gleichung $y^3 - z^3 = -x^3$ und daher $y^3 + (-z)^3 = (-x)^3$. Wegen $x,y,z \neq 0$ erhalten wir somit eine neue Lösung in $\mathbb{Z} \setminus \{0\}$, für die die rechte Seite durch 3 teilbar ist. Also lässt sich ohne Einschränkung $3 \mid z$ annehmen. Ist d der größte gemeinsame Teiler von x,y,z, so ist auch

$$\left(\frac{x}{d}\right)^3 + \left(\frac{y}{d}\right)^3 = \left(\frac{z}{d}\right)^3$$

eine Lösung in $\mathbb{Z} \setminus \{0\}$. Da $\frac{x}{d}, \frac{y}{d}, \frac{z}{d}$ teilerfremd sind, kann man auch direkt annehmen, dass x,y,z teilerfremd sind.

(i) Es ist $\omega\omega^* = N(\omega) = 1$ und $\omega + \omega^* = 1$. Wir rechnen wie folgt

$$\begin{aligned}
(x + y)(x - \omega y)(x - \omega^* y) &= (x + y)(x^2 + y^2 - \omega xy - \omega^* xy) \\
&= (x + y)(x^2 - xy + y^2) \\
&= x^3 - x^2 y + xy^2 + x^2 y - xy^2 + y^3 \\
&= x^3 + y^3 \\
&= z^3.
\end{aligned}$$

(j) Es ist $N(x + y) = (x + y)^2 = x^2 + 2xy + y^2$. Wir haben

$$\begin{aligned}
N(x - y\omega) &= (x - \omega y)(x - \omega y)^* \\
&= (x - \omega y)(x - \omega^* y) \\
&= (x - \omega^{**} y)(x - \omega^* y) \\
&= N(x - \omega^* y).
\end{aligned}$$

Die Norm von $N(x - y\omega)$ berechnet sich zu $x^2 - xy + y^2$. Schließlich ist $N(x + y) - N(x - \omega) = x^2 + 2xy + y^2 - (x^2 - xy + y^2) = 3xy$, was durch 3 teilbar ist. Dies zeigt $N(x + y) \equiv_{(3)} N(x - \omega y)$.

(k) Wir zeigen zunächst, dass π (bis auf Assoziiertheit) das einzige Primelemen ist, dessen Norm durch 3 teilbar ist. Angenommen σ wäre prim mit $N(\sigma) = 3k$ für ein $k \in \mathbb{Z}$. Dann gibt es die zwei Zerlegungen

$$3k = -\pi\pi k = \pm\sigma\sigma^* k.$$

Wegen der eindeutigen Primfaktorzerlegung in R folgt, dass π und σ assoziert sind.

Ist $\alpha = \sigma_1^{e_1} \dots \sigma_r^{e_r}$ eine Zerlegung in paarweise verschiedene Primelemente. So ist $N(\alpha) = N(\sigma_1)^{e_1} \dots N(\sigma_r)^{e_r}$. Insbesondere ist $\pi \mid \alpha$, falls $3 \mid N(\alpha)$. Da z durch 3 (und somit durch π) teilbar ist, ist insbesondere einer der Faktoren in $(**)$ durch π teilbar. Daher ist die Norm einer der Faktoren durch 3 teilbar und somit sind wegen Teilaufgabe (j) alle Faktoren durch π teilbar. Wäre $x - \omega y$ durch 3 teilbar, so wäre $3 \mid x$ und $3 \mid y$ ein Widerspruch zur Teilerfremdheit von x,y,z. Analog argumentiert man mit $x - \omega^* y$.