Universität Konstanz
Fachbereich Mathematik und Statistik
Sommersemester 2016

Margaret Thomas
Julian Weißer

Übungsblatt 8 zur Zahlentheorie + Lösungen der Aufgaben 2 und 4

Aufgabe 1. (Ganzer Abschluss)

(a) Zeige, dass $\alpha := \sqrt{\frac{-1+\sqrt{-3}}{2}}$ ganz über $\mathbb{Z}[\sqrt{-3}]$ ist, $\mathrm{MinPoly}(\alpha|\mathbb{Q}(\sqrt{-3}))$ aber nicht in $\mathbb{Z}[\sqrt{-3}][X]$ liegt. Warum ist das kein Widerspruch zu Satz 2.4.14?

(b) Bestimme den ganzen Abschluss von $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{-3})$.

Aufgabe 2. (Norm über endlichen Körpern)

Sei $L|K$ eine Erweiterung endlicher Körper. Zeige, dass dann die Normabbildung $N_{L|K} : L \to K$ surjektiv ist.

Hinweis: Verwende ohne Beweis die Tatsache aus der Algebra, dass die Galoisgruppe $\mathrm{Gal}(L|K)$ von einer Potenz des Frobenius erzeugt wird, um die Norm in der Form $N_{L|K}(x) = x^a$ darzustellen.

Lösung: Schreibe $K = \mathbb{F}_{p^m}$ und $L = \mathbb{F}_{p^n}$ mit einer Primzahl p. Weil $L|K$ eine Körpererweiterung ist, muss $m \mid n$ gelten. Setze $d := [L : K]$ und $q := p^m$. Dann ist $q^d = p^n = \#L$.

Die Galoisgruppe $\mathrm{Gal}(L|K)$ wird von $\varphi : x \mapsto x^q$ erzeugt, und die i-te Potenz von φ bildet x auf $\varphi^i(x) = x^{q^i}$ ab. Wir kürzen $N_{L|K}$ mit N ab. Nach Satz 2.6.6 gilt $N(x) = \prod_{i=0}^{d-1} \varphi^i(x)$, damit ist

$$N(x) = x \cdot x^q \cdot x^{q^2} \cdots x^{q^{d-1}} = x^{1+q+q^2\cdots+q^{d-1}} = x^{\frac{q^d-1}{q-1}},$$

setze $a := \frac{q^d-1}{q-1}$. Die (eingeschränkte) Norm ist ein Gruppenhomomorphismus $L^\times \to K^\times$, damit gilt $\#L^\times = \#\ker(N) \cdot \#\mathrm{im}(N)$. Wir zeigen $s := \#\ker(N) \leq a$, dann folgt die Behauptung aus

$$\#\mathrm{im}(N) = \frac{\#L^\times}{s} \geq \frac{\#L^\times}{a} = \frac{p^n - 1}{\frac{q^d-1}{q-1}} = q - 1 = \#K^\times.$$

Sei dazu $z \in L^\times$ ein Erzeuger von $\ker(N)$ ($L^\times$ ist zyklisch, und Untergruppen davon ebenfalls), dann gilt natürlich $z^a = N(z) = 1$. Andererseits gilt $z^s = 1$ wegen $s = \#\ker(N)$ und s ist die kleinste Zahl > 0 mit dieser Eigenschaft, somit $s \leq a$.

Aufgabe 3. (Norm algebraischer Erweiterungen)

Sei $f := X^3 + 3X^2 + 2 \in \mathbb{Q}[X]$ und $\alpha \in \mathbb{C}$ eine Nullstelle von f. Berechne $\mathrm{N}_{\mathbb{Q}(\alpha)|\mathbb{Q}}(x)$ und $\mathrm{Sp}_{\mathbb{Q}(\alpha)|\mathbb{Q}}(x)$ für $x \in \mathbb{Q}(\alpha)$. Überlasse das Ausrechnen der Determinante einer Maschine oder einem Hörer der linearen Algebra!

Aufgabe 4. (Diskriminante)

Sei K ein Körper und $n \in \mathbb{N}$.

(a) Sei $f = \prod_{i=1}^{n}(X - \alpha_i) \in K[X]$ mit $\alpha_i \in \overline{K}$. Zeige:

$$\Delta_f = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} f'(\alpha_i).$$

(b) Sei nun $f := X^n + aX + b \in K[X]$. Zeige:

$$\Delta_f = (-1)^{\frac{n(n-1)}{2}}((1-n)^{n-1}a^n + n^n b^{n-1}).$$

Lösung:

(a) Berechne die Ableitung mit der Produktregel: $f' = \sum_{k=1}^{n} \prod_{j \neq k}(X - \alpha_j)$, Einsetzen ergibt $f'(\alpha_i) = \prod_{i \neq k}(\alpha_i - \alpha_k)$. Produktbildung liefert

$$\prod_{i=1}^{n} f'(\alpha_i) = \prod_{i=1}^{n}\prod_{i \neq k}(\alpha_i - \alpha_k) = \prod_{i<k} -(\alpha_i - \alpha_k)^2 = (-1)^{\frac{n(n-1)}{2}}\Delta_f.$$

(b) Schreibe wieder $f = \prod_{i=1}^{n}(X - \alpha_i)$. Das Produkt der Nullstellen von f ist gerade $\prod_{i=1}^{n} \alpha_i = (-1)^n b$. Nach (a) ist $\prod_{i=1}^{n} f'(\alpha_i) = (1-n)^{n-1}a^n + n^n b^{n-1}$ zu zeigen.
Fall 1: $a = 0$. Wir haben $f = X^n + b$, $f' = nX^{n-1}$ und finden

$$\prod_{i=1}^{n} f'(\alpha_i) = \prod_{i=1}^{n} n\alpha_i^{n-1} = n^n \left(\prod_{i=1}^{n} \alpha_i\right)^{n-1} = n^n(-1)^{n(n-1)} b^{n-1} \overset{n(n-1) \text{ gerade}}{=} n^n b^{n-1}.$$

Fall 2: $b = 0, a \neq 0$. Dann ist $f = X^n + aX = X(X^{n-1} + a)$. Wir sehen, dass $\alpha_1 = 0$ eine einfache Nullstelle von f ist und $\alpha_i \neq 0$ für $i > 1$, also $\alpha_i^n + a\alpha_i = 0 \Leftrightarrow \alpha_i^{n-1} = -a$. Es folgt

$$\prod_{i=1}^{n} f'(\alpha_i) = a\prod_{i=2}^{n}(n-1)\alpha_i^{n-1} = a \cdot \prod_{i=2}^{n}(n-1)(-a) = (1-n)^{n-1}a^n$$

Fall 3: $a \neq 0 \neq b$. Es ist $f' = nX^{n-1} + a$. Mit dem Hinweis ergibt sich $\alpha_i^n = -(a\alpha_i + b)$. Damit ist

$$f'(\alpha_i) = \frac{\alpha_i(n\alpha_i^{n-1} + a)}{\alpha_i} = \frac{-n(a\alpha_i + b) + a\alpha_i}{\alpha_i} = \frac{a(1-n)\alpha_i - nb}{\alpha_i}.$$

Wir setzen zusammen und formen weiter um:

$$\begin{aligned}
\prod_{i=1}^{n} f'(\alpha_i) &= (-1)^n b^{-1} \prod_{i=1}^{n}(a(1-n)\alpha_i - nb) \\
&\overset{(*)}{=} \frac{a^n(1-n)^n}{b} f\left(\frac{nb}{a(1-n)}\right) \\
&= \frac{a^n(1-n)^n}{b}\left(\left(\frac{nb}{a(1-n)}\right)^n + a\frac{nb}{a(1-n)} + b\right) \\
&= n^n b^{n-1} + a^n n(1-n)^{n-1} + a^n(1-n)(1-n)^{n-1} \\
&= (1-n)^{n-1}a^n + n^n b^{n-1}.
\end{aligned}$$

Die Gleichheit $(*)$ erhält man, indem man die Produktdarstellung $f\left(\frac{nb}{a(1-n)}\right) = \prod_{i=1}^{n}\left(\frac{nb}{a(1-n)} - \alpha_i\right)$ bemüht.