Algebraische Zahlentheorie: [MTH-1483]

Ilia Pirashvili

Arbeitsblatt 9

0.1 Aufgaben 9

Aufgabe 1 (2 Punkte). Sei α ein algebraisches Element und $\mathfrak{m}_\alpha = x^{p^k} - p$, wobei $p \in \mathbb{Z}$ eine Primzahl ist und $k \in \mathbb{N}$. Beweise mithilfe des Eisensteinkriteriums, dass

$$\mathcal{B} = \{1, \alpha, \dots, \alpha^{a-1}\}$$

eine Ganzheitsbasis ist.

Beweis. Wir haben

$$\begin{aligned} |\Delta(\mathcal{B})| &= |\mathsf{N}(\mathfrak{m}'_\alpha(\alpha))| = |\mathsf{N}(p^k \alpha^{p^{k-1}}| \\ &= |\mathsf{N}(p^k)\mathsf{N}(\alpha)^{p^{k-1}}| \\ &= |\left(p^k\right)^{p^k} \cdot p^{p^{k-1}}, \end{aligned}$$

also ist $\Delta(\mathcal{B}) = p^a$ wobei $a \in \mathbb{N}$. Daher sind die einzigen Elemente die wir auf Ganzalgebraität überprüfen müssen von der Form

$$\sum_{i=0}^{p^k-1} \frac{1}{p} a_i \alpha^i \quad 0 \le a_i \le p-1.$$

Das $\mathfrak{m}_\alpha$ das Eisensteinkriterium für die Primzahl p erfüllt ist klar. Daher sind die obigen Elemente aber nie ganzalgebraisch, was unsere Aufgabe beweist. □

Aufgabe 2 (6 Punkte). Sei

$$\zeta_n = \exp\left(\frac{2\pi i}{n}\right).$$

Für einen beliebigen $n \ge 1$ definieren wir das n-te zyklotomische Polynom $\Phi_n(x)$ durch Induktion, wobei

$$\Phi_1(x) = x - 1$$

$$\vdots$$

$$\Phi_n(x) = \frac{x^n - 1}{\prod \Phi_d(x)}.$$

Das Produkt wird hier über alle Teiler von n genommen, die streng kleiner sind, also $d < n$ und $d \mid n$. Daher gilt

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

i) Beweise, dass

$$\Phi_n(\zeta_n) = 0.$$

ii) Sei $n = p$ eine Primzahl. Beweise, dass

$$\Phi_p(x) = 1 + x + \cdots + x^{p-1}.$$

Von nun an, sei $n = p^k$, wobei p eine Primzahl ist und $k \geq 2$.

iii) Zeige, dass

$$\Phi_{p^k}(x) = \Phi_p(x^{p^{k-1}}) = 1 + x^{p^{k-1}} + x^{2p^{k-1}} + \cdots + x^{(p-1)p^{k-1}}.$$

Spezifisch, dass $\mathsf{grad}(\Phi_{p^k}(x)) = p^k - p^{k-1}$.

iv) Beweise, dass $\Phi_{p^k}(x+1)$ das Eisensteinkriterium erfüllt und als solches irreduzibel ist. Schlussfolgere, dass für $n = p^k$, Φ_n das Minimalpolynom von ζ_n ist und daher

$$[\mathbb{Q}(\zeta_{p^k}) : \mathbb{Q}] = p^k - p^{k-1}$$

gilt. (Es wurde schon von Gauß beweisen, dass Φ_n für alle n irreduzibel ist!)

v) Beweise, dass, bis au Vorzeichen, $\Delta(1, \zeta_n, \cdots, \zeta_n^m)$ ein Vielfaches von p ist. Hier gilt $n = p^k$ und $m = p^k - p^{k-1}$.

vi) Sei $K = \mathbb{Q}(\zeta_{p^k})$. Schlussfolgere, dass $\mathfrak{o}_K = \mathbb{Z}[\zeta_{p^k}]$.

Wem es zu allgemein ist, kann Aufgaben iii)-vi) auch nur für die Fälle $n = 8$ und $n = 9$ beweisen.

Beweis. i) Da ζ_n eine Wurzel von $x^n - 1 = \prod_{d|n} \Phi_d(x)$ ist, reicht es aus, dass $\Phi_d(\zeta_n) \neq 0$ für alle Teiler $d|n$ von n die streng kleiner sind als n. Sei ζ_n eine Wurzel von $\Phi_d(x)$, mit $d < n$. Dann ist ζ_n auch eine Wurzel von $x^d - 1$. Daher

$$1 = (\zeta_n)^d = \exp\left(\frac{2d\pi i}{n}\right)$$

gilt, ist $n \mid d$ ein Teiler von d, was unserer Annahme an d widerspricht (das es streng kleiner als n sein sollte).

ii) Da p prim ist, haben wir nur zwei Möglichkeiten von d. Daher ist

$$x^p - 1 = \Phi_1(x)\Phi_p(x) = (x-1)\Phi_p(x),$$

woraus

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = 1 + x + \cdots + x^{p-1}.$$

folgt.

iii) Bei Definition gilt

$$y^p - 1 = (y-1)\Phi_p(y).$$

Setze

$$y = x^{p^{k-1}}.$$

Da $y^p = x^{p^k}$ haben wir

$$x^{p^k} - 1 = (x^{p^{k-1}} - 1)\Phi_p(x^{p^{k-1}}).$$

Bei Definition haben wir auch

$$x^{p^k} - 1 = \prod_{d|p^k} \Phi_d(x).$$

Wir bemerken, dass wenn $d \mid p^k$, entweder $d|p^{k-1}$ oder $d = p^{k-1}$. Daher

$$x^{p^k} - 1 = \prod_{d|p^{k-1}} \Phi_d(x) \cdot \Phi_{p^k}(x) = (x^{p^{k-1}} - 1) \cdot \Phi_{p^k}(x).$$

Wir vergleichen dies mit der vorigen Gleichung und erhalten

$$\Phi_p(x^{p^{k-1}}) = \Phi_{p^k}(x).$$

iv) Sei

$$f(x) = \Phi_{p^n}(x+1) = 1 + (x+1)^{p^{k-1}} + (x+1)^{2p^{k-1}} + \cdots + (x+1)^{(p-1)p^{k-1}}.$$

Da das freie Term unseres Polynoms $f(x)$ gleich p ist, brauchen wir nur zu zeigen, dass

$$f(x) \equiv x^{p^{k-1}(p-1)} \pmod{p} \mod p.$$

Man erinnere sich, dass die Abbildung $y \mapsto y^p$ in Charakteristik p ein Ringhomomorphismus ist (Frobenius). Daher ist

$$f(x) \equiv 1 + (x^{p^{k-1}} + 1) + (x^{p^{k-1}} + 1)^2 + \cdots + (x^{p^{k-1}} + 1)^{p-1} \mod p.$$

Um diese Summe zu bestimmen, erinnern wir uns, dass

$$1 + y + \cdots y^{p-1} = \frac{y^p - 1}{y - 1}.$$

(Geometrische Folge). Sei $y = x^{p^{k-1}} + 1$. Wir erhalten

$$f(x) = \frac{(x^{p^{k-1}} + 1)^p - 1}{x^{p^{k-1}}} = \frac{x^{p^k} + 1 - 1}{x^{p^{k-1}}} = x^{p^k - p^{k-1}} \mod p.$$

v) Wir benutzen Satz 2.4.13:

$$\Delta(1, \zeta_n, \cdots, \zeta_n^{d-1}) = (-1)^{\frac{d(d-1)}{2}} \mathsf{N}(\Phi_n'(\zeta_n)),$$

wobei $n = p^k$ und $d = p^k - p^{k-1}$. Da

$$\Phi_{p^k}(x) = \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1}$$

folgt

$$\Phi_{p^k}'(x) = \frac{p^k x^{p^k - 1}(x^{p^{k-1}} - 1) - (x^{p^k} - 1)(x^{p^{k-1}} - 1)'}{(x^{p^{k-1}} - 1)^2}.$$

ζ_n annihiliert $x^n - 1$. Daher

$$\Phi_{p^k}(\zeta_{p^k}) = \frac{p^k \zeta_{p^k}^{p^k - 1}}{\zeta_{p^k}^{p^{k-1}} - 1}.$$

Die führt zu

$$\Delta(1, \zeta_n, \cdots, \zeta_n^{d-1}) = (-1)^{\frac{d(d-1)}{2}} \mathsf{N}\left(\frac{p^k \zeta_{p^k}^{p^k - 1}}{\zeta_{p^k}^{p^{k-1}} - 1}\right).$$

Teil ii) besagt, dass das freie Term des Minimalpolynoms von ζ_{p^k} gleich 1 ist. Daher ist $\mathsf{N}(\zeta_{p^n} = \pm 1$. Die Multiplikativität der Norm besagt nun, dass $\Delta(1, \zeta_n, \cdots, \zeta_n^{d-1})$ ein Teiler von $\pm \mathsf{N}(p^k)\mathsf{N}(\zeta_{p^k}) = \pm p^{kd}$ ist, was das Resultat impliziert.

v) Das selbe Argument wie bei $k = 1$ in der Vorlesung gilt auch hier. □