Zeitschrift: Elemente der Mathematik
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 40 (1985)
Heft: 3

Artikel: Lineare Abhängigkeiten von Einheitswurzeln
Autor: Johnsen, Karsten
DOI: https://doi.org/10.5169/seals-38830

ELEMENTE DER MATHEMATIK

Revue de mathématiques élémentaires – Rivista di matematica elementare

Zeitschrift zur Pflege der Mathematik
und zur Förderung des mathematisch-physikalischen Unterrichts

El. Math. | Band 40 | Nr. 3 | Seiten 57–80 | Basel, 10. Mai 1985

Lineare Abhängigkeiten von Einheitswurzeln

In seinem Tagebuch ([1]; Nr. 40) notiert C. F. Gauss am 9. Oktober 1796 den Satz, dass für eine ungerade Primzahl p jede nicht triviale ganzzahlige Linearkombination der primitiven p-ten Einheitswurzeln von Null verschieden ist. Dies ist offenbar gleichwertig mit der Irreduzibilität des p-ten Kreisteilungspolynoms $\Phi_p(t) = t^{p-1} + t^{p-2} + \cdots + t + 1$ über dem Körper $\mathbf{Q}$ der rationalen Zahlen (vgl. [3]). Bezeichnen wir allgemein mit $W(f(t))$ den von den Nullstellen eines Polynoms $f(t)$ erzeugten $\mathbf{Q}$-Teilraum von $\mathbf{C}$, so können wir den Satz von Gauss in der Form aussprechen:
Für eine Primzahl p ist $\dim W(\Phi_p(t)) = p - 1 = \operatorname{grad} \Phi_p(t)$.

Wir setzen allgemein $\dim f(t) = \dim W(f(t))$ und sprechen von der *Dimension* des Polynoms $f(t)$. Wegen $\Phi_4(t) = (t - i)(t + i)$ ist $\dim \Phi_4(t) = 1$, also $\dim \Phi_4(t) < \operatorname{grad} \Phi_4(t) = 2$. Wir wollen in dieser Note für jede natürliche Zahl m die Dimension des m-ten Kreisteilungspolynoms $\Phi_m(t)$ berechnen. Mit $\mathbf{Q}_m$ bezeichnen wir den m-ten Kreisteilungskörper. Bekanntlich gilt $\dim \mathbf{Q}_m = \operatorname{grad} \Phi_m(t) = \varphi(m)$. Ist $m = p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s}$ die kanonische Primzahlzerlegung von m, so gilt ([2]); Satz 123)

$$\mathbf{Q}_m = \mathbf{Q}_{p_1^{n_1}} \otimes \mathbf{Q}_{p_2^{n_2}} \otimes \cdots \otimes \mathbf{Q}_{p_s^{n_s}}.$$

Daraus folgt sofort

$$W(\Phi_m(t)) = W(\Phi_{p_1^{n_1}}(t)) \otimes \cdots \otimes W(\Phi_{p_s^{n_s}}(t)),$$

also

$$\dim \Phi_m(t) = \prod_{i=1}^{s} \dim \Phi_{p_i^{n_i}}(t).$$

Wir können uns daher auf den Fall beschränken, dass $m = p^n$ eine Primzahlpotenz ist. Für $i \in \{1, 2, \ldots, n\}$ setzen wir $W_{p^i} = W(\Phi_{p^i}(t))$. Offenbar wird dann W_{p^i} von den p^{n-i}-ten Potenzen der primitiven p^n-ten Einheitswurzeln erzeugt.
Die $\mathbf{Q}$-Teilräume W_{p^i} sind invariant unter der Galoisgruppe von $\mathbf{Q}_{p^n}$, und es gilt:

Satz 1

a) $\mathbf{Q}_{p^n} = W_p \oplus W_{p^2} \oplus \cdots \oplus W_{p^n}$,

b) $$\dim \Phi_{p^i}(t) = \begin{cases} \varphi(p) = p - 1 & \text{für } i = 1 \\ \varphi(p^i) - \varphi(p^{i-1}) = (p-1)^2 p^{i-2} & \text{für } i \geq 2. \end{cases}$$

Beweis: Es ist $\mathbf{Q}_{p^n} = W_p + W_{p^2} + \cdots + W_{p^n}$.

Wegen

$$\begin{aligned}\dim \mathbf{Q}_{p^n} &= \varphi(p^n)\\ &= (\varphi(p^n) - \varphi(p^{n-1})) + (\varphi(p^{n-1}) - \varphi(p^{n-2})) + \cdots + (\varphi(p^2) - \varphi(p)) + \varphi(p)\end{aligned}$$

genügt es also für alle $i \in \{2, 3, \ldots, n\}$ zu zeigen:

$$\dim W_{p^i} \leq \varphi(p^i) - \varphi(p^{i-1}).$$

Dabei können wir o.B.d.A. $i = n$ annehmen. Bekanntlich gilt:

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

Ist r eine primitive p^n-te Einheitswurzel, so folgt für alle j mit $1 \leq j \leq p^{n-1}$, die nicht durch p teilbar sind,

$$r^{j+p^{n-1}(p-1)} + r^{j+p^{n-1}(p-2)} + \cdots + r^{j+p^{n-1}} + r^j = 0. \tag{1}$$

Dies sind $\varphi(p^{n-1})$ unabhängige lineare Gleichungen zwischen den $\varphi(p^n)$ verschiedenen primitiven p^n-ten Einheitswurzeln. Also ist $\dim W_{p^n} \leq \varphi(p^n) - \varphi(p^{n-1})$.

Aus dem Beweis ergibt sich noch

Folgerung 2. *Sei $n \geq 2$, $L = \{l \mid 1 \leq l \leq p^{n-1}, p \nmid l\}$ und U_j der von den $r^{j+p^{n-1}k}$ für $0 \leq k \leq p-1$ erzeugte $\mathbf{Q}$-Teilraum. Dann gilt*

a) $W_{p^n} = \bigoplus_{j \in L} U_j$,

b) für alle $j \in L$ ist $\dim U_j = p - 1$.

Aus Satz 1 und den Bemerkungen vorher folgt

Satz 3. *Die primitiven m-ten Einheitswurzeln sind genau dann linear unabhängig, falls m quadratfrei ist.*

Als Beispiel für eine weitere Anwendung von Satz 1 zeigen wir

Satz 4. *Ist r eine primitive p^n-te Einheitswurzel, so bilden die Konjugierten des Elementes*

$$s = r^{p^{n-1}} + r^{p^{n-2}} + \cdots + r^p + r$$

eine Normalbasis von $\mathbf{Q}_{p^n}$.

Beweis: Wir führen den Beweis durch Induktion nach n. Für $n = 1$ ist die Behauptung gerade der oben zitierte Satz von Gauss. Sei $n > 1$ und $u = r^{p^{n-1}} + r^{p^{n-2}} + \cdots + r^p$, also $s = u + r$.

Da r^p eine primitive p^{n-1}-te Einheitswurzel ist, können wir also mit Induktion annehmen, dass die Konjugierten von u eine Normalbasis von $\mathbf{Q}_{p^{n-1}}$ bilden. Für $i \in K = \{k \mid 1 \le k \le p^n, p \nmid k\}$ sei σ_i der durch $r \to r^i$ definierte Automorphismus von $\mathbf{Q}_{p^n}$. Wir setzen $u^{\sigma_i} = u^{(i)}$.
Sei nun

$$\sum_{i \in K} c_i s^{\sigma_i} = \sum_{i \in K} c_i (u^{(i)} + r^i) = \sum_{i \in K} c_i u^{(i)} + \sum_{i \in K} c_i r^i = 0$$

mit irgendwelchen $c_i \in \mathbf{Q}$. Wegen $\sum_{i \in K} c_i u^{(i)} \in W_p \oplus W_{p^2} \oplus \cdots \oplus W_{p^{n-1}}$ und $\sum_{i \in K} c_i r^i \in W_{p^n}$ ist also

$$\sum_{i \in K} c_i u^{(i)} = \sum_{i \in K} c_i r^i = 0 .$$

Für $i, j \in K$ ist $u^{(i)} = u^{(j)}$ genau dann, wenn $r^{pi} = r^{pj}$, also $p(i-j) \equiv 0 \bmod p^n$ oder $i \equiv j \bmod p^{n-1}$ ist. Wegen der linearen Unabhängigkeit der Konjugierten von u folgt

$$c_j + c_{j+p^{n-1}} + \cdots + c_{j+(p-1)p^{n-1}} = 0 \tag{2}$$

für alle $j \in L = \{l \mid 1 \le l \le p^{n-1}, p \nmid l\}$. Aus $\sum_{i \in K} c_i r^i = 0$ ergibt sich mit Folgerung 2

$$c_j = c_{j+p^{n-1}} = \cdots = c_{j+(p-1)p^{n-1}} \tag{3}$$

für alle $j \in L$. Aus (2) und (3) zusammen folgt nun $c_i = 0$ für alle $i \in K$. Also sind die Konjugierten von s linear unabhängig.

Der Satz 4 ist vielleicht aus historischen Gründen erwähnenswert. Man gewinnt daraus für alle Kreisteilungskörper und damit nach dem Satz von Kronecker und Weber für alle Abelschen Körper eine Normalbasis. Dies verallgemeinert eine Schlussweise von D. Hilbert, der im Zahlbericht ([2]; Satz 132) eine Normalbasis für Abelsche Körper m-ten Grades mit zu m teilerfremder Diskriminante nachweist.

Karsten Johnsen, Mathematisches Seminar, Christian Albrechts Universität, Kiel

LITERATURVERZEICHNIS

1 C. F. Gauss: Tagebuch (Notizenjournal). Veröffentlicht von F. Klein in der Festschrift zur Feier des hundertjährigen Bestehens der Königlichen Gesellschaft der Wissenschaften zu Göttingen (1901). Ges. Werke X/1, S. 483–574.
2 D. Hilbert: Die Theorie der algebraischen Zahlkörper. Jber. dt. Math.-Verein. *4*, 175–546 (1897).
3 K. Johnsen: Bemerkungen zu einer Tagebuchnotiz von Carl Friedrich Gauss. Hist. Math. *9*, 191–194 (1982).

 0013-6018/85/060057-03$1.50 + 0.20/0