Der kubische Reziprozitätssatz, Teil 2

Simon Cramer

Anmerkung: In diesem Kapitel sind p, q rationale Primelemente, wobei $p \equiv 1(3)$ und $q \equiv 2(3)$. Da wir in diesem Kapitel nur mit kubischen Charakteren arbeiten werden, setzen wir $\chi_\pi(\alpha) := (\alpha/\pi)_3$.

Proposition 9.3.4

(a) $\overline{\chi_\pi(\alpha)} = \chi_\pi(\alpha)^2 = \chi_\pi(\alpha^2)$

(b) $\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha})$

Beweis:
(a) $\chi_\pi(\alpha) \in \{1, \omega, \omega^2\}$. Jede dieser Zahlen ist quadriert identisch zum komplex Konjugierten. $\chi_\pi(\alpha)^2 = \chi_\pi(\alpha^2)$ nach Proposition 9.3.3. c).
(b) Nach 9.3.3. b) gilt:

$$\alpha^{(N\pi-1)/3} \equiv \chi_\pi(\alpha)(\pi)$$

Durch komplexe Konjugation folgt:

$$\overline{\alpha}^{(N\pi-1)/3} \equiv \overline{\chi_\pi(\alpha)}(\overline{\pi})$$

Nun ist $N\pi = N\overline{\pi}$ und daher $\overline{\alpha}^{(N\pi-1)/3} = \overline{\alpha}^{(N\overline{\pi}-1)/3} \equiv \chi_{\overline{\pi}}(\overline{\alpha})(\overline{\pi})$.
Da nur Werte aus $\{1, \omega, \omega^2\}$ angenommen werden, folgt aus $\chi_{\overline{\pi}}(\overline{\alpha})(\overline{\pi}) \equiv \overline{\chi_\pi(\alpha)}(\overline{\pi})$ die Gleichheit.

□

Korollar: $\chi_q(\overline{\alpha}) = \chi_q(\alpha^2)$ und $\chi_q(n) = 1$, wenn $(n, q) = 1$.

Beweis:
(i) Da q rational prim, ist $q = \overline{q}$. Somit gilt $\chi_q(\overline{\alpha}) = \chi_{\overline{q}}(\overline{\alpha}) = \overline{\chi_q(\alpha)} = \chi_q(\alpha^2)$.
(ii) $n = \overline{n}$, somit gilt $\chi_q(n) = \chi_{\overline{q}}(\overline{n}) = \overline{\chi_q(n)} = \chi_q(n)^2$. Nun ist $\chi_q(n) \neq 0$, da $q \nmid n$ und daher $\chi_q(n) = 1$.

□

Wir haben also gezeigt, dass für $(n, q) = 1$, n kubischer Rest modulo (q) ist. Insbesondere gilt dann für $q_1, q_2 \equiv 2(3)$ mit $q_1 \neq q_2$, das $\chi_{q_1}(q_2) = \chi_{q_2}(q_1)$.

Wir wissen bereits, dass es zu jedem Primelement in D insgesamt 6 Assoziierte Elemente gibt. Wir wollen nun eine Definition bereitstellen, um eindeutig eines dieser Elemente auszuwählen.

Definition: Sei $\pi \in D$ prim. π heißt "primär", wenn $\pi \equiv 2(3)$. Für $\pi = a+b\omega$ bedeutet diese Notation, dass $a \equiv 2(3)$ und $b \equiv 0(3)$.

Proposition 9.3.5

Sei $\pi \in D$ mit $N\pi = p \equiv 1(3)$. Unter den Assoziierten von π ist genau ein Element primär.

Beweis:

Sei $\pi = a + b\omega$. Die Assoziierten $\pi, \omega\pi, \omega^2\pi, -\pi, -\omega\pi, -\omega^2\pi$ können in folgender Form geschrieben werden:

(a) $a + b\omega$
(b) $-b + (a - b)\omega$
(c) $(b - a) - a\omega$
(d) $-a - b\omega$
(e) $b + (b - a)\omega$
(f) $(a - b) + a\omega$

Es gilt $N\pi = p = a^2 - ab + b^2 \equiv 1(3)$, somit kann nicht $3 \mid a$ und $3 \mid b$ gleichzeitig gelten. Betrachen wir nun (a) und (b), so können wir annehmen, dass $3 \nmid a$ teilt. Wenn nämlich $3 \mid a$ gelten würde, würde direkt folgen, dass $3 \nmid b$ und somit könnten wir in (b) $a := -b$ definieren und alle anderen Koeffizienten entsprechend. Die Assoziierten sind schliesslich nur gedreht zueinander und daher ist es egal, bei welchem Element wir starten. Auf diese Weise können wir aus (a) und (d) folgern, dass $a \equiv 2(3)$. Aus $p = a^2 - ab + b^2$ folgt nun $1 \equiv 4 - 2b + b^2(3) \Leftrightarrow b(b - 2) \equiv 0(3)$. Im ersten Fall, $3 \mid b$, ist (a) primär. Im zweiten Fall, $b \equiv 2(3)$, ist (e) primär.

Die Existenz ist also gezeigt. Die Eindeutigkeit folgt sofort. Ohne Einschränkung sei (a) primär. (b) - (e) sind offensichtlich nicht primär, da der Realteil $\not\equiv 2(3)$ ist. Bei (f) ist der Imaginärteil $\not\equiv 0(3)$, somit ist (f) ebenfalls nicht primär und die Eindeutigkeit ist gezeigt.

□

Jetzt können wir den kubischen Reziprozitätssatz formulieren.

Theorem: "Der kubische Reziprozitätssatz"

Seien $\pi_1, \pi_2 \in D$ primär, $N\pi_1, N\pi_2 \neq 3$ und $N\pi_1 \neq N\pi_2$. Dann gilt:

$$\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1)$$

Anmerkungen:

(i) Wir müssen 3 Fälle betrachten: Beide Primelemente sind rational prim, ein Element rational, das andere komplex prim und den Fall, dass beide Elemente komplex prim sind. Der erste Fall ist trivial, nach dem vorangegangenen Korollar.

(ii) Der kubischer Charakter der Einheiten:
$\chi_\pi(1) = 1$ ist offensichtlich. $\chi_\pi(-1) = 1$, da $\forall\pi$ (-1) eine Lösung ist. Für $N\pi \neq 1$ folgt aus 9.3.3. (b), dass $\chi_\pi(\omega) = \omega^{(N\pi-1)/3)}$. Es folgt sofort die Gleichheit, da $\{1, \omega, \omega^2\}$ zyklische Gruppe der Ordnung 3 ist und somit

$$\omega^{(N\pi-1)/3} = \begin{cases} 1 & \text{für } N\pi \equiv 1(9) \\ \omega & \text{für } N\pi \equiv 4(9) \\ \omega^2 & \text{für } N\pi \equiv 7(9) \end{cases}.$$

(iii) $\pi \sim (1-\omega)$ ist ein Spezialfall.

Beweis

Sei $\pi \in D$ ein komplexes Primelement. Dann ist $N\pi = p \equiv 1(3)$. Da $D/\pi D$ endlicher Körper von Charakteristik p ist, enthält $D/\pi D$ eine Kopie von $\mathbb{Z}/p\mathbb{Z}$. Da beide Körper auch p Elemente besitzen, sind sie isomorph. Wir können also χ_π als kubischen Charakter auf $\mathbb{Z}/p\mathbb{Z}$ betrachten und daher mit Gauß Summen $g_a(\chi_\pi)$ und Jacobi Summen $J(\chi_\pi, \chi_\pi)$ arbeiten.

Wir haben bereits gezeigt, dass für kubische Charaktere χ folgendes gilt:
(i) $g(\chi)^3 = pJ(\chi, \chi)$
(ii) Wenn $J(\chi, \chi) = a + b\omega$, dann ist $a \equiv 2(3)$ und $b \equiv 0(3)$.

Da $J(\chi, \chi)\overline{J(\chi, \chi)} = p$, folgt aus (ii) sofort, dass $J(\chi, \chi)$ ein primäres Primelement in D ist.

Lemma 1: Sei π primär. Dann ist $J(\chi_\pi, \chi_\pi) = \pi$.

Beweis:

Sei $J(\chi_\pi, \chi_\pi) = \pi'$. Nun ist $\pi\overline{\pi} = p = \pi'\overline{\pi}'$, also muss $\pi \mid \pi'$ oder $\pi \mid \overline{\pi}'$ gelten (also $\pi' = \pi\gamma$ oder $\overline{\pi}' = \pi\gamma$ für eine Einheit γ). Nun sind allerdings $\pi, \pi', \overline{\pi}'$ allesamt primär. Somit können sie nicht zueinander assoziiert sein (9.3.5) und daher muss $\pi = \pi'$ oder $\pi = \overline{\pi}'$ gelten. Nach der Definition git:

$$J(\chi_\pi, \chi_\pi) = \sum_{x \in \mathbb{Z}_p} \chi_\pi(x)\chi_\pi(1-x) \equiv \sum_{x \in \mathbb{Z}_p} x^{(p-1)/3}(1-x)^{(p-1)/3}(\pi)$$

Die Summe läuft über ein Polynom der Form $x^{\frac{2}{3}(p-1)} + c_1 x^{\frac{2}{3}(p-1)-1} + ... + c_{p-1}x^{\frac{1}{3}(p-1)}$ wobei $c_1, ..., c_{p-1} \in \mathbb{Z}$. Da $(p-1) > \frac{2}{3}(p-1)$ gilt nach Kapitel 4, Übung 11, dass $\sum_{x \in \mathbb{Z}_p} x^{(p-1)/3}(1-x)^{(p-1)/3} \equiv 0(p)$. Es folgt sofort, dass auch $J(\chi_\pi, \chi_\pi) \equiv 0(\pi)$, da $p = \pi\overline{\pi}$. Somit gilt $\pi \mid \pi'$ und daher $\pi = \pi'$, was zu zeigen war.

□

Korollar: $g(\chi_\pi)^3 = p\pi$.

Beweis:
Folgt sofort aus Lemma 1 und der Feststellung (i) $g(\chi)^3 = pJ(\chi, \chi)$.

□

Nun zum kubischen Reziprozitätsgesetz. Zuerst betrachten wir den Fall $\pi_1 = q \equiv 2(3)$ und $\pi_2 = \pi$ mit $N\pi = p \equiv 1(3)$.

Wir erheben die Gleichung aus dem Korollar auf die $(q^2-1)/3$ -te Potenz und rechnen dann modulo q:

$$g(\chi_\pi)^{q^2-1} \equiv \chi_q(p\pi)(q)$$

Es ist $\chi_q(p) = 1$, also folgt:

$$g(\chi_\pi)^{q^2} \equiv \chi_q(\pi)g(\chi_\pi)(q) \tag{1}$$

Wir berechnen nun die linke Seite anhand der Definition der Gauß Summe:

$$g(\chi_\pi)^{q^2} = (\sum_{t \in \mathbb{Z}_p} \chi_\pi(t)\zeta^t)^{q^2} \equiv \sum_{t \in \mathbb{Z}_p} \chi_\pi(t)^{q^2}\zeta^{q^2 t}(q)$$

Die Gültigkeit der Kongruenz modulo q folgt nach 6.1.6. Nun ist $q^2 = 1(3)$ und da $\chi_\pi(t)$ in der zyklischen Gruppe $\{1, \omega, \omega^2\}$ liegt, haben wir:

$$g(\chi_\pi)^{q^2} \equiv g_{q^2}(\chi_\pi)(q)$$

Nach 8.2.1 ist $g_{q^2}(\chi_\pi) = \chi_\pi(q^{-2})g(\chi_\pi) = \chi_\pi(q)g(\chi_\pi)$. Also haben wir:

$$g(\chi_\pi)^{q^2} \equiv \chi_\pi(q)g(\chi_\pi)(q) \tag{2}$$

Wir setzen (1) und (2) gleich und haben:

$$\chi_q(\pi)g(\chi_\pi) \equiv \chi_\pi(q)g(\chi_\pi)(q)$$

Wir multiplizieren beide Seiten mit $\overline{g(\chi_\pi)}$. Es ist $g(\chi_\pi)\overline{g(\chi_\pi)} = p$, somit haben wir:

$$\begin{aligned} \chi_q(\pi)p &\equiv \chi_\pi(q)p \ (q) \\ \chi_q(\pi) &\equiv \chi_\pi(q) \ (q) \\ \Rightarrow \chi_q(\pi) &= \chi_\pi(q) \end{aligned}$$

Es bleibt nur noch der letzte Fall zu zeigen; π_1 und π_2 komplex prim mit $N\pi_1 = p_1 \equiv 1(3)$ und $N\pi_2 = p_2 \equiv 1(3)$.

Hier starten wir von der Gleichung $g(\chi_{\overline{\pi}_1})^3 = p_1\overline{\pi}_1$, erheben sie zur $(N\pi_2 - 1)/3$ -ten Potenz und rechnen modulo π_2.

$$\begin{aligned} g(\chi_{\overline{\pi}_1})^{N\pi_2-1} &\equiv \chi_{\pi_2}(p_1\overline{\pi}_1)(\pi_2) \\ g(\chi_{\overline{\pi}_1})^{p_2} &\equiv \chi_{\pi_2}(p_1\overline{\pi}_1)g(\chi_{\overline{\pi}_1})(\pi_2) \end{aligned} \tag{$*$}$$

Wir berechnen wieder die linke Seite anhand der Definition:

$$g(\chi_{\overline{\pi}_1})^{p_2} = (\sum_{t\in\mathbb{Z}_{p_1}} \chi_{\overline{\pi}_1}(t)\zeta^t)^{p_2} \equiv \sum_{t\in\mathbb{Z}_{p_1}} \chi_{\overline{\pi}_1}(t)^{p_2}\zeta^{p_2 t} \equiv g_{p_2}(\chi_{\overline{\pi}_1})(\pi_2)$$

Mit 8.2.1 folgt wieder:

$$g(\chi_{\overline{\pi}_1})^{p_2} \equiv \chi_{\overline{\pi}_1}(p_2^{-1})g(\chi_{\overline{\pi}_1}) \equiv \chi_{\overline{\pi}_1}(p_2^2)g(\chi_{\overline{\pi}_1})(\pi_2) \tag{$**$}$$

Wir setzen $(*)$ und $(**)$ gleich und erhalten nach Multiplikation mit $\overline{g(\chi_{\overline{\pi}_1})}$ und anschließendem Dividieren durch p_1:

$$\begin{aligned} &\chi_{\overline{\pi}_1}(p_2^2) \equiv \chi_{\pi_2}(p_1\overline{\pi}_1)(\pi_2) \\ \Rightarrow\ &\chi_{\overline{\pi}_1}(p_2^2) = \chi_{\pi_2}(p_1\overline{\pi}_1) \end{aligned} \tag{3}$$

Nun starten wir bei $g(\chi_{\pi_2})^3 = p_2\pi_2$, nehmen beide Seiten hoch $(p_1 - 1)/3$ und rechnen modulo π_1 und kommen analog zu:

$$\chi_{\pi_2}(p_1^2) = \chi_{\pi_1}(p_2\pi_2) \tag{4}$$

Nach 9.3.4. gilt außerdem: $\chi_{\overline{\pi}_1}(p_2^2) = \chi_{\overline{\pi}_1}(\overline{p_2^2}) = \overline{\chi_{\pi_1}(p_2^2)} = \chi_{\pi_1}(p_2^2)^2 = \chi_{\overline{\pi}_1}(p_2)$

Jetzt haben wir alles was wir brauchen. Wir berechnen:

$$\begin{aligned} \chi_{\pi_1}(\pi_2)\chi_{\pi_2}(p_1\overline{\pi}_1) &\overset{(3)}{=} \chi_{\pi_1}(\pi_2)\chi_{\overline{\pi}_1}(p_2^2) \overset{\text{Anm.}}{=} \chi_{\pi_1}(\pi_2)\chi_{\pi_1}(p_2) = \chi_{\pi_1}(\pi_2 p_2) \\ &\overset{(4)}{=} \chi_{\pi_2}(p_1^2) = \chi_{\pi_2}(p_1\pi_1\overline{\pi}_1) \\ &= \chi_{\pi_2}(\pi_1)\chi_{\pi_2}(p_1\overline{\pi}_1) \end{aligned}$$

Wir kürzen $\chi_{\pi_2}(p_1\overline{\pi}_1)$ und haben unser gewünschtes Resultat:

$$\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1)$$

.

Der kubischer Charakter der 2

Gesucht: $\pi \in D$, sodass $x^3 \equiv 2(\pi)$ lösbar ist.

Wir können ohne Einschränkung annehmen, dass π primär ist, da $x^3 \equiv 2(\pi)$ lösbar g.d.w. $x^3 \equiv 2(\pi')$ lösbar für $\pi' \sim \pi$.

1. Fall: $\pi = q$ rational prim $\Rightarrow \chi_q(2) = 1 \Rightarrow x^3 \equiv 2(q)$ lösbar $\forall q \equiv 2(3)$.
2. Fall: $\pi = a + b\omega$ mit $N\pi = p \equiv 1(3)$.

Proposition 9.6.1.

$x^3 \equiv 2(\pi)$ ist lösbar g.d.w. $\pi \equiv 1(2)$.

Beweis:

$$\pi = \pi^{(4-1)/3} = \pi^{(N2-1)/3} \equiv \chi_2(\pi)(2)$$

Nach kubischer Reziprozität gilt $\chi_2(\pi) = \chi_\pi(2)$ und damit $\pi \equiv 1(2)$ g.d.w. $\chi_\pi(2) = 1$.

□

Proposition 9.6.2.

Sei $p \equiv 1(3)$. $x^3 \equiv 2(p)$ ist lösbar g.d.w. $\exists C, D \in \mathbb{Z}$ sodass $p = C^2 + 27D^2$.

Beweis:

Nach 8.3.2. können wir $4p = A^2 + 27B^2$ schreiben, mit $A = 2a - b$ und $B = \frac{b}{3}$, wobei A und B eindeutig bis auf Vorzeichen sind.

"⇒" $x^3 \equiv 2(p)$ lösbar $\Rightarrow x^3 \equiv 2(\pi)$ lösbar $\Rightarrow \pi \equiv 1(2)$ nach 9.6.1.
$\Rightarrow b$ ist gerade $\Rightarrow A, B$ sind gerade. Setze also $C = A/2$, $D = B/2$ und es gilt $p = C^2 + 27D^2$.

"⇐" Ang. $p = C^2 + 27D^2$. Dann gilt $4p = (2C)^2 + 27(2D)^2$.
$\Rightarrow B = \pm 2D$, also B gerade und damit auch b gerade.
$\Rightarrow p = a^2 - ab + b^2 \equiv a^2(2) \Rightarrow a$ ungerade $\Rightarrow \pi = a + b\omega \equiv 1(2)$
$\Rightarrow x^3 \equiv 2(\pi)$ lösbar. Da $D/\pi D \cong \mathbb{Z}/p\mathbb{Z}$ ex. $h \in \mathbb{Z}$ sodass $h^3 \equiv 2(\pi)$
$\Rightarrow h^3 \equiv 2(p)$ und somit ist $x^3 \equiv 2(p)$ lösbar.

□

Beispiel:

$x^3 \equiv 2(7)$ hat keine Lösung, da 7 nicht in der Form $7 = C^2 + 27D^2$ geschrieben werden kann.

$x^3 \equiv 2(31)$ hingegen ist lösbar, da $31 = 2^2 + 27 \cdot 1^2$.