Kubische Reziprozität, Teil 1

Isabel Heinert

24. Mai 2017

1 Der Ring $\mathbb{Z}[\omega]$

Sei $\omega = -\frac{1}{2} + \frac{\sqrt{3}i}{2}$, die erste dritte Einheitswurzel.

Dann ist $\mathbb{Z}[\omega] := \{a + b\omega | a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.

In Kapitel 1 des Buches wird gezeigt, dass $\mathbb{Z}[\omega]$ zusammen mit der Addition und Multiplikation einen Euklidischen Ring bildet. Somit ist $\mathbb{Z}[\omega]$ auch ein Hauptideal- und faktorieller Ring, in dem jedes Element $\alpha \in \mathbb{Z}[\omega]$, $\alpha \neq 0$ eine (bis auf Einheiten und Reihenfolge) eindeutige Zerlegung in Primfaktoren besitzt. Außerdem wird die Abgeschlossenheit bezüglich der komplexen Konjugation nachgewiesen.

Bezeichnung $D := \mathbb{Z}[\omega]$.

Wir wollen D im Folgenden auf Einheiten und Primelemente untersuchen. Wichtig dafür ist der Begriff der Norm:

Definition Sei $\alpha = a + b\omega \in D$. Die *Norm* von α ist definiert als $\mathrm{N}\alpha = \alpha\overline{\alpha} = a^2 - ab + b^2 \in \mathbb{N}_0$.

Proposition 1.1 *(i)* $\alpha \in D$ *ist eine Einheit* $\Leftrightarrow N\alpha = 1$.
(ii) Die Einheiten in D sind: $1, -1, \omega, -\omega, \omega^2, -\omega^2$.

Beweis. Aussage (i).
"$\Rightarrow$" Sei α eine Einheit, also multiplikativ invertierbar in D $\Rightarrow \exists \beta \in D$ so, dass $\alpha\beta = 1$.
Es gilt $N\alpha\beta = 1\overline{1} = 1$, und mit der Assoziativität der Multiplikation in Ringen $N\alpha\beta = \alpha\beta\overline{\alpha\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = N\alpha N\beta$. D.h. $N\alpha N\beta = 1$, und damit $N\alpha = 1$.

"$\Leftarrow$" Sei $N\alpha = 1$. Also nach Definition der Norm $\alpha\overline{\alpha} = 1$. $\overset{\overline{\alpha} \in D}{\Rightarrow}$ α ist eine Einheit.

Aussage (ii). Mit der Äquivalenzaussage in Teil (i) lassen sich nun alle Einheiten in D berechnen. Sei $\alpha = a + b\omega \in D$ mit $N\alpha = a^2 - ab + b^2 = 1 \Leftrightarrow\ 4N\alpha = (2a - b)^2 + 3b^2 = 4$.

Mögliche Lösungen der Gleichung sind:
(1) $2a - b = \pm 1$ und $b = \pm 1$
(2) $2a - b = \pm 2$ und $b = 0$.

Die sechs Gleichungssysteme führen zu folgenden Wahlmöglichkeiten von a und b:

a	b	$\alpha = a + b\omega$
1	1	$1 + \omega = -\omega^2$
0	1	ω
0	-1	$-\omega$
-1	-1	$-1 - \omega = \omega^2$
1	0	1
-1	0	-1

So erhalten wir alle sechs Einheiten in D. □

Es gilt im Allgemeinen:

Definition p heißt *Primelement*, wenn aus $p|ab$ stets $\Rightarrow p|a \vee p|b$.

Untersucht man nun die Primelemente in D, ist es wichtig zu bemerken, dass Primelemente in $\mathbb{Z}$ nicht zwangsläufig Primelemente in D sind.

Beispiel $7 = (3+\omega)(2-\omega)$ ist offensichtlich nicht prim in D.

Die Begriffe müssen also unterschieden werden:

Bezeichnung (i) Ist p Primelement in $\mathbb{Z}$, dann heißt p *rationales Primelement*.
(ii) Ist π Primelement in D, dann heißt π einfach *Primelement*.

Proposition 1.2 *Sei $\pi \in D$.*
Ist $N\pi = p$, p ein rationales Primelement, dann ist π ein Primelement in D.

Beweis. Angenommen π ist nicht prim in D.
D.h. π ist nicht irreduzibel, und aufgrund von $N\pi = p \neq 1$ keine Einheit. Also kann man π als Produkt von Nichteinheiten $\neq 0$ schreiben: $\pi = \delta\gamma$, wobei $N\delta, N\gamma > 1,\ \delta, \gamma \in D$.
Dann ist $N\pi = p = N\delta N\gamma$. Ein Widerspruch zur rationalen Primeigenschaft von p.
$\Rightarrow \pi$ ist prim in D.

□

Die folgende Proposition klassifiziert alle Primelemente in D:

Proposition 1.3 *$\pi \in D$ ist prim $\Leftrightarrow N\pi = p$ und $p \equiv 1(3)$ oder $p = 3$,*
oder $N\pi = p^2$ und $p \equiv 2(3)$, wobei p rational prim ist.

Falls $N\pi = p$: $\pi \nsim$ rationales Primelement.
Falls $N\pi = p^2$: $\pi \sim p$ (π und p sind assoziiert).
Falls $p = 3$: $N\pi = 3 \Leftrightarrow \pi \sim 1 - \omega$.

Beweis. "$\Leftarrow$" *Fall $p \equiv 2$ (3)*:
Angenommen p ist nicht prim. Dann ist $p = \pi\gamma$ für $\pi,\ \gamma \in D$, mit $N\pi, N\gamma > 1$. Und die Norm $Np = p^2 = N\pi N\gamma \overset{N\gamma \neq 1}{\Rightarrow} N\pi = p$. π ist in der Form $\pi = a + b\omega$ für $a, b \in \mathbb{Z}$.
Also ist $N\pi = \underbrace{p = a^2 - ab + b^2}_{\Leftrightarrow\ 4p = (2a-b)^2 + 3b^2}$. D.h. $p \equiv (2a-b)^2$ (3) $\overset{3 \nmid p}{\Rightarrow}$ $p \equiv 1$ (3). Ein Widerspruch.
Wenn also $p \equiv 2$ (3) $\Rightarrow$ p ist prim in D.
Somit sind die $\pi \in D$ mit $\pi \sim p$ Primelemente in D, und es gilt $N\pi = Np = p^2$.

Fall $N\pi = p$ und $p \equiv 1$ (3) oder $p = 3$:
Da die Norm von π rational prim ist, folgt mit *Proposition* 1.2 die Behauptung.

"$\Rightarrow$" Sei π prim.
Also $N\pi \neq 1$. D.h. $N\pi = \pi\overline{\pi} = n$ für ein $n \in \mathbb{N} \setminus \{1\}$. Das n besitzt über $\mathbb{N}$ eine eindeutige Primfaktorzerlegung: $n = \prod_{i \in I} p_i^{l_i}$, wobei die p_i rational prim sind.
$\overset{\pi \text{prim}}{\Rightarrow}$ $\pi | p_i$ für ein $i \in$I $\overset{p := p_i}{\Leftrightarrow}$ $\pi\gamma = p$ für ein $\gamma \in D$.
Dann ist $N\pi N\gamma = p^2 \Rightarrow N\pi = N\gamma = p$ oder $N\pi = p^2 \wedge N\gamma = 1$.

Falls $N\pi = p^2$: dann $N\gamma = 1 \Rightarrow \gamma$ eine Einheit $\Rightarrow \pi \sim p$.
Falls $N\pi = p$: Angenommen $\pi = uq$, u eine Einheit, q rational prim.
Dann ist $p = N\pi = NuNq = q^2$. Ein Widerspruch $\Rightarrow \pi \nsim$ rat. Primelement.

($\triangle$) Haben also gezeigt:
$\pi \in D$ prim $\Rightarrow \exists$ rationales Primelement p so, dass $N\pi = p$, wobei $\pi \nsim$rat.Primelement, oder $N\pi = p^2$, wobei $\pi \sim p$.

Jetzt betrachten wir die verschiedenen Fälle, die für p *modulo* 3 auftreten können:

Fall $p \equiv 2\ (3)$:

Wie bereits gezeigt, gilt in diesem Fall: $\pi \in D$ mit $\pi \sim p$ sind prim in D $\overset{(\triangle)}{\Rightarrow}\ N\pi = p^2$.

Fall $p \equiv 1\ (3)$:

Betrachte das Legendre-Symbol

$$\Big(\frac{-3}{p}\Big) = \Big(\frac{-1}{p}\Big)\Big(\frac{3}{p}\Big) = (-1)^{\frac{p-1}{2}}\Big(\frac{3}{p}\Big) = (-1)^{\frac{p-1}{2}}\Big(\frac{p}{3}\Big)(-1)^{\frac{p-1}{2}}(-1)^{\frac{3-1}{2}} = \underbrace{(-1)^{p-1}}_{=1,\ da\ p\neq 2}(\frac{p}{3}) \overset{p\equiv 1\ (3)}{=} \Big(\frac{1}{3}\Big) = 1$$

da 1 quadratischer Rest *modulo* 3 ist.

D.h. $\exists\ a \in \mathbb{Z},\ s.d.\ a^2 \equiv -3\ (p)$. Also ist $p|a^2-(-3) = (a+\sqrt{3}i)(a-\sqrt{3}i) = (a+1+2\omega)(a-1-2\omega)$.

Angenommen p ist prim in D. Dann muss π sowohl den Real- als auch Imaginärteil einer der beiden Faktoren teilen. Da $p \nmid 2\ \Rightarrow\ p \nmid \pm 2\omega$. Ein Widerspruch.
$\Rightarrow$ p ist nicht prim in D.
Also $p = \pi\gamma$ für $\pi, \gamma \in D, N\pi,\ N\gamma > 1$. Dann $Np = p^2 = N\pi N\gamma \overset{N\gamma\neq 1}{\Rightarrow}\ N\pi = p$.

Fall $p \equiv 0\ (3)$, also $p = 3$:

Betrachte das Polynom $x^3 - 1 = (x-1)(x-\omega)(x-\omega^2)$.
Das impliziert $x^2 + x + 1 = (x-\omega)(x-\omega^2)$, wodurch wir mit $x = 1$ die Darstellung

$$3 = (1-\omega)(1-\omega^2) = (1+\omega)(1-\omega)^2 = -\omega^2(1-\omega)^2$$

erhalten − die bis auf Einheiten eindeutige Primfaktorzerlegung der 3 in D, denn:
Die Norm ist $9 = \underbrace{N(-\omega^2)}_{=1,\ \text{da Einheit}}\ N(1-\omega)^2 = N(1-\omega)N(1-\omega)\ \Rightarrow\ N(1-\omega) = 3$

$\overset{\text{Prop.1.2}}{\Rightarrow}\ 1-\omega$ ist prim in D mit $N(1-\omega) = p = 3$.

Außerdem gilt $\forall\ \pi$ mit $\pi \sim 1-\omega:\ N\pi = p = 3$, und somit: $N\pi = 3\ \Leftrightarrow\ \pi \sim 1-\omega$.

□

2 Restklassenringe

Die Betrachtung von Kongruenzen in D ist sehr nützlich. Dabei lassen sich die Kongruenzklassen von D modulo γ, wobei $\gamma \in D$ eine Nichteinheit, als Restklassenringe $D/\gamma D$ auffassen.

Bezeichnung $D_\gamma := D/\gamma D$.

Proposition 2.1 *Sei $\pi \in D$ prim. Dann ist D_π ein endlicher Körper mit $N\pi$ Elementen.*

Beweis. (1) zz: D_π ist ein Körper:
D ist ein Euklidischer Ring $\Rightarrow$ Hauptidealring, und da π Primelement in D ist, ist πD ein maximales Ideal in D. Damit ist $D/\pi D = D_\pi$ ein Körper.

(2) zz: D_π besitzt $N\pi$ Elemente:

Hier müssen die verschiedenen Fälle für π aus Proposition 1.3 einzeln betrachtet werden:

1.Fall: Sei $\pi = q \equiv 2(3)$, q rational prim.
Betrachte ein beliebiges $\mu = m + n\omega \in D$. m, n lassen sich in jeweils zwei eindeutige Summanden $m = qs + a$ und $n = qt + b$, wobei $a, b, s, t \in \mathbb{Z}$, $0 \leq a, b < q$, aufteilen.
Also ist $\mu \equiv a + b\omega\ (q)$ und die Menge $R := \{a + b\omega | 0 \leq a, b < q\}$ enthält somit Repräsentanten aller Restklassen in D_π.

Angenommen $a + b\omega \equiv a' + b'\omega\ (q)$, wobei $0 \leq a, a', b, b' < q, \in \mathbb{Z}$.
Damit ist $q|(a + b\omega) - (a' + b'\omega)$, also $\frac{a-a'}{q} \in \mathbb{Z}$ und $\frac{b-b'}{q} \in \mathbb{Z}$. Nach Voraussetzung ist $|a - a'| < q,\ |b - b'| < q \ \Rightarrow\ a = a', b = b'$. Die Restklassen verschiedener Repräsentanten in R sind also verschieden in D_π. Damit enthält R *genau einen* Repräsentanten jeder Restklasse in D_π, d.h. $|R| = |D_\pi|$. Mit $|R| = q^2 = Nq$, gilt $|D_\pi| = N\pi$.

2.Fall: Sei $\pi\overline{\pi} = p \equiv 1\ (3), p$ rational prim.
Betrachte wieder ein beliebiges $\mu = m + n\omega \in D$. Auch hier wollen wir Vielfache von π abspalten, um Repräsentanten der Restklassen in D_π zu erhalten.

π ist kein rationales Primelement, also in der Form $\pi = a + b\omega$ für $a, b \neq 0 \in \mathbb{Z}$.
Mit $N\pi = p = a^2 - ab + b^2 \ \Rightarrow\ p \nmid b$. (Andernfalls wäre $p|b \wedge p|a \ \Rightarrow\ p^2|(a^2 \wedge ab \wedge b^2) \ \Rightarrow\ p^2|p$. Ein Widerspruch.) Also ist b mod p invertierbar.
$\Rightarrow\ \exists c := nb^{-1}\ (p) \in \mathbb{Z}$ mit $cb \equiv n\ (p)$. Dann ist $\mu - c\pi = m + n\omega - c(a + b\omega) \equiv m + n\omega - ca - n\omega \equiv m - ca\ (p)$. Also $\mu - c\pi \equiv \mu\ (\pi) \equiv \underbrace{m - ca}_{=:l \in \mathbb{Z}}\ (\pi)$, da $\pi|p$.
Nun lässt sich $l \in \mathbb{Z}$ eindeutig aufteilen: $l = sp + r,\ \ s, r \in \mathbb{Z},\ 0 \leq r < p$.
Also $l \equiv r\ (p) \ \Rightarrow\ l \equiv r\ (\pi)$, da $\pi|p$. Somit gilt $\forall \mu \in D : \mu \equiv r\ (\pi), r \in \{0, 1, ..., p - 1\} =: R$.

Angenommen $r \equiv r'\ (\pi),\ r, r' \in R$. Also $r - r' = \pi\gamma$ für ein $\gamma \in D$. Betrachte die Norm: $(r - r')^2 = \underbrace{N\pi}_{p} N\gamma \Rightarrow p|r - r' \ \Rightarrow\ r = r'$, da $|r - r'| < p$.
Damit enthält R *genau einen* Repräsentanten jeder Restklasse von D_π, d.h. $|R| = |D_\pi|$. Mit $|R| = p$, gilt $|D_\pi| = N\pi$.

3.Fall: Sei $\pi \sim 1 - \omega$, $N\pi = 3$.
Sei $\mu = m + n\omega \in D$ beliebig. Es gilt $\mu + n\pi = m + n\omega + n(1 - \omega) = m + n \in \mathbb{Z}$. Da $\mu + n\pi \equiv \mu\ (\pi) \ \Rightarrow \mu \equiv \underbrace{m + n}_{=:d \in \mathbb{Z}}\ (\pi)$. Also gilt $\forall \mu \in D : \mu \equiv d\ (\pi)$ für ein $d \in \mathbb{Z}$.

Im Folgenden verläuft der Beweis analog zu *Fall* 2, als Spezialfall mit $p = 3$. Dies führt zur Repräsentantenmenge $R := \{0, 1, 2\}$, und damit $|D_\pi| = |R| = 3 = N\pi$.

□

3 Kubischer Rest-Charakter

Sei π ein Primelement in D.
Die Einheitengruppe von D_π hat die Ordnung $|D_\pi^*| = N\pi - 1$, da alle Restklassen $\neq [0]$ in D_π Einheiten sind.

Wir erhalten eine analoge Aussage zu Fermats Kleinem Satz:

Proposition 3.1 *Sei $\pi \nmid \alpha$, dann ist $\alpha^{N\pi-1} \equiv 1\ (\pi)$.*

Beweis. $[\alpha] \neq [0]$ in D_π, da $\pi \nmid \alpha \ \Rightarrow\ [\alpha] \in D_\pi^*$. Nach Lagrange teilen Elementordnungen die Gruppenordnung, also $[\alpha]^{N\pi-1} = [1]$. Mit $[\alpha]^{N\pi-1} = [\alpha^{N\pi-1}]$ folgt die Behauptung.

□

Lemma 1 *Sei $N\pi \neq 3$, also $\pi \nsim 1-\omega$. Die Restklassen von $1, \omega, \omega^2$ sind verschieden in D_π.*

Beweis. Angenommen:
1) $\omega \equiv 1\ (\pi)$. Dann $\pi | 1-\omega$. $1-\omega \in D$ ist prim $\Rightarrow \pi \sim 1-\omega$.
Also $N\pi = N(1-\omega) = 3$. Ein Widerspruch zur Voraussetzung und damit $\omega \not\equiv 1\ (\pi)$.
2) $\omega^2 \equiv 1\ (\pi)$. Dann $\pi | 1-\omega^2$. Da $N(1-\omega^2) = (1-\omega^2)(1-\omega) = 1-\omega-\omega^2 = 3$,
ist $1-\omega^2$ prim in D $\Rightarrow\ \pi \sim 1-\omega^2\ \Rightarrow\ N\pi = N(1-\omega^2) = 3$. Ein Widerspruch, also $\omega^2 \not\equiv 1\ (\pi)$.
3) $\omega \equiv \omega^2\ (\pi)$. Dann $\pi | \omega - \omega^2 = \omega(1-\omega)$. Da ω eine Einheit in D ist, ist $\pi \sim 1-\omega$
$\Rightarrow\ N\pi = N(1-\omega) = 3$. Ein Widerspruch, also $\omega \not\equiv \omega^2\ (\pi)$.

□

Lemma 2 *Sei $N\pi \neq 3$. Es gilt $3 \mid |D_\pi^*| = N\pi - 1$.*

Beweis. $\{1, \omega, \omega^2\} \subseteq D$ ist eine zyklische Gruppe von Ordnung 3. Also ist $ord(\omega) = ord(\omega^2) = 3$.
Da $[1], [\omega], [\omega^2] \in D_\pi^* \overset{Lagrange}{\Rightarrow} 3 | |D_\pi^*| = N\pi - 1$.

□

Proposition 3.2 *Sei $\pi \in D$ prim, $\pi \nmid \alpha$ und $N\pi \neq 3$.*
Es existiert ein eindeutiges $m \in \{0,1,2\}$, s.d. $\alpha^{\frac{N\pi-1}{3}} \equiv \omega^m\ (\pi)$.

Beweis. Nach *Proposition* 3.1 ist $\alpha^{N\pi-1} \equiv 1\ (\pi)$.
D.h. $\pi \mid \alpha^{N\pi-1} - 1$, wobei $\alpha^{N\pi-1} - 1 = \underbrace{(\alpha^{\frac{N\pi-1}{3}} - 1)}_{=:a1}\underbrace{(\alpha^{\frac{N\pi-1}{3}} - \omega)}_{=:a2}\underbrace{(\alpha^{\frac{N\pi-1}{3}} - \omega^2)}_{=:a3}$.
$\overset{\pi \text{prim}}{\Rightarrow}\ \pi | a_j$ für ein $j \in \{1,2,3\}$.

Aber π teilt auch höchstens eines der a_j:
Angenommen π teilt mehrere Faktoren. Dann teilt es auch die Differenz:

$$\left.\begin{array}{ll} 1)\ \pi \mid a_1 - a_2 = -1 + \omega = -1(1-\omega) \\ 2)\ \pi \mid a_1 - a_3 = -1 + \omega^2 = \omega^2(1-\omega) \\ 3)\ \pi \mid a_2 - a_3 = -\omega + \omega^2 = -\omega(1-\omega) \end{array}\right\} \Rightarrow\ \pi \sim 1-\omega \Rightarrow\ N\pi = 3, \text{ ein Widerspruch.}$$

$\Rightarrow\ \pi$ teilt *genau einen* der Faktoren a_j,
also $\underbrace{\pi \mid \alpha^{\frac{N\pi-1}{3}} - \omega^m}_{\Leftrightarrow\ \alpha^{\frac{N\pi-1}{3}} \equiv \omega^m\ (\pi)}$ für ein *eindeutiges* $m \in \{0,1,2\}$.

□

Auf Grundlage dieses Ergebnisses können wir den Kubischen Rest-Charakter definieren:

Definition Sei $N\pi \neq 3$.
Der *Kubische Rest − Charakter von α modulo π* ist definiert als

$$\left(\frac{\alpha}{\pi}\right)_3 \quad = \quad \begin{cases} 0 & falls\ \pi \mid \alpha \\ [\alpha^{\frac{N\pi-1}{3}}]\ in\ D_\pi & falls\ \ \pi \nmid \alpha \end{cases}$$

wobei nach *Proposition* 3.2 $\quad [\alpha^{\frac{N\pi-1}{3}}] \in \{[1], [\omega], [\omega^2]\} \ \subseteq D_\pi$.

Proposition 3.3 *a)* $\left(\frac{\alpha}{\pi}\right)_3 = [1] \ \Leftrightarrow \ x^3 \equiv \alpha\ (\pi)$.

b) $\alpha^{\frac{N\pi-1}{3}} \equiv \left(\frac{\alpha}{\pi}\right)_3\ (\pi)$.

c) $\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$.

d) wenn $\alpha \equiv \beta\ (\pi)$, *dann* $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$.

Beweis.
a) $\exists$ Isomorphismus $(D_\pi^*,\ \cdot) \overset{\varphi}{\cong} (\mathbb{Z}_{N\pi-1},\ +)$.
Also $[\alpha^{\frac{N\pi-1}{3}}] = [1]$ in $(D_\pi^*,\ \cdot) \overset{\varphi}{\Leftrightarrow} [\varphi(\alpha)(\frac{N\pi-1}{3})] = [0]$ in $(\mathbb{Z}_{N\pi-1},\ +)$.
$\Leftrightarrow\ 3 | \varphi(\alpha)$
$\Leftrightarrow\ \exists\, z:\ 3z = \varphi(\alpha)$
$\Leftrightarrow\ \exists\, x:\ x^3 \equiv \alpha\ (\pi)$.

b) Gilt nach Definition.

c) $\underbrace{\left(\frac{\alpha\beta}{\pi}\right)_3}_{\in\{[1],[\omega],[\omega^2]\}} \overset{(b)}{\equiv} \alpha\beta^{\frac{N\pi-1}{3}} \equiv \alpha^{\frac{N\pi-1}{3}} \beta^{\frac{N\pi-1}{3}} \overset{(b)}{\equiv} \underbrace{\left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3}_{\in\{[1],[\omega],[\omega^2]\}} (\pi)$.

$\overset{\text{Lemma1}}{\Rightarrow} \left(\frac{\alpha\beta}{\pi}\right)_3 \equiv \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3 (\pi) \ \Leftrightarrow \ \left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$.

d) $\underbrace{\left(\frac{\alpha}{\pi}\right)_3}_{\in\{[1],[\omega],[\omega^2]\}} \overset{(b)}{\equiv} \alpha^{\frac{N\pi-1}{3}} \overset{\alpha\equiv\beta\,(\pi)}{\equiv} \beta^{\frac{N\pi-1}{3}} \overset{(b)}{\equiv} \underbrace{\left(\frac{\beta}{\pi}\right)_3}_{\in\{[1],[\omega],[\omega^2]\}} \quad (\pi)$

$\overset{\text{Lemma1}}{\Rightarrow} \left(\frac{\alpha}{\pi}\right)_3 \equiv \left(\frac{\beta}{\pi}\right)_3 (\pi) \ \Leftrightarrow \ \left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$.

□