§ 20. Kreisteilungspolynome

Definition (20.1)

Sei $n \in \mathbb{N}$. Eine *n*-te Einheitswurzel in $\mathbb{C}$ ist ein Element $\zeta \in \mathbb{C}$ mit $\zeta^n = 1$. Mit μ_n bezeichnen wir die Menge aller n-ten Einheitswurzeln. Es handelt sich um eine Untergruppe von $\mathbb{C}^\times$.

Lemma (20.2)

Sei $k \in \mathbb{Z}$. Genau dann gilt $\mu_n = \langle \zeta_n^k \rangle$, wenn $\mathrm{ggT}(k, n) = 1$ ist.

Definition der Kreisteilungspolynome

Definition (20.3)

Sei $n \in \mathbb{N}$, $n \geq 2$.

- Eine primitive n-te Einheitswurzel ist ein Element $\zeta \in \mu_n$ mit $\mu_n = \langle \zeta \rangle$.
- Wir bezeichnen mit $\mu_n^\times \subseteq \mu_n$ die Menge der primitiven n-ten Einheitswurzeln.
- Das Polynom $\Phi_n \in \mathbb{C}[x]$ gegeben durch

$$\Phi_n \quad = \quad \prod_{\zeta \in \mu_n^\times} (x - \zeta)$$

wird das n-te Kreisteilungspolynom genannt.

Die Ganzzahligkeit der Kreisteilungspolynome

- Aus technischen Gründen setzen wir $\Phi_1 = x - 1$, obwohl wir für $n = 1$ keine primitiven n-ten Einheitswurzeln definiert haben.
- Für alle $n \in \mathbb{N}$ ist $\varphi(n) = \operatorname{grad} \Phi_n$.

Lemma (20.4)

Für alle $n \in \mathbb{N}$ gilt $x^n - 1 = \prod_{d|n} \Phi_d$, wobei d die natürlichen Teiler von n durchläuft.

Satz (20.5)

Es gilt $\Phi_n \in \mathbb{Z}[x]$ für alle $n \in \mathbb{N}$.

Beweis von Satz 20.5

z.zg: $\Phi_n \in \mathbb{Z}[x]$ für alle $n \in \mathbb{N}$

Zeige durch vollst. Ind. über $n \in \mathbb{N}$ zunächst $\Phi_n \in \mathbb{Q}[x]$

für alle $n \in \mathbb{N}$. Ind.-Anf. $n=1$ $\Phi_1 = x-1 \in \mathbb{Q}[x]$

Sei nun $n>1$, setze die Aussage für Werte $<n$ voraus.

Lemma 20.4 $\Rightarrow$ $x^n - 1 \overset{(*)}{=} \Phi_n \cdot g$, wobei $g = \prod_{\substack{d \mid n \\ d<n}} \Phi_d$

Ind.-V. $\Rightarrow \Phi_d \in \mathbb{Q}[x]$ für alle Teiler $d \in \mathbb{N}$ von n mit $d<n$

$\Rightarrow g \in \mathbb{Q}[x]$ $(*) \Rightarrow \Phi_n = \frac{x^n-1}{g}$ Division mit Rest

$\Rightarrow \exists\, q, r \in \mathbb{Q}[x]$ mit $x^n - 1 = q \cdot g + r$, wobei

$r = 0$ oder $\operatorname{grad}(r) < \operatorname{grad}(g)$ Annahme: $r \neq 0$

In $\mathbb{C}[x]$ gilt $\Phi_n \cdot g = x^n - 1 = qg + r \Rightarrow$

$r = g(\Phi_n - q) \Rightarrow \operatorname{grad}(r) \geq \operatorname{grad}(g)$ ↯ also: $r = 0$

$\Rightarrow \Phi_n g = qg \overset{\mathbb{Q}[x] \text{ Ind.-B.}}{\Rightarrow} \Phi_n = q \in \mathbb{Q}[x]$
kürzungsr.

Zeige nun die Ganzzahligkeit, ebenfalls durch vollst. Ind.

$n = 1 \quad \Phi_1 = x - 1 \in \mathbb{Z}[x]$

Ind.-schritt: Sei $n > 1$, setze $\Phi_d \in \mathbb{Z}[x]$ für $d < n$ voraus

$x^n - 1 \overset{(*)}{=} \Phi_n \cdot g$, wobei g wie oben definiert Ind.-V. $\Rightarrow g \in \mathbb{Z}[x]$

$(*) \Rightarrow g \in \mathbb{Z}[x]$ teilt $x^n - 1 \in \mathbb{Z}[x]$ im Polynomring $\mathbb{Q}[x]$

Satz 13.9 (i) $\Rightarrow$ g teilt $x^n - 1$ auch in $\mathbb{Z}[x] \Rightarrow \exists f \in \mathbb{Z}[x]$ mit

$x^n - 1 = f \cdot g \quad \Rightarrow \quad f \cdot g = x^n - 1 = \Phi_n \cdot g$

$\mathbb{Z}[x]$ ist Int.-B.

$\Longrightarrow$ Kürzungsregel $\quad \Phi_n = g \in \mathbb{Z}[x]$. $\square$

Die Irreduzibilität der Kreisteilungspolynome

Lemma (20.6)

Für jedes Polynom $f \in \mathbb{F}_p[x]$ gilt $f^p = f(x^p)$.

Satz (20.7)

Für jedes $n \in \mathbb{N}$ ist das Kreisteilungspolynom Φ_n in $\mathbb{Z}[x]$ und $\mathbb{Q}[x]$ irreduzibel.

Richtigstellung

An dieser Stelle muss ich eine Sache korrigieren, die ich in der Vorlesung erwähnt, aber falsch in Erinnerung hatte. Das Jahr 1916 war das Todesjahr von Richard Dedekind. Seinen Beweis der Irreduzibilität der Kreisteilungspolynome hat er viel früher formuliert, nämlich bereits im Jahr 1857.

Ein berühmter deutscher Mathematiker (unter anderem auch Zahlentheoretiker), der auch während des Ersten Weltkriegs in der Forschung aktiv war, war David Hilbert. Zum Beispiel wäre er 1915 beinahe Albert Einstein bei der Formulierung der Feldgleichungen seiner Allgemeinen Relativitätstheorie zuvorgekommen. Allerdings hat er, soviel ich weiß, keinen Kriegsdienst geleistet, wahrscheinlich auf Grund seiner Berühmtheit, vielleicht auch bereits auf Grund seines damaligen Alters.

Ich weiß noch, dass ich unter anderem als Student für ein Seminar einmal eine Arbeit eines Gruppentheoretikers gelesen habe, die mit „im Felde“ überschrieben war, also anscheinend an der Front geschrieben wurde. Aber an den genauen Titel und den Namen des Mathematikers erinnere ich mich nicht mehr.

Auf jeden Fall ist es bemerkenswert, unter welchen widrigsten Umständen Menschen teilweise in der Lage waren, die Forschung voranzubringen. Stephen Hawking ist wahrscheinlich zur Zeit das prominenteste Beispiel, aber es gibt viele weitere. Zum Beispiel stellte der französische Mathematiker André Weil ein wesentlichen Teil der Arbeit, die ihn berühmt machen sollte (die Schaffung neuer Grundlagen für die Algebraische Geometrie, die dadurch u.a. auch auf Grundkörper positiver Charakteristik angewendet werden konnte), während eines Gefängnisaufenthaltes zur Zeit des Zweiten Weltkriegs fertig, zu dem er wegen seiner Kriegsdienstverweigerung verurteilt worden war.

Beweis von Lemma 10.6:

geg. Primzahl p, $f \in \mathbb{F}_p[x]$ Beh.: $f(x^p) = f^p$

Erinnerung: In $\mathbb{F}_p$, und auch in jedem Ger. Ring R der Charakteristik p, gilt

$$(a+b)^p = a^p + b^p \quad \forall a, b \in R$$

("Freshman's Dream") Durch vollst. Ind. zeigt man leicht, dass $(a_1 + \dots + a_n)^p = a_1^p + \dots + a_n^p$ für alle $n \in \mathbb{N}$ und bel. $a_1, \dots, a_n \in R$ gilt.

Wende dies auf $R = \mathbb{F}_p[x]$ an. Schreibe

$$f = \sum_{k=0}^{n} a_k x^k \text{ mit } a_0, a_1, \dots, a_n \in \mathbb{F}_p$$

$$\Rightarrow f^p = \left(\sum_{k=0}^{n} a_k x^k\right)^p = \sum_{k=0}^{n} (a_k x^k)^p$$

$$= \sum_{k=0}^{n} a_k^p x^{kp} = \sum_{k=0}^{n} a_k (x^p)^k = f(x^p)$$

$\uparrow a^p = a \ \forall a \in \mathbb{F}_p$

□ □

Beweis von Satz 20.7

Beh.: Jedes Φ_n $(n \in \mathbb{N})$ ist irreduzibel in $\mathbb{Z}[x]$ und $\mathbb{Q}[x]$. (Nach Satz 13.9 (ii) reicht es z.zg., dass Φ_n in $\mathbb{Z}[x]$ reduzibel ist.)

Ang. Φ_n ist in $\mathbb{Z}[x]$ reduzibel $\Rightarrow \exists$ Nicht-Einheiten f, g in $\mathbb{Z}[x]$ mit $\Phi_n = f \cdot g$. Da Φ_n normiert ist, ist $f \in \mathbb{Z}$ oder $g \in \mathbb{Z}$ ausgeschlossen also: $\operatorname{grad}(f), \operatorname{grad}(g) \geq 1$. O.B.d.A. sei f irreduzibel.

Beh.: Ist $S \in \mu_n^\times$ mit $f(S) = 0$ und ist p eine Primzahl mit $p \nmid n$, dann gilt auch $f(S^p) = 0$.

Ang. $f(S^p) \neq 0$. $p \nmid n \Rightarrow S^p \in \mu_n^\times \Rightarrow$

$\Phi_n(\zeta^p) = 0 \Rightarrow f(\zeta^p)\, g(\zeta^p) \overset{f(\zeta^p)\neq 0}{\Rightarrow} g(\zeta^p) = 0$

$\Rightarrow \zeta$ ist eine Nullstelle des Polynoms $g(x^p)$

$f(\zeta) = 0$, f ist das Min-pol. von ζ über $\mathbb{Q} \Rightarrow$

$f \mid g(x^p)$ in $\mathbb{Q}[x] \overset{\text{Satz 13.9(1)}}{\underset{f, g(x^p) \in \mathbb{Z}[x]}{\Longrightarrow}} f \mid g(x^p)$ in $\mathbb{Z}[x]$

$\Rightarrow \exists\, h \in \mathbb{Z}[x]$ mit $g(x^p) = h \cdot f$

Seien $\bar{f}, \bar{g}, \bar{h}$ die Bilder von f, g, h in $\mathbb{F}_p[x]$

$\Rightarrow \bar{g}(x^p) = \bar{h} \cdot \bar{f} \overset{\text{Lemma 20.6}}{\Longrightarrow} \bar{g}^p = \bar{h}\, \bar{f}$ $(*_1)$

Sei $\bar{f}_1 \in \mathbb{F}_p[x]$ ein irred. Faktor von $\bar{f}$. Dann zeigt $(*_1)$, dass $\bar{f}_1$ ein Teiler von $\bar{g}^p$ ist. $\overset{\bar{f}_1 \text{ irred.}}{\Longrightarrow} \bar{f}_1 \mid \bar{g}$

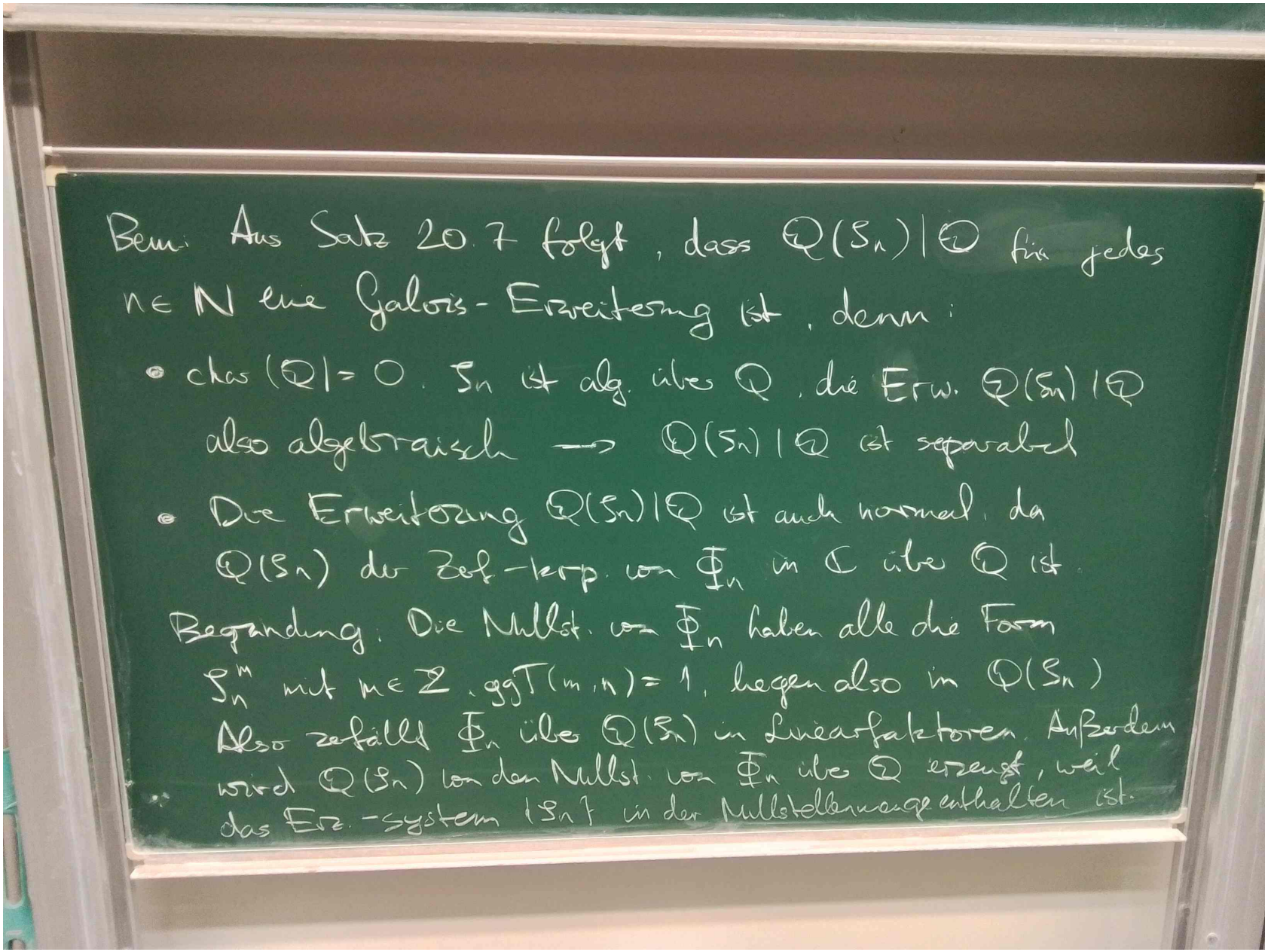
$\Phi_n = f \cdot g \Rightarrow \bar{\Phi}_n = \bar{f} \cdot \bar{g}$, wobei $\bar{\Phi}_n \in \mathbb{F}_p[x]$ das Bild von Φ_n

ist $\bar{f}_1 \mid \bar{f}$. $\bar{f}_1 \mid \bar{g} \Rightarrow \bar{f}_1^2 \mid \bar{\Phi}_n$ $\quad \bar{\Phi}_n \mid x^n - \bar{1} \Rightarrow \bar{f}_1^2 \mid (x^n - \bar{1})$

Jede Nullst. von $\bar{f}_1^2$ in einem alg. Abschluss $\mathbb{F}_p^{alg}$ von $\mathbb{F}_p$ ist somit eine mehrfache Nullst. von $x^n - \bar{1}$. Aber die Ableitung von $x^n - \bar{1}$ ist $n \cdot x^{n-1}$, und wegen $ggT(x^n - \bar{1}, n \cdot x^{n-1}) = \bar{1}$ hat $x^n - \bar{1}$ in $\mathbb{F}_p^{alg}$ keine mehrfachen Nullstellen. ↯ $\quad (\Rightarrow$ Beh.$)$

Jede primitive n-te Einheitswurzel hat die Form ζ^m für ein $m \in \mathbb{N}$ mit $ggT(m,n) = 1$. Die Zahl n hat eine Darstellung $n = p_1 \cdot \ldots \cdot p_r$, wobei p_j Primzahl mit $p_j \nmid n$ für $1 \le j \le r$. Mehrfache Anw. d. Beh. zeigt, dass $\zeta^{p_1}, \zeta^{p_1 p_2}, \ldots, \zeta^m$ alles Nullstellen von f sind $\Rightarrow$ Jede prim. n-te Einheitswurzel ist Nullstelle von f. $\Rightarrow \operatorname{grad}(f) = \varphi(n) = \operatorname{grad} \Phi_n \Rightarrow \operatorname{grad}(g) = 0$

$\Rightarrow g \in \mathbb{Z}$ ↯. $\square$



(Korrekturanmerkung nächste Seite)

Korrekturanmerkung

Dass die Kreisteilungserweiterungen $\mathbb{Q}(\zeta_n)|\mathbb{Q}$ galois'sch sind, hätte man auch bereits vor Satz 20.7 feststellen können. Die Irreduzibilität von Φ_n spielt bei dem Argument keine Rolle. Wichtig ist nur, dass die komplexen Nullstellen von Φ_n alles Potenzen von $\zeta_n = e^{2\pi i/n}$ sind.

Substanziell benötigt wird die Irreduzibilität beim Beweis des nächsten Satzes, genauer bei Teil (i) von Satz 20.8. Hier wird der Fortsetzungssatz für Galoisgruppen verwendet, der nur mit einem irreduziblen Polynom funktioniert.

Die Galoisgrupen der Kreisteilungskörper

Satz (20.8)

Sei $n \in \mathbb{N}$ mit $n \geq 2$ und $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q})$.

(i) Für jedes $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$ gibt es ein eindeutig bestimmtes Element $\sigma_a \in G$ definiert durch $\sigma_a(\zeta_n) = \zeta_n^a$.

(ii) Es gibt einen Gruppenisomorphismus $\phi_n : (\mathbb{Z}/n\mathbb{Z})^\times \to G$ mit $\phi_n(a + n\mathbb{Z}) = \sigma_a$ für alle $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$.

Beweis von Satz 20.8 Sei $n \in \mathbb{N}$, $n \geq 2$.

Sei $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q})$, wobei $\zeta_n = e^{2\pi i/n}$

zu (i) Sei $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,n) = 1$. Dann ist $\zeta_n^a \in \mu_n^*$, also eine Nullstelle von Φ_n. Φ_n ist irred. über $\mathbb{Q}$, ζ_n, ζ_n^a sind Nullstellen von Φ_n $\overset{\text{Fortsetzungs-}}{\underset{\text{satz für Galoisgr.}}{\Longrightarrow}}$ $\exists\, \sigma_a \in G$ mit $\sigma_a(\zeta_n) = \zeta_n^a$. Da $\mathbb{Q}(\zeta_n)$ über $\mathbb{Q}$ von ζ_n erzeugt wird, ist σ_a durch das Bild $\sigma_a(\zeta_n)$ eindeutig bestimmt.

zu (ii) Beh.: Es existiert ein Isom. $\phi_n : (\mathbb{Z}/n\mathbb{Z})^* \to G$ mit $\phi_n(a+n\mathbb{Z}) \overset{(*)}{=} \sigma_a$ für alle $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,n) = 1$.

Definiere $\phi_n(a+n\mathbb{Z})$ für $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,n) = 1$ und $\boxed{0 \leq a < n}$ durch $\phi_n(a+n\mathbb{Z}) = \sigma_a$.

zeige: Die Gleichung (*) gilt für alle $a \in \mathbb{Z}$ mit $ggT(a,n) = 1$.

Sei a eine solche Zahl. Division mit Rest
$\Rightarrow \exists\, q, r \in \mathbb{Z}$ mit $a = qn + r$ und $0 \leq r < n$.

$a \equiv r \bmod n$, $ggT(a,n) = 1 \Rightarrow ggT(r,n) = 1$

Nach Def. gilt $\phi_n(a + n\mathbb{Z}) = \phi_n(r + n\mathbb{Z}) = \sigma_r$

Zu zeigen also: $\sigma_r = \sigma_a$ genügt: $\sigma_r(\zeta_n) = \sigma_a(\zeta_n)$, also $\zeta_n^r = \zeta_n^a$. Tatsächlich gilt

$\zeta_n^a = \zeta_n^{qn+r} = (\zeta_n^n)^q \cdot \zeta_n^r = 1 \cdot \zeta_n^r = \zeta_n^r$

noch zu überprüfen: (1) ϕ_n ist injektiv

(2) ϕ_n ist surjektiv (3) ϕ_n ist Gruppenhom.

zu (1) Seien $a, b \in \mathbb{Z}$ mit $ggT(a,n) = ggT(b,n) = 1$ und $\phi_n(a+n\mathbb{Z}) = \phi_n(b+n\mathbb{Z})$

z.zg.: $a+n\mathbb{Z} = b+n\mathbb{Z}$

$\phi_n(a+n\mathbb{Z}) = \phi_n(b+n\mathbb{Z}) \Rightarrow \sigma_a = \sigma_b \Rightarrow$

$\sigma_a(\zeta_n) = \sigma_b(\zeta_n) \Rightarrow \zeta_n^a = \zeta_n^b \Rightarrow$

$\zeta_n^{b-a} = 1 \overset{\text{ord}(\zeta_n)=n \text{ in } \mathbb{C}^\times}{\Longrightarrow} n \mid (b-a) \Rightarrow a \equiv b \bmod n$

$\Rightarrow a+n\mathbb{Z} = b+n\mathbb{Z}$.

zu (2) Sei $\sigma \in G$ z.zg.: $\exists a \in \mathbb{Z}$ mit $ggT(a,n) = 1$ und $\phi_n(a+n\mathbb{Z}) = \sigma$ $\quad \Phi_n(\zeta_n) = 0$

„Nullst." $\Rightarrow$ „auf-Nullst." $\Phi_n(\sigma(\zeta_n)) = 0 \Rightarrow \sigma(\zeta_n) \in \mu_n^\times$

$\Rightarrow \exists a \in \mathbb{Z}$ mit $ggT(a,n) = 1$ und $\sigma(\zeta_n) = \zeta_n^a$

$\Rightarrow \sigma(\zeta_n) = \sigma_a(\zeta_n) \Rightarrow \sigma = \sigma_a$ (da jedes $\tau \in G$ durch $\tau(\zeta_n)$ evtl. bestimmt ist) $\Rightarrow$

$\sigma = \phi_n(a + n\mathbb{Z})$

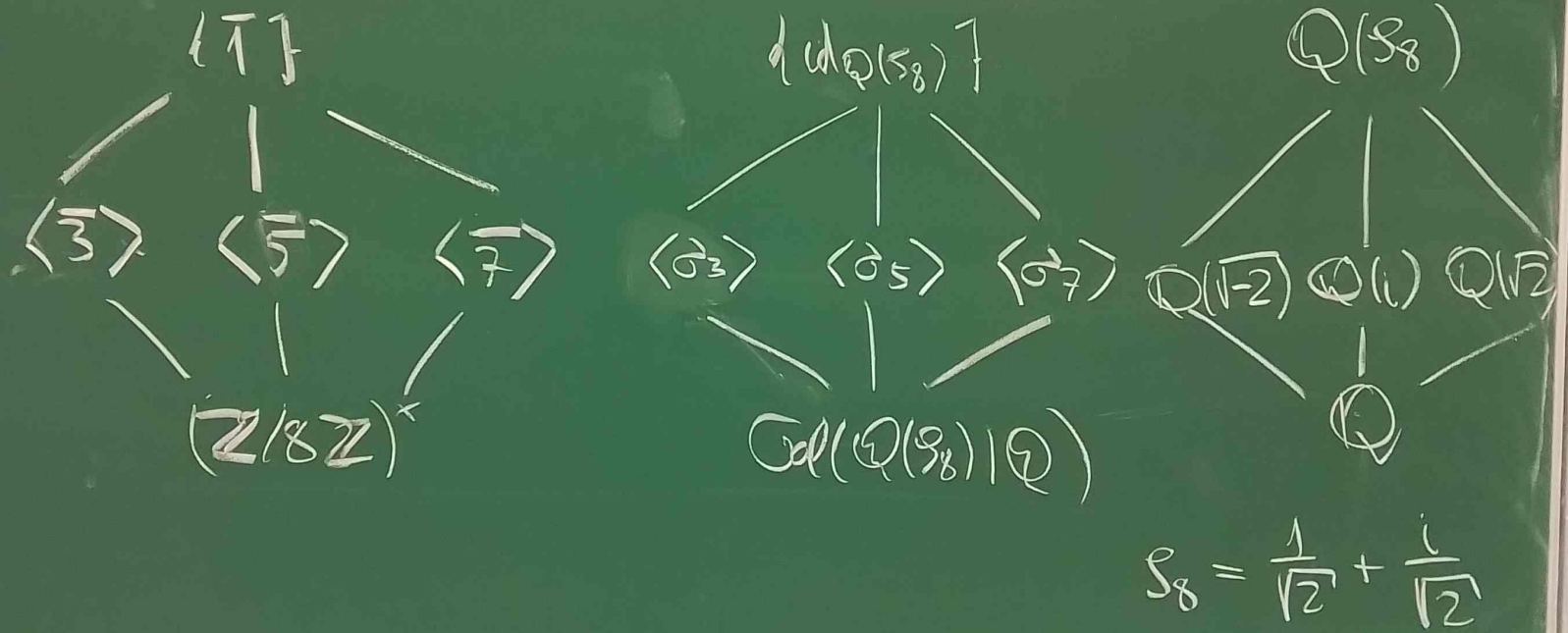
zu (3) Seien $a, b \in \mathbb{Z}$ mit $ggT(a,n) = ggT(b,n) = 1$ z.Zg.: $\phi_n((a+n\mathbb{Z})\cdot(b+n\mathbb{Z})) = \phi_n(a+n\mathbb{Z}) \circ \phi(b+n\mathbb{Z}) \Leftrightarrow \phi_n(ab+n\mathbb{Z}) = \sigma_a \circ \sigma_b \Leftarrow$

$\sigma_{ab} = \sigma_a \circ \sigma_b \Leftrightarrow \sigma_{ab}(\zeta_n) = (\sigma_a \circ \sigma_b)(\zeta_n)$

Tatsächlich gilt $(\sigma_a \circ \sigma_b)(\zeta_n) = \sigma_a(\zeta_n^b) = (\zeta_n^a)^b = \zeta_n^{ab} = \sigma_{ab}(\zeta^n)$ $\square$

Ausblick (Galoistheorie)

Untergr. von $(\mathbb{Z}/8\mathbb{Z})^\times$	Untergr. von $\mathrm{Gal}(\mathbb{Q}(\zeta_8)\mid\mathbb{Q})$	Teilkörper von $\mathbb{Q}(\zeta_8)$



$$\zeta_8 = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$$