4.8. $\varphi: G \to H,\ N = \ker\varphi$

$\hat{\varphi}: {}^{G}\!/_{N} \to H$ ist $aN \mapsto \varphi(a)$

$\hat{\varphi}$ ist wohldefiniert, injektiv und Homomorphismus

d.h. ${}^{G}\!/_{N} \underset{\text{Isomorphismus}}{\overset{\wedge}{=}} \operatorname{im}\varphi$ (Untergruppe von H)

$aN = \{b \in G \mid \varphi(b) = \varphi(a)\}$

$\underset{\varphi(a)}{aN} = \underset{\varphi(b)}{bN}$

$\hat{\varphi}((aN)(bN)) = \hat{\varphi}(abN) = \varphi(ab) = \varphi(a)\varphi(b) = \hat{\varphi}(aN)\hat{\varphi}(bN)$ ($\Rightarrow$ Homomorphiesatz)

$\rho_n : \mathbb{Z}(+) \to \mathbb{Z}_n$

$\rho_n(a+b) = \rho_n(a) +_n \rho_n(b)$

$\ker\rho_n = \langle n \rangle$

$\underbrace{\mathbb{Z}(+)/\langle n \rangle}_{a+\langle n\rangle} \cong \mathbb{Z}_n$

Nochmals: φ erklärt Äquivalenzrelation auf G

$a \sim_\varphi b \quad \Leftrightarrow \quad \varphi(a) = \varphi(b)$

${}^{G}\!/_{N}$ ist die Menge der Äquivalenzklassen

Allgemein: $\varphi: M \to N$ (Menge)

$a, b \in M: \quad a \sim_\varphi b \quad \Leftrightarrow \quad \varphi(a) = \varphi(b)$

${}^{M}\!/_{\sim_\varphi}$ ist die Menge der Äquivalenzklassen $[a]$

$\hat{\varphi}: {}^{M}\!/_{\sim_\varphi} \to N$ mit $[a] \mapsto \varphi(a)$ injektiv

$\varphi: R \to S$ (Ring-Homomorphismus)

- $\varphi: R(+) \to S(+)$ Gruppenhomomorphismus $(\varphi(a+b) = \varphi(a) + \varphi(b))$
- $\varphi(ab) = \varphi(a)\varphi(b)$
- $\varphi(1_R) = 1_S$

$\ker\varphi = \{a \in R \mid \varphi(a) = 0\}$

${}^{R(+)}\!/_{\ker\varphi} \cong \operatorname{im}(+)$

$\ker\varphi$ ist Ideal von R

Sei I Ideal von R (insbesondere I ist Untergruppe von $R(+)$)

$R/I := \{a+I : a\in R\}$ [Menge der Nebenklassen] $= \{a+i \mid i\in I\}$

$(a+I)+(b+I) \overset{\text{def.}}{=} (a+b)+I$

Definiere: $(a+N)(b+N) := ab+I \in R/I$

4.9. Satz

a) R/I ist bezüglich diesen Verknüpfungen ein Ring

b) Die Abbildung $\psi : R \mapsto R/S$ mit $a \mapsto a+I$ ist Ringhomomorphismus (surjektiv)

c) Sei $\varphi : R \to S$ Ringhomomorphismus

Definiere: $\hat{\varphi} : R/S \to S$ mit $a+I \mapsto \varphi(a)$

Dann ist $\hat{\varphi}$ wohldefiniert, surjektiv und Ringhomomorphismus

Beweis $(a+N)(b+N) := ab+I$ wohldefiniert:

$a+I = a'+I$

$b+I = b'+I$

$a' = a+i, \quad i\in I$

$b' = b+j, \quad j\in I$

$a'b' = (a+i)(b+i) = ab+\underbrace{aj+ib+ij}_{=x\in I}$ wegen Ideal

$a'b' = ab+x$

$a'b'+I = ab+\underbrace{x+I}_{\in I} = ab+I$

Welche Gruppen kennen wir?

$\mathbb{Z}(+)$, $\mathbb{Z}_n(+)$, $K(+)$, K^* (multiplikative Gruppe des Körpers K),...

S_n (symmetrische Gruppe)

R (Ring): $E(R) = \{a\in R \mid \exists b\in R \text{ mit } ab=1\}$ Einheitsgruppe

$E(\mathbb{Z}) = \{1,-1\}$ $E(K[X]) = \{\text{Menge aller Polynome vom grad} = 0\}'' = '' K^*$

$E(K) = K^*$

im $1,-1\in E(R)$

Zum Beispiel:

$E(\mathbb{Z}_8) = \{1,3,5,7\}$

$E(\mathbb{Z}_n)$

$E(K_N)$, $K_N = K_n[X]$, $n = \operatorname{grad} N$

4.10. Satz

Sei $A \in K_N \left(= K_n\left[X\right]\right)$

$A \in E\left(K_N\right) \quad \Leftrightarrow \quad \underbrace{\text{ggT}\left(A,N\right)}_{G} = 1$

Beweis:

Sei $\text{grad}\, G \geq 1$

$C := \frac{N}{G} \neq 0 \in K_N$

$AC = A \cdot \frac{N}{G} = \frac{A}{G} \cdot N$

$A \cdot_N C = 0$

Angenommen: $A \cdot_N B = 1$

$0 = \left(N \cdot_N C\right) \cdot_N B = C \cdot_N \left(A \cdot_N B\right) = C$

Sei $G = 1$ Satz von Bezout

$1 = PA + QN, \quad P, Q \in K\left[X\right]$

$1 = \rho_N\left(1\right) = \rho_N\left(PA + QN\right)$

$= \rho_N\left(PA\right) + \rho_N\left(QN\right)$

$= \rho_N\left(\rho_N\left(P\right)\underbrace{\rho_N\left(A\right)}_{=A}\right)$

$= \rho_N\left(P\right) \cdot_N A$

Korollar Sei N irreduzibel

$\Rightarrow \text{ggT}\left(A,N\right) = 1$

$\Rightarrow K_N$ ist Körper

Ziel:

Ist G eine endliche Untergruppe von K^*, so ist G zyklisch

Sei $G = \left\{a,b,c,d,...\right\}$ multiplikative Gruppe $\left(a,b \in G \;\Rightarrow ab \in G\right)$

$a \in G$ Potenzen von a

$a^0 := 1,\ a^1 := a,\ a^2 := a \cdot a,\ a^3 = a \cdot \left(a^2\right) \overset{!}{=} a \cdot \left(aa\right) = \left(aa\right) \cdot a = aaa$

$i \in \mathbb{N} \quad a^i := a\left(a^{i-1}\right) \overset{!}{=} \underbrace{a \cdot a \cdots a}_{i}$

$a^3\left(a^{-1}\right)^3 = \left(aaa\right)\left(a^{-1}a^{-1}a^{-1}\right) = \left(aa\right)\left(\underbrace{aa^{-1}}_{=1}\right)\left(a^{-1}a^{-1}\right) = aaa^{-1}a^{-1} = aa^{-1} = 1$

Allgemein:

$$\left(a^i\right)^{-1} = \left(a^{-1}\right)^i$$

Deswegen definiert man für $i \in \mathbb{N}$

$$a^{-i} := \left(a^{-1}\right)^i$$

a^i ist definiert für alle Zahlen $i \in \mathbb{Z}$

4.10. Potenzgesetze

Für alle $i, j \in \mathbb{Z}$

$$a^{i+j} = a^i a^j$$

$$\left(a^i\right)^j = a^{i \cdot j}$$

Bemerkung: Sei G additiv geschrieben

$$\left(a, b \in G \Rightarrow a + b \in G\right)$$

$$i \cdot a = \underbrace{a + a + \ldots + a}_{i} \qquad i \in \mathbb{N}$$

$$0_a := 0$$

$$(-i)\,a := -(ia)$$

„Potenzgesetze“

$$(i + j) = ia + ja \qquad \forall i, j \in \mathbb{Z}$$

$$i(ja) = (i \cdot j)\,a$$

Beispiele:

$G = \mathbb{Z}(+)$: $i \cdot a$ ist das Produkt der Zahlen $i, a \in \mathbb{Z}$

$G = \mathbb{Z}_n(+)$

Für $i \in \mathbb{Z}$ sei $\overline{i} := \rho_n(i)$ der Rest modulo n

z.B. $2a = a +_n a = \rho_n(a + a) = \rho_n(2a) = \overline{2} \cdot_n a$ $(= 0,$ wenn $n = 2)$

Allgemeiner

$$ia = a +_n a +_n a + \ldots +_n a = \rho_n(i \cdot a) = \overline{i} \cdot_n a$$

G sei multiplikative $a \in G$

$$\langle a \rangle := \left\{a^i \mid i \in \mathbb{Z}\right\}$$

4.12. $\langle a \rangle$ ist Untergruppe von G

Definition: Gruppe G heißt zyklisch, wenn ein $a \in G$ existiert mit $G = \langle a \rangle$

A heißt **Erzeuger** von G

oder primitives Element, mit a ist auch a^{-1} Erzeuger

Zum Beispiel:

$G = \mathbb{Z}(+)$ ist zyklisch mit Erzeuger 1, oder –1 ($i \in \mathbb{Z}$, $i = i \cdot 1$)

$G = \mathbb{Z}_n(+)$ ist zyklisch $i \in \mathbb{Z}_n \quad i = \underbrace{1 +_n 1 +_n \ldots +_n 1}_{i}$

Die Erzeuger von z.B. $\mathbb{Z}_8$ sind die Zahlen $\{1,3,5,7\}$

die $\langle 3 \rangle = \{0,3,6,1,4,7,2,5\}$

Sei $G = \langle a \rangle$ zyklische Gruppe

$\varphi : \mathbb{Z} \to G$ mit $i \mapsto a^i$ ist Gruppen-Homomorphismus, surjektiv

$\ker \varphi = \{ i \in \mathbb{Z} \mid a^i = 1 \}$ Untergruppe von $\mathbb{Z}$

Es existiert ein $n \in \mathbb{N}_0$ mit $\ker \varphi = \langle n \rangle$

Homomorphiesatz:

$$\mathbb{Z}(+) \Big/ \langle n \rangle \cong G = \langle a \rangle$$

n=0 $\ker \varphi = 0$

$G \cong \mathbb{Z}(+)$

$n = 1 \quad \Rightarrow \quad G \cong \mathbb{Z}_n$