§4 Ringe

- Ring, komm. Ring mit Eins
- Unterring, Ringhomomorphismen
- Kerne von Ringhomomorphismen sind „Ideale" I

  I additive Untergruppe, $r \cdot i \in I$, $i \cdot r \in I$ für alle $i \in I$, $r \in R$

Falls I Ideal in Ring R, dann wird R/I zu einem Ring durch $(r+I)(s+I) := rs + I$

R/I = Menge der Nebenklassen $r + I$

Bsp: R kommutativer Ring, $r \in R$

Hauptideal $r \cdot R = \{ r \cdot s \mid s \in R \}$ ist Ideal

denn
$$\left[\begin{array}{c} rs_1 + rs_2 = r(s_1+s_2) \\ 0 = r \cdot 0 \\ -(r \cdot s) = r \cdot (-s) \\ (r \cdot s) \cdot \underset{\in R}{r'} = r' \cdot (r \cdot s) = r \cdot (s \cdot r') \end{array}\right]$$

Spezialfall 1: $R = \mathbb{Z}$, $m\mathbb{Z}$ Ideal

Spezialfall 2: $R = K[X]$, $P(x)$ Polynom in $K[x]$: $\underset{\text{Ideal}}{P(x) \cdot K[x]} = \{ P(x) \cdot Q(x) \mid Q \in K[x] \}$

Körper K, z.B. $K = \mathbb{R}$

z.B. $\mathbb{C} \cong \underbrace{\overset{\overset{X}{\cup}}{\mathbb{R}[X]} / \underbrace{(X^2+1)\cdot\mathbb{R}[X]}_{I}}_{X + I}$

das konstante Polynom 1

$$(X+I)^2 + (1+I) = \underbrace{(X^2+1)}_{\in I} + I = I = \text{die } 0 \text{ in } \mathbb{R}[X]/I$$

d.h. $(X+I)^2 = -1 + I$

$$(X+I)\cdot(X+I) = \underset{\overset{\shortparallel}{X^2}}{X\cdot X} + I$$

die Äqu.klasse vom Polynom X

die Äqu.klasse von X^2+1

$$(X^2+I) + (1+I) = (X^2+1) + I = 0 + I$$

die Äqu.klasse vom Polynom X^2

die Äqu.klasse vom Polynom 1

Definitionen: R komm. Ring mit Eins

- Wenn $a, b \in R$, dann heißt <u>a ein Teiler von b</u> bzw. <u>b ein Vielfaches von a</u>, falls es ein $c \in R$ gibt mit $a \cdot c = b$. Man schreibt $a \mid b$

  <u>Bem:</u> $a \mid b \iff b \in a \cdot R \iff b \cdot R \subseteq a \cdot R$

- Ein Element $e \in R$ heißt <u>Einheit</u>, falls e ein (multiplikatives) Inverses e^{-1} hat, d.h. falls $e \cdot e^{-1} = e^{-1} \cdot e = 1$ gilt.

  <u>Bsp:</u> $\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

  $\bar{1} \cdot \bar{1} = \bar{1}$, $\bar{5} \cdot \bar{5} = \overline{25} = \bar{1}$ sind Einheiten

  $\bar{0}$, $\bar{2}$, $\bar{3}$ und $\bar{4}$ sind kein Einheiten

<u>Bem:</u> a) Einheiten von R sind genau die Teiler von 1

b) Nullteiler (d.h. Elemente, die 0 nicht-trivial teilen, a so, dass es ein $c \neq 0$ gibt mit $a \cdot c = 0$)

sind nie Einheiten

z.B. in $\mathbb{Z}/6\mathbb{Z}$: $\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$, also sind $\bar{2}, \bar{3}, \bar{4}$ Nullteiler

$\bar{4} \cdot \bar{3} = \overline{12} = \bar{0}$

Falls $a \cdot c = 0$, $a \neq 0$, $c \neq 0$ und a^{-1} existiert,

dann $c = 1 \cdot c = a^{-1} \cdot a \cdot c = a^{-1} \cdot 0 = 0$

Satz: R ist kommutativer endlicher (nicht-trivialer) Ring mit Eins.
Dann ist jedes $r \in R$ entweder Einheit oder Nullteiler.

Beweis: Betrachte die Abbildung $\mu_r : R \to R$, $x \mapsto r \cdot x$

1. Fall μ_r ist bijektiv, also surjektiv, also $1 \in \text{Bild}(\mu_r)$, d.h. es existiert $x \in R$ mit $r \cdot x = 1$, d.h. r Einheit

2. Fall μ_r ist nicht bijektiv, also nicht injektiv (R endlich!)
μ_r ist Gruppenhomomorphismus für die additive Gruppe von R (Distributivgesetz!)
d.h. $\text{Kern}(\mu_r) \neq \{0\}$ Wähle $0 \neq x \in \text{Kern}(\mu_r)$, d.h. $r \cdot x = 0$
also r Nullteiler. $\square$

Notation: Die Menge der Einheiten von R wird mit R^* bezeichnet.

Bem: $(R^*, \cdot, 1)$ ist Gruppe! Beachte: falls $e \in R^*$, so auch $e^{-1} \in R^*$, denn $(e^{-1})^{-1} = e$.

Def: Ein Körper ist ein kommutativer Ring mit 1, wo $R^* = R \setminus \{0\}$,
d.h. alle Elemente $\neq 0$ sind Einheiten.

§ 5 Die endlichen Ringe $\mathbb{Z}/m\mathbb{Z}$

Satz: $\mathbb{Z}/m\mathbb{Z}$ ist genau dann ein Körper, wenn m Primzahl ist.

Beweis: $\bar{r} \in \mathbb{Z}/m\mathbb{Z}$ ist genau dann invertierbar, wenn $\mu_{\bar{r}}: \bar{x} \mapsto \bar{r}\cdot\bar{x}$ invertierbar ist (Beweis zum letzten Satz)

1. Fall: m ist keine Primzahl, $m = p\cdot q$, p,q echte Teiler von m
(o.E. $m>0$, $1<p,q<m$)

$\bar{p}, \bar{q}$ sind dann Nullteiler und damit keine Einheiten

2. Fall: m ist Primzahl, $\operatorname{Kern}(\mu_{\bar{r}})$ ist Untergruppe von $\mathbb{Z}/m\mathbb{Z}$, also $= \begin{cases} \{0\} \\ \mathbb{Z}/m\mathbb{Z} \end{cases}$

Falls $\bar{r} \neq 0$, dann $\bar{r}\cdot\bar{1} = \bar{r} \in \operatorname{Bild}(\mu_{\bar{r}}) \neq \{0\}$

Homomorphiesatz $\operatorname{Bild}(\mu_{\bar{r}}) \cong (\mathbb{Z}/m\mathbb{Z}) \big/ \operatorname{Kern}(\mu_{\bar{r}}) \cong \begin{cases} \{0\} & \text{falls } \operatorname{Kern} = \mathbb{Z}/m\mathbb{Z} \\ \mathbb{Z}/m\mathbb{Z} & \text{falls } \operatorname{Kern} = \{0\} \end{cases}$

ausgeschlossen, da $\operatorname{Bild}(\mu_{\bar{r}}) \neq \{0\}$

Also $\operatorname{Kern}(\mu_{\bar{r}}) = \{0\}$, d.h. $\mu_{\bar{r}}$ ist bijektiv und $\bar{r}$ Einheit. $\boxtimes$

Falls man betonen möchte, dass es um einen Körper geht, schreibt man auch

$\mathbb{F}_m$ statt $\mathbb{Z}/m\mathbb{Z}$ (für Primzahlen m)

<u>Bem</u> (ohne Beweis)

Falls K endlicher Körper, dann $|K| = p^n$ p Primzahl,
und für jedes p^n gibt es (bis auf Isomorphie genau einen) Körper $\mathbb{F}_{p^n}$ mit p^n Elementen.

Falls $n > 1$, dann ist $\mathbb{F}_{p^n} \not\cong \mathbb{Z}/p^n\mathbb{Z}$

$\mathbb{Z}/4\mathbb{Z}$:

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
0	$\bar{0}$	$\bar{0}$	$\bar{0}$	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\mathbb{F}_4$

$\cdot$	0	1	a	b
0				
1				
a				
b				

<u>Notation</u>: $\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

$\bar{\ }: \mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$, $\bar{2} = \bar{8} = -\bar{4} = 2 + 6\mathbb{Z} = 8 + 6\mathbb{Z}$ etc

$= \{z \in \mathbb{Z} \mid z \equiv 2 \mod 6\}$

$= \{z \in \mathbb{Z} \mid z$ lässt Rest 2 bei Division durch 6$\}$

Was sind die Einheiten in $\mathbb{Z}/m\mathbb{Z}$?

Satz: $(\mathbb{Z}/m\mathbb{Z})^* = \{a + m\mathbb{Z} \mid a \in \mathbb{Z},\ ggT(a,m) = 1\}$

Bem: falls $a + m\mathbb{Z} = b + m\mathbb{Z}$, dann ist $ggT(a,m) = ggT(b,m)$

Sei $a \notin m\mathbb{Z}$

Beweis: Falls $ggT(a,m) = g \neq 1$. Dann $\underset{\substack{\uparrow \\ \mathbb{Z} \setminus m\mathbb{Z}}}{\bar{a}} \cdot \overline{\frac{m}{g}} = \overline{\underset{\substack{\uparrow \\ \mathbb{Z}}}{\frac{a}{g}}} \cdot \bar{m} = \bar{0}$, also $\bar{a}$ Nullteiler.

Falls $ggT(a,m) = 1$, dann existieren $x, y \in \mathbb{Z}$ mit $a \cdot x + m \cdot y = 1$

Also $\bar{a} \cdot \bar{x} + \underbrace{\bar{m} \cdot \bar{y}}_{= \bar{0}} = \bar{1}$, d.h. $\bar{a} \cdot \bar{x} = \bar{1}$, also $\bar{a}$ Einheit. $\boxed{\text{
}}$

$\bar{a}^{-1} = \bar{x}$

Bem: Falls $ggT(a,m) = 1$, so rechnet man $\bar{a}^{-1}$ in $\mathbb{Z}/m\mathbb{Z}$ über die ggT-Darstellung, die man aus dem Euklidischen Algorithmus erhält, aus.

(Das geht schnell für maschinelle Berechnung)

Def: $\varphi(m) :=$ die Anzahl der zu m teilerfremden positiven Zahlen $< m$

„Eulersche φ-Funktion"

$|(\mathbb{Z}/m\mathbb{Z})^*| = \varphi(m)$

Bsp $\varphi(6) = 2$, $\varphi(7) = 6$, allgemeiner: $\varphi(p) = p-1$ für Primzahl p.

(Bem falls m keine Primzahl, so ist $\varphi(m) < m-1$)

$\varphi(8) = 4$, $\varphi(9) = 6$, ..., $\varphi(12) = 4$

Erinnerung an den Satz von Lagrange: G endliche Gruppe

$g \in G$: $\operatorname{ord}(g) \mid |G|$ und $g^{|G|} = e$

„das kleinste positive Zahl k mit $g^k = e$"

Satz:

(a) Satz von Euler: $a^{\varphi(m)} + m\mathbb{Z} = 1 + m\mathbb{Z}$ für $\operatorname{ggT}(a,m) = 1$

$G = (\mathbb{Z}/m\mathbb{Z})^*$

$a^{\varphi(m)}$ lässt Rest 1 bei der Division durch m, $a^{\varphi(m)} \equiv 1 \mod m$

(b) kleiner Satz von Fermat: $a^{p-1} + p\mathbb{Z} = 1 + p\mathbb{Z}$ falls $p \nmid a$

$G = (\mathbb{Z}/p\mathbb{Z})^*$ p Primzahl

$a^{p-1} \equiv 1 \mod p$

a^{p-1} lässt Rest 1 bei der Division durch p