$\mathbb{Z}, \mathbb{Z}_2 \quad 2\mathbb{Z} \subset \mathbb{Z}$

deelring: zelfde bewerkingen

$\emptyset \neq S \subset R$ is deelring $\Leftrightarrow$ • $\forall a,b \in S: a-b \in S$
• $\forall a,b \in S: a \cdot b \in S$

Vbd $\mathbb{Z}[i]$ is deelring van $\mathbb{C}$

$\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$ (getallen van Gauss)

$a \in R$ heet nuldeler als $\exists b \in R$ zdd $a \cdot b = 0$ $\quad a \neq 0$, $b \neq 0$

Vbd in $\mathbb{Z}_{12}$: $3 \cdot 4 = 0$

Stelling: $\mathbb{Z}_n$ heeft geen nuldelers $\Leftrightarrow$ n is priem

Bewijs: $\Rightarrow$ Stel $n = p \cdot q$ dan in $\mathbb{Z}_n$: $p \cdot q = n = 0$

$\Leftarrow$ als n priem en $a \cdot b = 0$

dan $n \mid a \cdot b \overset{n \text{ priem}}{\Longrightarrow} n \mid a$ of $n \mid b$

$\Rightarrow a = 0$ of $b = 0$

Definitie: R $\underbrace{\text{commutatieve}}_{\text{m.b.t. } *}$ ring en $1 \in R$

R heet integriteitsgebied (integral domain) indien R geen nuldelers heeft.

$\mathbb{Z}_p, \mathbb{Z}, \mathbb{Z}[i], \mathbb{Q}, \mathbb{R}, \mathbb{C}$ itg

Def: Een lichaam is een itg. en elk element $\neq 0$ heeft inverse

Eigenschap: Als $\mathbb{F}$ lichaam dan heeft $\mathbb{F}$ geen nuldelers

$0 = a \cdot b \Rightarrow a^{-1} \cdot 0 \cdot b^{-1} = a^{-1} \cdot a \cdot b \cdot b^{-1} = 1 \cdot 1 = 1$
$a \neq 0, b \neq 0$

Als Groep een **1** heeft dan $1 \neq 0$ (eis)

$\mathbb{Z}_p$ lichaam: p priem
$p \nmid a$
$ggd(a, p) = 1$
$\Rightarrow \exists x, y$ zdd
$ax + py = 1$
$ax = 1 \mod p$

$\mathbb{Z}_3[i] = \{a + bi \mid a, b \in \mathbb{Z}_3\}$
lichaam? $(a+bi)(c+di) = 1$
$a, b \in \mathbb{Z}_3$ $c, d\, \mathbb{Z}_3$

St. R itg, $|R| < \infty$, dan R lichaam

Bewijs kies $r \in R$, $r \neq 0$, beschouw
$r, r^2, r^3, r^4, \dots, r^k, r^{k+1} \in R$ ~~oneindige rij~~
$r^i = r^j$ $i \neq j$ omdat R eindig
w.l.o.g. ~~stel~~ $i < j$

$$\Rightarrow R^i = R^i \cdot R^{j-i} \Rightarrow 0 = R^i - R^i \cdot R^{j-i} = \underbrace{R^i}_{\neq 0} \cdot \underbrace{(1-R^{j-i})}_{=0} = 0$$

want geen
nuldelers

$$R^{j-i} = 1 \begin{cases} j-i = 1 \Rightarrow R = 1 \\ j-i \geq 2 \Rightarrow R^{j-i} = R \cdot R^{j-i-1} = 1 \Rightarrow R^{-1} = R^{j-i-1} \end{cases}$$

Gevolg: $\mathbb{Z}_3[i]$ is lichaam (met 9 elementen)

$0 = (a+bi)(c+di)$

$$\Rightarrow \underbrace{(a^2+b^2)}_{\in \mathbb{Z}_3}\underbrace{(c^2+d^2)}_{\in \mathbb{Z}_3} = 0$$

$\Rightarrow \mathbb{Z}_3$ geen nuldelers dus

$a^2+b^2=0$ of $c^2+d^2=0$

$\Downarrow$

$a=0$ en $b=0$

in $\mathbb{Z}_3$

(a,b)	a^2+b^2
$(1,0)$	1
$(2,0)$	1
$(1,1)$	2
$(2,1)$	2
$(2,2)$	2

$\mathbb{Z}_5 = 1^2+2^2 = 0$

$\mathbb{Z}_p$ is lichaam, p priem

$\mathbb{Z}_3[i]$ " " , 9 elementen

$\mathbb{Z}_5[i]$ geen lichaam

$\mathbb{Z}_{17}[i]$ " "

<u>Vragen</u>

Hoeveel lichamen met p elementen? 1

Zijn er lichamen met 25 elementen? Ja, 1

" " " " 36 " ? Nee

" " " " p^2 " ? Ja 1

<u>St.</u> p priem $n \geq 1$ dan bestaat er lichaam met p^n elementen, uniek (op isomorfie na)

$\underbrace{\text{andere}}_{\text{eindige}}$ lichamen bestaan er niet

$\mathbb{Z}_3[i]$

$|a+bi| = 3$

$3a + 3bi = 0$

We zeggen $char(\mathbb{Z}_3[i]) = 3$

<u>Def:</u> R ring $char(R) = \min_{k \geq 1} \{ k \mid k \cdot r = 0 \ \forall r \in R \}$

Grootste gemeenschappelijke orde

Vbd $char(\mathbb{Z}) = 0$ (conventie)

$char(\mathbb{Z}_6) = 6$

Als $1 \in R$ dan $char(R) = |1| = k$

Bewijs kies $r \in R$

$$\underbrace{r+r+r+\dots+r}_{k\,x} = k \cdot r = k \cdot 1 \cdot r$$
$$= \underbrace{(1+1+1+1+\dots+1)}_{k\,x} \cdot r = 0 \cdot r = 0$$

Gevolg: als R itg, dan

$char(R) = 0$ of $char(R) = p$, priem

Bewijs ~~stel ...~~ stel $char(R) = n = k \cdot m$

n niet priem $\quad k \neq 1 \neq m$

$$0 = n \cdot 1 = \underbrace{(1+1+1+\dots+1)}_{n\,x} = \underbrace{(1+\dots+1)}_{k\,x}\underbrace{(1+\dots+1)}_{m\,x}$$

$\Rightarrow \underbrace{1+\dots+1}_{k\,x} = 0$ of $\underbrace{(1+\dots+1)}_{m\,x} = 0$ want itg, geen nuldelers

$k < n \lightning |1| = n \qquad m < n \lightning |1| = n$

R ring, $A \subset R$

A heet een ideaal indien:
- $(A,+)$ is groep
- $\forall a \in A, r \in R: ra \in A \quad (RA \subset A)$

Vbd in $\mathbb{Z}$ is $3\mathbb{Z}$ een ideaal

$a, b \in \mathbb{Z}$: $a \sim b \Leftrightarrow a - b \in A = 3\mathbb{Z}$

$\Rightarrow$ 3 equivalentieklassen: ~~A, A+1, A+2~~

$A,\ 1+A,\ 2+A$

optelling: $(a+A)+(b+A) = a+b+A$

vermenigvuldiging: $(a+A)(b+A) = a \cdot b + A$ | goed gedefinieerd

Stel $a_1 \sim a_2$ $\quad (a_1 - a_2 \in A,$

$b_1 \sim b_2$ $\quad b_1 - b_2 \in A)$

dan $a_1 \cdot b_1 \sim a_2 \cdot b_2$

$a_1 + b_1 \sim a_2 + b_2$