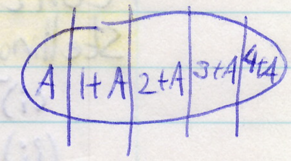
A&S
HC7

R ring

$A \subset R$ heet ideaal indien:
- A optelgroep
- $\forall r \in R, \forall a \in A: ra \in A$, $\quad RA \subset A$

op R: $r_1 \sim r_2 \iff r_1 - r_2 \in A$



V.b.d: $R = \mathbb{Z}$, $A = 5\mathbb{Z}$
$k_1 \sim k_2 \iff k_1 - k_2 \in 5\mathbb{Z}$ ofwel 5 deelt $k_1 - k_2$
Notatie: R/A verzameling van nevenklassen: $R/A = \{r + A \mid r \in R\}$
V.b.d: $\mathbb{Z}_5 = \mathbb{Z}/\langle 5 \rangle = \{k + \langle 5 \rangle / k \in \mathbb{Z}\}$. $\langle 5 \rangle$: ideaal voortgebracht door 5

R/A geven we de structuur van een ring:
$(r+A) + (s+A) = r+s+A$
$(r+A)\cdot(s+A) = rs + A$, onafhankelijk van representant:
stel: $r \sim t$, $s \sim u$ ($t \in r+A$, $u \in s+A$), dan $(t+A)(u+A) = tu + A$
$t = r + a_1$, $u = s + a_2$, $a_1, a_2 \in A$ $\quad \in A$, want optelgroep

$$u \cdot t = (s+a_2)(r+a_1) = rs + \underbrace{s \cdot a_2}_{\in A} + \underbrace{r \cdot a_1}_{\in A} + \underbrace{a_1 a_2}_{\in A}$$

$u \cdot t - r \cdot s = a \in A$
zo ook: $t + u \sim r + s$
rekenregels voor $+$ en $\cdot$ volgen uit die van R
Nulelement: $0 + A = A$, $-(r+A) = -r + A$
Als $1 \in R$ dan eenheidselement: $1 + A$
R/A factorring

V.b.d:
- $\mathbb{Z}/\langle 5 \rangle = \mathbb{Z}_5$
- $\mathbb{R}[x] = \{a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n \mid a_i \in \mathbb{R}, i = 0, \dots, n, n \geq 0, n \in \mathbb{Z}\}$
- $A = \langle x^2+1 \rangle = \{f(x)(x^2+1) \mid f(x) \in \mathbb{R}[x]\}$

in $\mathbb{R}[x]$ geldt dan dat $x^2 \sim -1$ (want $x^2 - (-1) \in A$)
b.v: $x^3 - 7x^2 - 6x + \sqrt{2}$ $\quad x^2 \sim x$
$\sim -x + 7 + 6x + \sqrt{2}$ $\quad x^4 \sim -x^2 \sim 1$
$= 5x + 7 + \sqrt{2}$. Conclusie 1: $f(x) \in \mathbb{R}[x]$, dan $f(x) \sim ax + b$, $a, b \in \mathbb{R}$
Conclusie 2: $ax + b \sim cx + d \Rightarrow (a-c)x + b - d \in A$
$\Rightarrow x^2 + 1$ deelt $(a-c)x + (b-d) \Rightarrow a = c$, $b = d$
$\mathbb{R}[x]/\langle x^2+1 \rangle = \{ax + b + \langle x^2+1 \rangle \mid a, b \in \mathbb{R}\}$

Optelling: $(ax+b)+A+(cx+d)+A=(a+c)x+(b+d)+A$

vermenigvuldiging: $(ax+b+A)(cx+d+A)=acx^2+(ad+bc)x+bd+A$

$=(ad+bc)x+(bd-ac)+A$

Conclusie: $\mathbb{R}[x]/\langle x^2+1\rangle=\mathbb{C}$, lichaam der complexe getallen

Stelling: R integriteitsgebied, A ideaal in R

(i) R/A is itg. $\Leftrightarrow$ A priemideaal

(ii) R/A is lichaam $\Leftrightarrow$ A maximaal ideaal

kennelijk is $\langle x^2+1\rangle$ een maximaal ideaal in $\mathbb{R}[x]$

" " $\langle 5\rangle$ " " $\mathbb{Z}$

" " ieder maximaal ideaal een priemideaal

$A\subset R$ heet priemideaal indien $\forall r,s\in R$ geldt $rs\in A$, dan $r\in A$ of $s\in A$

V.b.d: $\langle 5\rangle$ in $\mathbb{Z}$ is priemideaal. stel $rs\in\langle 5\rangle$ dan $5|rs\Leftrightarrow 5|r$ of $5|s$

$r\in\langle 5\rangle$ of $s\in\langle 5\rangle$

$\langle p\rangle$ is priemideaal in $\mathbb{Z}$, p priem

$\langle x^2+1\rangle$ is priemideaal in $\mathbb{R}[x]$: (x^2+1) deelt $f(x)g(x)\Rightarrow x^2+1$ deelt $f(x)$

ideaal

of x^2+1 deelt $g(x)$

A heet maximaal ideaal indien $A\subset B\subset R$, dan $B=A$ ofwel $B=R$

V.b.d: $\langle x^2+1\rangle$ in $\mathbb{R}[x]$

Opm: priemideaal $\neq$ maximaal ideaal. tegenvoorbeeld: $\langle x\rangle$ in $\mathbb{Z}[x]$

$=\{f(x)\in\mathbb{Z}[x]\mid f(0)=0\}$

$f(x)g(x)\in\langle x\rangle\Rightarrow f(0)g(0)=0\Rightarrow f(0)=0\Rightarrow f(x)\in\langle x\rangle$

of $g(0)=0\Rightarrow g(x)\in\langle x\rangle$

echter: $\langle x\rangle\subsetneq\langle x,2\rangle\subsetneq\mathbb{Z}[x]\Rightarrow\langle x\rangle$ niet maximaal

Bewijs:

(i) stel $rs\in A$, dan $(r+A)(s+A)=rs+A=A$ (nulelement in R/A)

$\Rightarrow r+A=A$ of $s+A=A\Rightarrow r\in A$ of $s\in A\Rightarrow A$ priem

stel A priem en stel $(r+A)(s+A)=A\Rightarrow rs\in A\Rightarrow r\in A$ of $s\in A$

$\Rightarrow r+A=A$ of $s+A=A$ $\Rightarrow R/A$ itg.

(ii) stel R/A is lichaam en stel $A\subset B\subset R$. Stel $b\in B$, $b\notin A\Rightarrow b+A$ heeft inverse

dus $\exists c\in R$ zdd $(b+A)(c+A)=1+A\Rightarrow \underset{\in B}{bc}=1+\underset{\in B}{a}$, $a\in A$ $\Rightarrow bc\in B$ en $(1+a)\in B$

$\Rightarrow 1\in B\Rightarrow r\cdot 1=r\in B$, $\forall r\in R\Rightarrow B=R\Rightarrow A$ max