A&S
HC8

$R$ ring, $1 \in R$, $A$ ideaal in $R$

**St:** (i) $R/A$ is itg $\Leftrightarrow$ $A$ priemideaal
(ii) $R/A$ is lichaam $\Leftrightarrow$ $A$ maximaal ideaal

**Bewijs:**
(ii) '$\Leftarrow$' stel $A$ maximaal, stel $r+A \neq A$, dus $r \notin A$
definieer $B = \{a + rx \mid x \in R, a \in A\} = \langle A, r \rangle$
dan $A \subset B \subset R$, $A$ is maximaal dus $A = B$ of $B = R$
maar $A \neq B$, dus $B = R \Rightarrow 1 \in B \Rightarrow \exists x \in R, \exists a \in A$ zdd: $1 = rx + a$
$\Rightarrow (r+A)^{-1} = x + A$
$(r+A)(x+A) = rx + A = 1 + A$ (want $1 - a = rx$), dus $R/A$ lichaam

**Gevolg:** (i) $\mathbb{R}[x]/\langle x^2+1 \rangle$ is lichaam, want $x^2+1$ is irreducibel
(ii) $\mathbb{Z}_2[x]/\langle x^3+x^2+1 \rangle$ is lichaam, want $x^3+x^2+1$ is irreducibel

**Def.:** $p(x) \in R[x]$ met $R$ een ring, $p(x)$ heet irreducibel indien:
$p(x) = f(x)g(x) \Rightarrow f(x)$ is constant of $g(x)$ is constant

(i) $x^2+1$ is irreducibel, want heeft geen wortels in $\mathbb{R}$ (geen nulpunt)
(ii) $x^3+x^2+1 = p(x)$, $p(0) = 1$, $p(1) = 1$ Gebruikt: een 2e of 3e graads polynoom is irreducibel $\Leftrightarrow$ geen nulpunten

**St:** $\mathbb{F}$ is lichaam en $p(x) \in \mathbb{F}[x]$, dan $p(x)$ irreducibel $\Leftrightarrow \langle p(x) \rangle$ maximaal
(ii) $\rightarrow$ in $\langle x^3+x^2+1 \rangle$ geldt $x^3 \sim x^2+1$, $x^4 \sim x^5+x \sim x^2+1+x$
$f(x) + \langle x^3+x^2+1 \rangle = f_0 + f_1x + f_2x^2 + \langle x^3+x^2+1 \rangle$, $f_0, f_1, f_2 \in \mathbb{Z}_2$
$\sim g_0 + g_1x + g_2x^2 + \langle x^3+x^2+1 \rangle$
dus $f(x) - g(x) \in \langle x^3+x^2+1 \rangle \Rightarrow f(x) = g(x)$ (want graad $\leq 2$)
dus $\mathbb{Z}_2[x]/\langle x^3+x^2+1 \rangle$ heeft 8 elementen (2 mogelijkheden voor $f_0$, $f_1$ en $f_2$)

**Bewijs:** stel $p(x)$ niet irreducibel
dan $p(x) = f(x)g(x)$ met gr. $f(x)$, gr. $g(x) <$ gr. $p(x)$
$\langle p(x) \rangle \underset{\neq}{\subset} \underset{\langle g(x) \rangle}{\langle f(x) \rangle} \underset{\neq}{\subset} \mathbb{F}[x]$ dus $\langle p(x) \rangle$ niet max

**stel:** $p(x)$ irreducibel en stel $\langle p(x) \rangle \underset{\neq}{\subset} A \underset{\neq}{\subset} \mathbb{F}[x]$
dan: $A = \langle g(x) \rangle$, $p(x) \in \langle g(x) \rangle$, $p(x) = f(x)g(x)$, met gr. $f(x) <$ gr. $p(x)$
$\Rightarrow p(x)$ reducibel $\lightning$

$\mathbb{F}[x]$ is PID

nl: $B$ ideaal in $\mathbb{F}[x]$, $B = \langle b(x) \rangle$ met gr. $b(x)$ minimaal en $b(x) \neq 0$

Bewijs: analoog aan $\mathbb{Z}$

Opm: $f(x) g(x) \in \mathbb{F}[x]$, $\mathbb{F}$ lichaam, dan $f(x) = q(x) \cdot g(x) + r(x)$
($g(x) \neq 0$ nulpolynoom) gr. $r(x) <$ gr. $g(x)$

Vbd: $g(x) = x^2 - 3$, $f(x) = 7x^3 + 2x^2 + 3x + 2$, bepaal $q(x)$, $r(x)$
$q(x) = 7x + 2$, $r(x) = (24x + 8)$

Vraag: $\mathbb{Z}_2[x] / \langle x^3 + x + 1 \rangle$ wat is de inverse van $(x + 1 + \langle x^3 + x + 1 \rangle)$?

$$(x + 1 + \langle x^3 + x + 1 \rangle)^{-1} = a(x) + \langle x^3 + x + 1 \rangle$$

met $a(x) \cdot (x + 1) = 1 + \langle x^3 + x + 1 \rangle$
$= 1 + b(x) \cdot (x^3 + x + 1)$

$a(x)(x+1) - b(x)(x^3 + x + 1) = 1$ (euclidisch algoritme)

Zij $A$ een ideaal in $\mathbb{Z}$ dan $A = \langle a \rangle$, $a \in \mathbb{Z}$, $a > 0$
met $a = \min\{x \mid x \in A, x > 0\}$
want: stel $x \in A$ dan $x = q \cdot a + r$, $0 \leq r < a$

$$\underbrace{\underset{\in A}{x} - \underbrace{q \cdot a}_{\in A}}_{\in A} = r$$

$r \in A$, dus $r = 0$

$A = \underbrace{\langle a \rangle}$ $\rightarrow$ hoofdideaal $\qquad$ $\mathbb{Z}$ hoofdideaalring / principle ideal ring: PID

$\langle 8, 12 \rangle = \{8 \cdot k + 12 \cdot l \mid k, l \in \mathbb{Z}\} = \langle 4 \rangle$

$\langle a, b \rangle = \langle \text{ggd}(a, b) \rangle \Rightarrow$ één voortbrenger