H5 Hoofdideaaldomeinen (PID) en ontbindingsringen (UFD)

Def als R domein dan heet $a \in R$ een irreducibel (irred) als $\forall b,c \in R \quad bc = a \Rightarrow b \in R^* \vee c \in R^*$

met andere woorden, a heeft alleen "flauwe ontbindingen" en dus flauwe delers.

Neem bijvoorbeeld de priemgetallen $\pm p \in \mathbb{Z}$
Deze hebben alleen flauwe delers $\{\pm 1\} = \mathbb{Z}^*$ met $\pm p$ zelf. We veralgemeniseren dit dus naar eenheden R^* als R een domein is

St $\overset{a \neq 0}{a \in R}$, $Ra \subset R$ priemideaal $\Rightarrow$ a irred.
(voor R een domein!)

Bew. stel Ra priem, dan stel $bc = a$. Omdat $bc \in Ra$ geldt $b \in Ra$ of $c \in Ra$. zvva: $c \in Ra$. Dan $c = da$ voor een $d \in R$ dus $bda = a \Rightarrow (1-bd)a = 0$
R domein dus $(1-bd)a = 0$, $a \neq 0 \Rightarrow 1 - bd = 0 \Rightarrow bd = 1$
$\Rightarrow b \in R^*$ dus $bc = a \Rightarrow b \in R^*$ of $c \in R^*$.
Dus a is irreducibel $\Diamond$

St (niet gerelateerd aan bovenstaande stelling!)
K lichaam en $f \in K[X]$ met $gr(f) = 2$ of $gr(f) = 3$ Dan is f irred. in $K[X]$ $\Leftrightarrow$ ~~desda~~
f heeft geen nulpunt in K

Bew "$\Rightarrow$" stel dat $f(\alpha) = 0$ voor $\alpha \in K$. Dan weten we $f \in Ker(ev_\alpha) = (X - \alpha)$ dus $f = p\,(X-\alpha)$
maar $gr(f) > 1 = gr(X-\alpha)$, dus $gr(p) = gr(f) - 1 > 0$
maar dan $p \notin K$ dus $p \notin K[X]^*$ dus f reducibel

Lemma R domein, $gr(fg) = gr(f) + gr(g)$
en $R[X]^* = R^*$

"$\Leftarrow$" stel f irreducibel. Dan is er een $p, q \in K[X]$ met $pq = f$. p, q zijn niet in $K[X]^* = K^*$ maar ook niet $p = 0$ of $q = 0$ want dan $f = 0$ (en f heeft graad 2 of 3 dus niet $= 0$) dus $gr(p), gr(q) \geq 1$ bovendien is $K[X]$ domein dus $gr(p) + gr(q) = 2$ of 3 dus één van p, q heeft graad 1, dus is van de vorm $p = a + bX$. $b \neq 0$ zvva is dit p :).
dan zien we $-ab^{-1} \in K$ want K lichaam dus $b \neq 0 \Rightarrow b^{-1}$ bestaat. En $ev_{-ab^{-1}}(f) =$
$q(a + b \cdot -ab^{-1}) \cdot ev_{-ab^{-1}}(q) = 0 \cdot ev_{-ab^{-1}}(q) = 0$
dus met $\alpha = -ab^{-1}$ hebben we een nulpunt $\alpha \in K$ $\blacksquare$

Spektakel!

Def een hoofdideaaldomein (PID, principle ideal domain) is een domein R waarin geldt dat elk ideaal $I \subset R$ van de vorm $I = Ra$ is voor een $a \in R$

Vbd alle lichamen zijn PID. immers $I \subset K$ ideaal $\Rightarrow$ $I \neq \emptyset$ en $(I \cap K^* = \emptyset)$ of $(I = K)$ en $K^* = K - \{0\}$ dus $I \cap K^* = \emptyset \Rightarrow I = \{0\}$ $\Rightarrow$ enige idealen van K zijn K en $\{0\}$ en $\{0\} = (0)$, $K = (1)$.

St 5.8 R PID. Dan TFAE voor $a \neq 0$

(i) Ra maximaal ideaal
(ii) Ra priemideaal
(iii) a irreducibel in R

Bew (i) $\Rightarrow$ (ii) : zie H4. (ii) $\Rightarrow$ (i) : St. 5.4
resteert (iii) $\Rightarrow$ (i). We zullen wel moeten gebruiken dat R PID is, want dit is nog niet gebruikt.

stel $a \neq 0$ en a is irreducibel, dus $bc = a \Rightarrow b \in R^*$ of $c \in R^*$ bekijk $(a) \subset R$. Omdat a geen eenheid is, is dit niet heel R. (want $(a) = R \Leftrightarrow 1 \in (a) \Leftrightarrow$ $\exists b \in R \; ba = 1 \Leftrightarrow a \in R^*$). $\Rightarrow$ (M1)

Stel nu dat er een ideaal $J \subset R$ is met $Ra \subsetneq J \subsetneq R$.
Omdat R (PID) is, $J = Rb$ voor een zekere $b \in R$ en $a \in Ra \subset Rb$ dus $a = rb$ voor een $r \in R$. maar $a = rb \Rightarrow r \in R^*$ of $b \in R^*$. Als $b \in R^*$ dan $Rb = R$.
Als $r \in R^*$ dan $b = r^{-1}a \in (a) \Rightarrow (b) \subset (a) \Rightarrow Rb = Ra$.
Dus voor $Ra \subset J \subset R$ volgt $Ra = J$ of $J = R$, (M2) $\square$

Gevolg Inh voor een PID geldt dat elk priemideaal $\neq \{0\}$ maximaal is.

Vbd $R = \{ a_0 + a_2X^2 + \cdots + a_nX^n \in K[X] \}$ polynomen over K die geen monoom a_1X hebben. lichaam.

Dit is een deelring van $K[X]$ en dus een ring.
We gaan laten zien dat de omkering " a irreducibel $\Rightarrow$ Ra priem " niet altijd geldt.
Daaruit mogen we concluderen dat R geen PID is

neem $X^2 \in R$. omdat $X^2 \notin K^*$ is X^2 geen eenheid in $K[X]$ dus ook niet in $R \subset K[X]$.
Stel $X^2 = fg$ voor $f, g \in R$. K is een domein dus $gr(f) + gr(g) = 2$ maar $gr(f) = 1$ bestaat niet, dan zit er n.l. een monoom in X in f. (evenzo voor g) $\Longrightarrow$ $gr(f) = 2$, $gr(g) = 0$. zvva
maar $g \neq 0$ want dan $X^2 = 0$ ↯. Dus $g \in K^* = K[X]^*$ en dus is er een $b \in K$ met $bg = 1$.
maar ook $b \in R$ want b is konst. polynoom dus heeft geen monoom van gr 1. dus $g \in K^*$ $\Rightarrow$ X^2 irreducibel.

toch is $RX^2 \subset R$ geen priemideaal. Immers $X^6 \in RX^2$ en $X^6 = X^3 \cdot X^3$. Maar $X^3 \notin X^2$ anders zit $X \in R$. Dus RX^2 is niet priem.

In feite zien we dat R geen PID is, immers (X^2, X^3) is geen hoofdideaal want $(a) = (X^2, X^3) \Rightarrow$
$ab = X^2 \quad ac = X^3 \quad \Rightarrow$ als a graad 0, dan $(a) = R \neq (X^2, X^3) \not\ni 1$
en als a graad 2 dan c graad 1 $\lightning$.

Er blijken te veel ringen geen PID's te zijn. Daarom bestaat er ook een zwakkere maar meer bruikbare eis: UFD.

Def een ontbindingsring (UFD, unique factorization domain) is een domein met de volgende eigenschappen:

elke $a \in R$ $a \neq 0$ kan worden geschreven als product van een eenheid $u \in R^*$ en irreducibele elementen $p_1, \ldots p_t$, $t \in \mathbb{Z}_{\geq 0}$

en deze is uniek op volgorde van de factoren én eenheden na, d.w.z. als

$$u \cdot p_1 p_2 \cdots p_t = v q_1 \cdots q_s \Longrightarrow$$

$t = s$ en er is een permutatie $\sigma \in S_t$ zdd $p_i = v_i q_{\sigma(i)}$ voor $v_i \in R^*$ $i = 1, \ldots s$

(kennelijk dan $u = v v_1 v_2 \cdots v_t$)

In een UFD geldt wel priemideaal $\Leftrightarrow$ irreducibel

St 5.12 $\quad R$ UFD $\quad a \in R \quad$ dan:

$$a \text{ irreducibel} \iff (a) \neq \{0\} \text{ is priemideaal}$$

Bew "$\Leftarrow$" : st. 5.4. Dit is waar voor élk domein!

"$\Rightarrow$" : als a irreducibel is en $bc \in (a)$

dan is bc dus te schrijven als $bc = ra$.

kies priemontbindingen voor b, c, d:

$b = u \cdot p_1 p_2 \cdots p_t \qquad c = u' p_1' p_2' \cdots p_s' \qquad d = v q_1 q_2 \cdots q_r$

$\Rightarrow \quad (uu') p_1 p_2 \cdots p_t p_1' p_2' \cdots p_s' = v q_1 q_2 \cdots q_r a$

dan geldt wegens de definitie van UFD $t + s = r^{+1}$ en

dat er een σ bestaat zodat één van de

p_i of p_i' op eenheid na gelijk is aan a. $\quad p_i = u_i a$ of $p_i' = u_i a$

$\Rightarrow \quad b = u p_1 \cdots u_i a \cdots p_t \quad$ of $\quad c = u p_1' \cdots u_i a \cdots p_s'$

$\Rightarrow \quad b \in (a) \quad$ of $\quad c \in (a)$ $\qquad \square$

Het is heel moeilijk om los te komen van het intuïtieve idee dat alles een eenduidige priemfactorisatie heeft zoals in $\mathbb{Z}$.

Daarom lijkt het soms overdreven dat deze st. bewezen moeten worden met zóveel aannames.

Vbd Om die reden nu een shockerend tegenvbd:

neem $\mathbb{Z}[\sqrt{-13}] \subset \mathbb{C}$

dan zien we dat $2, 7, 1 - \sqrt{-13}, 1 + \sqrt{-13}$

irred. zijn, want $N : a + b\sqrt{-13} \mapsto a^2 + 13b^2 \in \mathbb{Z}$

men kan aantonen $u \in \mathbb{Z}[\sqrt{-13}] \iff N(u) = 1 \iff u = \pm 1$

en als $N(\alpha) = p_1 p_2$ voor p_1, p_2 priem en p_i

niet te schrijven als $a^2 + 13b^2$, $p_1 p_2$ priem, dan is

α irreducibel, immers als $\alpha = \beta\gamma$ dan $N(\beta\gamma) = N(\beta) N(\gamma) = p_1 p_2$

$\Rightarrow \quad N(\beta) = p_1 p_2 \quad$ of $\quad N(\gamma) = p_1 p_2 \quad \Rightarrow$

en de normen zijn 4, 49, 14, 14 dus $p_1 p_2$ voor $p_1 = 2$ of 7

niet te schrijven als $a^2 + 13b^2$.

Maar $14 = 2 \cdot 7$, $14 = (1-\sqrt{-13})(1+\sqrt{-13})$
dit zijn dan twee "echt verschillende" priemontb. van 14.
dus $\mathbb{Z}[\sqrt{-13}]$ is geen UFD!

— Dat UFD een afzwakking is van PID, moet wel worden aangetoond:

St 5.13 Elke PID is een UFD

Bewijs gaat in twee delen: 1) er is een priemontb. $\forall a \in R-\{0\}$
2) deze is eenduidig

Stap 1

Opm Niet alleen uniciteit, maar ook existentie van een priemontbinding is in het algemeen niet te bewijzen! VB neem $R = \{p \in \mathbb{Q}[X] \mid p(0) \in \mathbb{Z}\}$
Dan heeft $X \in R$ niet eens een priemontb.
want elke $pq = X \Rightarrow p \in \mathbb{Z} - \{0\}$, $q = \frac{1}{p}X$
~~waaruit~~ voor $p \neq \pm 1$ dat deze ontb. niet-triviaal is, dus X is niet irred. Anderzijds is $\frac{1}{p}X \in R$ niet irred, want dit is $2 \cdot \frac{1}{2p}X$ bijvoorbeeld.
Zo kan men met een soort inductie aantonen dat X geen priemontb. heeft! $\boxtimes$

We moeten laten zien dat elke $a \in R-\{0\}$ een priemontb. in irred. elem. heeft. Dit doen we uit het ongerijmde. Stel a_1 heeft deze niet.

Bekijk het ideaal Ra_1. Dit is niet heel R, anders was $a_1 \in R^*$ en dan was er een ontbinding $a_1 = up_1 \cdots p_t$ $(t=0)$ $(u=a)$
Dus er is een maximaal ideaal $M \supset Ra_1$ (en $M \neq R$ (M1))

en R is PID $\Rightarrow$ $M = Rp_1$ voor een zekere $p_1 \in R$. En dus $a_1 \in Ra_1 \subset Rp_1 \Rightarrow a_1 = a_2 p_1$ voor een $a_2 \in R$

Wat geldt nu voor p_1? Rp_1 is maximaal, en voorgaande st: $\Leftrightarrow$ Rp_1 priem, $\Leftrightarrow$ p_1 irreducibel.

Dus $a_2 \notin R^*$, anders heeft $a_1 = a_2 p_1$ een priemontbinding. $\Rightarrow$ Ra_2 is niet heel de ring R.
en $a_1 \in Ra_2 \Rightarrow Ra_1 \subset Ra_2$ en omdat $p_1 \notin R^*$, $Ra_1 \neq Ra_2$
$\Rightarrow$ maak zo inductief een keten $Ra_1 \subsetneq Ra_2 \subsetneq \cdots$
met $Ra_n \subsetneq Ra_{n+1}$ voor $\forall n \in \mathbb{N}_{\geq 1}$

Bekijk de verz. $I = \bigcup_{n \in \mathbb{N}_1} Ra_n$. Dit is een ideaal, zie de bewijzen
van H4: $x, y \in I \Rightarrow x \in Ra_m, y \in Ra_n$, $Ra_n \supset Ra_m$ of $Ra_n \subset Ra_m$ dus $x - y \in Ra_M$, $M = \max\{n, m\}$.
evenzo $r \in R$, $x \in I \Rightarrow rx \in Ra_n \subset I$ $\Rightarrow$ I ideaal

Bovendien is R een PID $\Rightarrow$ $I = Rd$ voor een $d \in R$. Dan $d \in I = \bigcup_{n \in \mathbb{N}_1} Ra_n$
dus $\exists n \in \mathbb{N}_1$ $d \in Ra_n$, dan dus $(d) \subset (a_n)$

Maar dan $Ra_{n+1} \subset I = Rd \subset Ra_n \Rightarrow Ra_n = Ra_{n+1}$ $\lightning$

dus a heeft priemontbinding.

Opm in bijv $R = \{ p \in \mathbb{Q}[X] \mid p(0) \in \mathbb{Z} \}$
kunnen we ook zo'n keten $(Ra_n)_{n \in \mathbb{N}}$ maken:
we kunnen namelijk laten zien dat elke $p \in \mathbb{Z}$ priem irreducibel is in R, dus neem
$a_1 = X$ (die had geen priemontb, zie voorgaande Opm.)

en neem p_k = k-de ~~kleinste~~ priemgetal >0: $2, 3, 5, 7, 11$ etc.

definieer dan $a_{k+1} = \frac{"a_k"}{p_k}$ dus deel coëff van X in a_k door p_k:

$$a_1 = X \quad a_2 = \tfrac{1}{2}X \quad a_3 = \tfrac{1}{2\cdot 3}X \quad a_4 = \tfrac{1}{2\cdot 3\cdot 5}X$$

Wat zien we? $(X) \subsetneq (\tfrac{1}{2}X) \subsetneq (\tfrac{1}{6}X) \subsetneq (\tfrac{1}{30}X) \subsetneq$
want bijv. $\tfrac{1}{2}X \notin (X)$ immers $\tfrac{1}{2} \notin \mathbb{Z}$. Ha!

Merk echter op dat het bestaan van p_k irred. zdd $a_k = p_k a_{k+1}$ eigenlijk past volgt uit (PID).

en R is geen PID want PID $\Rightarrow$ UFD
en R is geen UFD (zie voorgaande opm.)

Stap 2 Elke $a \in R - \{0\}$ heeft priemontbinding.
Maar is deze ook uniek? (Ja, dat gaan we nu natuurlijk bewijzen!)

Schrijf $a = u p_1 p_2 \cdots p_s = v q_1 q_2 \cdots q_t$
Aan te tonen dat deze op een permutatie en eenheden na gelijk zijn. Dus $s = t$ en er is een $\sigma \in S_t$ ...

Met inductie naar s.

IB $s = 0$: dan $a = u \in R^*$ en $a = v \cdot q_1 q_2 \cdots q_t$
dus schrijf $R^* \ni av^{-1} = uv^{-1} = q_1 \cdots q_t$. Maar irreducibele elementen zijn geen eenheden, terwijl ab
$ab \in R^* \Rightarrow d(ab) = 1$ voor een $d \in R$ dus
$(da)b = 1$ voor een $da \in R \Rightarrow b \in R^*$ etc.
oftewel $abcd \cdots \ell \in R^* \Rightarrow$ alle in R^*,
dus dit kan alleen als $t = 0 \Rightarrow u = v$
dus zijn we klaar bij $s = 0$.

IH Stel voor een $s \in \mathbb{N}_0$, $\forall t \in \mathbb{N}_0$ geldt, als
$u p_1 \cdots p_s = v q_1 \cdots q_t \Rightarrow s = t$ en
op volgorde en eenheden gelijk $\overset{\text{dan}}{\Rightarrow}$ ...

p_i, q_j irred., $u, v \in R^*$

IS stel $a = up_1 \cdots p_{s+1} = v q_1 \ldots q_r$, $r \in \mathbb{N}_0$ willekeurig

dan geldt $a \in Rp_{s+1}$, dit is een priemideaal wegens st. 5.8.

Nu eerst: $t \neq 0$. Want als $t = 0$ dan $a = 1$, $1 \in Rp_{s+1}$ schendt (P1) want $Rp_{s+1} \neq R \Rightarrow t > 0$

Dan geldt dus dat een van de q_i $i \in \{1, .. t\} \neq \emptyset$ of v in Rp_{s+1} ligt want dat is (P2).

$\Rightarrow$ dit moet een q_i zijn want $v \in R^*$, $v \in Rp_{s+1}$ zou impliceren $Rp_{s+1} \cap R^* \neq \emptyset \Rightarrow Rp_{s+1} = R$ $\perp$

dus voor een zekere q_i rechts geldt $q_i \in Rp_{s+1}$. Maar q_i is irreducibel, dus $q_i = kp_{s+1} \Rightarrow k \in R^*$ per definitie.

Dus schrijf σ $up_1p_2 .. p_{s+1} = \underbrace{(vr)}_{\in R^*} q_1 \ldots q_{i-1} q_{i+1} \cdots q_r p_{s+1}$

$\Rightarrow (up_1 \cdots p_s - (vk)q_1 \cdots q_{i-1} q_{i+1} \cdots q_r) p_{s+1} = 0$

omdat $p_{s+1} \neq 0$ volgt $up_1 \cdots p_s = (vk) q_1 .. q_{i-1} q_{i+1} \cdots q_r$

$\Rightarrow$ pas IH toe, en vind ~~ees~~ $s = r-1$ dus $s+1 = r$

en $\exists \sigma \in \{f : [s] \to \{1 .. i-1, i+1, r\}\}$ $p_i = v_i \cdot q_{\sigma(i)}$ $\forall i = 1, \ldots s$

definiëren dan $J \in S_{s+1}$ met $J(j) = \sigma(j)$ voor $j = 1 \ldots s$

en $J(s+1) = i$, welgedefinieerd want i zat nog niet in beeld van σ. Dit is een permutatie

en $p_i = v_i' q_{\sigma(i)}$ $v_i' = v_i$ en $v_{s+1} = k$ ..

Dus $up_1 .. p_{s+1} = vq_1 .. q_r$ is uniek op volgorde van factoren en eenheden na $\boxtimes$

St 5.15 K lichaam, dan weten we (3.4, pas deling met rest toe voor $g \in I$ gr(g) minimaal.) dat elk ideaal I een hoofdideaal is, dus $K[X]$ is ontbindingsring. We kunnen bovendien elk irred. elem. monisch nemen door kopcoëffn met u^{-1} te verm..

Voor $f \in K[X]$, schrijf $f = u\, h_1^{n_1} \cdot h_2^{n_2} \cdots h_k^{n_k}$ $k \geq 1$ voor h_j monische irred. elem en $n_j \in \mathbb{Z}_{>0}$ aantal keer dat dit elem. voorkomt in priemontb. van f. (f niet const.)

Dan $K[X]/(f) \cong K[X]/(h_1^{n_1}) \times \cdots \times K[X]/(h_k^{n_k})$

Bew Met inductie naar $k \geq 1$

IB voor $k = 1$: $(f) = (u h_1^{n_1}) = (h_1^{n_1})$ dus $\cong$ is zelfs een gelijkheid $=$.

IS voor $k \geq 1$: schrijf $f = f_{k-1} h_k^{n_k}$ voor $f_{k-1} = u h_1^{n_1} \cdots h_{k-1}^{n_{k-1}}$. We willen aantonen dat $K[X]/(f) \cong K[X]/(f_{k-1}) \times K[X]/(h_k^{n_k})$

Dan zijn we klaar wegens IH. Het enige middel dat we kennen is de chinese reststelling, dus we zullen wel iets moeten doen als:

$I = (f_{k-1})$ $J = (h_k^{n_k})$ en dan bewijzen:

$I + J = R$, $I \cdot J = (f)$.

Het tweede is redelijk triviaal en waarschijnlijk al in algemene gevallen bewezen in H2:

"Voor R commutatief $(a_1, \ldots a_n) \cdot (b_1, \ldots b_m) = (a_1 b_1, a_1 b_2, \cdots, a_i b_j, \cdots a_n b_m)$"

Dit is een kwestie van definities uitschrijven.

Nu gaan we door naar $I + J = (f_{k-1}, h_k^{n_k}) \subset K[X]$
$K[X]$ is <u>PID</u> $\Rightarrow (f_{k-1}, h_k^{n_k}) = (g) \quad \exists g \in K[X]$

Stel dit is niet heel de ring, dwz $g \notin K[X]^* = K^* = K - \{0\}$

Dan is er een priemontb. $u q_1 \cdots q_t$ van g en $t > 0$ dus er is een irred monisch polynoom p dat g deelt en dus $(g) \subset (p)$

dan $f_{k-1} \subset (g) \subset (p) \qquad (h_k^{n_k}) \subset (g) \subset (p)$
Dus p deelt $h_k^{n_k} \Rightarrow p = h_k$ wegens eenduidigheid van priemontb. en het feit dat we p monisch kiezen.

(Def. kopcoeffiënt $= 1$)

maar dan wordt f_{k-1} gedeeld door h_k, in tegenspraak met de aanname $\Rightarrow g \in K[X]^*$
en dus I, J copriem $\Rightarrow$ chinese reststelling, dus

$$K[X]/(f) \cong K[X]/(f_{k-1}) \times K[X]/(h_k^{n_k})$$

$$\overset{IH}{\Longrightarrow} \quad K[X]/(f) \cong K[X]/(h_1^{n_1}) \times \cdots \times K[X]/(h_k^{n_k})$$

$\diamond$

VB neem $K = \mathbb{R}$ en $f = X^3 + X \in \mathbb{R}[X]$ dan
$f = X \cdot (X^2 + 1)$ in monische irreducibele factoren,
en $\mathbb{R}[X]/(X^3 + 1) \cong \mathbb{R}[X]/(X) \times \mathbb{R}[X]/(X^2 + 1)$
$\cong \mathbb{R} \times \mathbb{C}$

— We zien, als K lichaam dan $K[X]$ PID (H3) en dus een UFD.

— We gaan nu iets veel algemeners bewijzen:
R UFD $\Rightarrow R[X]$ UFD
Hiervoor ontwikkelen we eerst wat terminologie & 3 lemma's

5.18 We nemen voor kortheid steeds:
R is domein, en $K = Q(R)$, het quotiënten-lichaam.
We weten al dat $K[X]$ een ontb.-ring (UFD) is, dus we zullen steeds $f \in R[X] \subset K[X]$ steeds ontbinden in $K[X]$ en vervolgens proberen om met die ontb. er een in $R[X]$ te vinden.

5.19 R domein $a, b \in R$

Def we zeggen "b deler van a", notatie $b \mid a$ als

$$\exists c \in R \quad cb = a$$

Def we zeggen dat "b <u>echte</u> deler van a" als

$$b \notin R^*, \ a \neq 0 \ , \ \exists c \in R \ \ c \notin R^* \quad cb = a$$

Def $a, b \in R$ noemen we geassocieerd als $a = ub$, $\exists u \in R^*$.
notatie: $a \sim b$ (is equivalentie relatie)

$$\left[\begin{array}{ll} a = ub \Rightarrow & b = u^{-1}a \\ a = ub, \ b = vc \Rightarrow & a = \underset{\substack{\cap \\ R^*}}{(uv)}c \\ a = 1a & \end{array}\right]$$

Prop $a, b \in R$, R domein. Dan

(i) $a \in R^* \iff (a) = R$ niet nieuw..
(ii) $b \mid a \iff (a) \subset (b)$
(iii) b **echte** deler $a \iff (a) \subsetneq (b) \subsetneq R$
(iv) $a \sim b \iff (a) = (b) \iff a \mid b \ \ b \mid a$

Bew (i): zie H2. (ii) $a = cb \Rightarrow a \in (b) \Rightarrow (a) \subset (b)$
$(a) \subset (b) \Rightarrow a \in (a) \subset (b) \Rightarrow a = cb$
(iii) $b \notin R^* \underset{(i)}{\iff} (b) \neq R$ en $b \mid a \underset{(ii)}{\iff} a \subset b$

bovendien als $(a) = (b)$ dan $b \in (a)$
dus $a = cb \quad b = da \Rightarrow a = cda \Rightarrow cd = 1$ (domein) want $(1-cd)a = 0$
$\Rightarrow c \in R^*$ contradictie met $a = cb, c \notin R^*$
en als $(a) \subsetneq (b) \subsetneq R$ neem dan $c \in (b), c \notin a$, dan $a = dcb$
als $dc \in R^*$ dan $c \in R^*$ dus $(b) = R$ ↯

(iv) $a = ub \ \exists u \in R^* \Rightarrow x \in (a) \ x = ca$ voor een $c \in R$
maar dan ook $x = (cu)b \Rightarrow (a) \subset (b)$ en
evenzo wegens $b = u^{-1}a$ volgt $(b) \subset (a) \Rightarrow (b) = (a)$
en $(b) = (a) \Rightarrow b \in (a)$ dus $a|b$ en $a \in (b)$ dus
$b|a$ dus $a|b \wedge b|a$
en $a|b \wedge b|a \Rightarrow a = cb, b = da \Rightarrow a = cda \Rightarrow$
$cd = 1$ (domein) $\Rightarrow c \in R^*$ dus $a \sim b$

$\boxtimes$

Opm (i) en (ii) zijn iha waar in will. commutatieve ringen.
(iii) en (iv) alleen in domeinen (we hebben dat immers gebruikt in $(1-cd)a = 0$) en niet in ringen met nuldelers.

Herh:

Ra is priemideaal $\Leftrightarrow$ a is geen eenheid en $a|bc$ dan $a|b \vee a|c$

a is irreducibel $\Leftrightarrow$ a is geen eenheid en heeft geen echte delers.

In een UFD (waarvan PID speciaal geval bleek) zijn deze twee definities equivalent, zoals we bijvoorbeeld van $\mathbb{Z}$ gewend zijn.

In $\mathbb{Z}$ representeren we alle priemgetallen $\pm p$ vaak met de positieve priemgetallen p.
In een UFD R kunnen we Iha ook voor elke equivalentieklasse $R/\sim$

of R^*

(die ongelijk aan $\{0\}$ is)
een representant p kiezen, die
dus op eenheden na alle irreducibele
elementen representeerd waarmee hij geassocieerd
b. in $\mathbb{Z}$ blijken die eenheden $\{\pm 1\}$.

We kunnen dingen als priemorde en ggd
dan ook uitbreiden naar UFD's

Def R UFD, $\mathcal{P}$ een representantensysteem
voor de $R/\sim - \{\{0\}\}$

schrijf $a, b \in R - \{0\}$ als priemontb.

$$a = u \cdot \prod_{p \in \mathcal{P}} p^{n(p)} \qquad b = v \cdot \prod_{p \in \mathcal{P}} p^{m(p)}$$

met $n(p), m(p) \in \mathbb{N}_0$ waarvan slechts eindig
veel $\neq 0$ ("bijna alle 0)

Dan $$\operatorname{ggd}(a,b) = \prod_{p \in \mathcal{P}} p^{\min\{n(p), m(p)\}}$$

Deze is op eenheden na uniek.
Dwz, kiezen we een ander representanten-
systeem $\mathcal{P}'$ dan zijn $\operatorname{ggd}(a,b)$ en $\operatorname{ggd}'(a,b)$
geassocieerd :)

Vbd in $\mathbb{Z}$ is ggd op ± 1 na uniek te
definiëren. Kiezen we alle priemrepresentanten
positief, dan is de ggd van $a = \pm \prod \dots$ en
$b = \pm \prod \dots$ ook altijd positief. Dit is
in praktijk de gehanteerde keuze.

5.23 $f = a_0 + a_1 X + \cdots + a_n X^n \neq 0$, $f \in R[X]$, R UFD

Def de <u>inhoud</u> v.h. polynoom f is $\mathrm{inh}(f) := \mathrm{ggd}(a_0, \ldots, a_n)$

voor $d = \mathrm{ggd}(a_0, \ldots, a_n) = \mathrm{inh}(f)$ kunnen we schrijven
$f = d \cdot f_0$ waarbij f_0 in $R[X]$ inhoud 1 heeft (haal $d = p_1^{\alpha_1} p_2^{\alpha_2} \cdots$ uit de factorisatie van a_j)

Def polynoom met inh. 1 heet <u>primitief</u>

Vb in een lichaam zijn geen irreducibele factoren, dus
$K/\sim = \{\{0\}, K^*\}$, dus het representantensysteem is $\emptyset = \mathcal{P}$.
Maar dan is er slechts één ggd te definiëren, n.l.
voor $a, b \in K - \{0\} \Rightarrow a, b \in K^*$ dus de priemontb. is
$a = a$, $b = b \Rightarrow \mathrm{inh}(f) = \prod_{p \in \emptyset} p^{\cdot\cdot} = 1$
dus elk polynoom in $K[X]$ is in zekere zin primitief.

nu breiden we $f = d \cdot f_0$ voor $f \in R[X]$ uit naar: $f \in K[X]$

Lemma elk polynoom $f \neq 0$, $f \in K[X]$ kan worden geschreven als $f = d f_0$
met $d \in K^*$ en $f_0 \in R[X]$ primitief. Deze schrijfwijze is op
eenheden <u>van R</u> na uniek bepaald.

Bew Zij c het product van de noemers van de coëfficiënten van f,
dus $c \in R - \{0\}$. Dan $cf \in R[X]$ (we houden alleen de tellers $\in R$ als coeff. over)
en $cf = \mathrm{inh}(cf) \cdot f_0$ met f_0 primitief in $R[X]$, $\mathrm{inh}(cf) \neq 0$
(want geen ggd is ooit 0) dus $f = c^{-1} \cdot \mathrm{inh}(cf) \cdot f_0$, neem
dus $d = c^{-1}\, \mathrm{inh}(cf) \in K - \{0\} = K^*$ $\Rightarrow$ existentie.
Uniciteit: stel $d \cdot f_0 = e \cdot g_0$ voor $d, e \in K^*$ en f_0, g_0 primitief.
We kunnen, als $d \notin R$ of $e \notin R$, de beide elem. met gemeenschappelijke
noemer vermenigvuldigen om ze in R te brengen. Neem dus zvva aan
dat $d, e \in R$, $\Rightarrow$ dan zijn d, e beide $\mathrm{inh}(f)$ dus vallen ze
samen op eenheden na. Dus $d = ue$ voor een $u \in R^*$. Maar dan
volgt $ue f_0 = e g_0 \Rightarrow g_0 = u f_0$ (gebruik dat R domein is)
dus op eenheden na zijn de polynomen en factoren gelijk $\square$

Vb neem $\mathbb{Z}[X]$ en $\mathbb{Q}[X]$, neem $f = \frac{120}{77}X^3 + \frac{48}{7}X^2 + \frac{96}{55}X \in \mathbb{Q}[X]$

Dan nemen we $c = \text{kgv}(77, 7, 55) = 385$

$\Rightarrow cf = 600X^3 + 2640X^2 + 672X$

$\text{inh}(cf) = \text{ggd}(600, 264, 672) = 8 \cdot \text{ggd}(75, 33, 84)$

$= 8 \cdot \text{ggd}(5^2 \cdot 3, 3 \cdot 11, 3 \cdot 28) = 24 \Rightarrow$ neem $d = \frac{24}{385}$

dat geeft $f = \frac{24}{385} \cdot \underbrace{(25X^3 + 11X^2 + 28X)}_{\text{primitief in } \mathbb{Z}[X]}$.

op eenheden ± 1 van $\mathbb{Z}$ na. ◇

Lemma 5.25 Het product van twee primitieve polynomen f, g, primitief in $R[X]$, is weer primitief in $R[X]$.

Bew $f = \sum a_i X^i$, $g = \sum b_j X^j$ primitief maar $fg = \sum c_k X^k$ niet.

Dus er is een irreducibele $p \in R$ dat elke c_k deelt: $c_k \in Rp$ voor alle k. Schrijf nu $\bar{f} = \sum \bar{a_i} X^i$, $\bar{g} = \sum \bar{b_j} X^j$ voor $\bar{a_i}, \bar{b_j} \in R/Rp$, dan $\bar{f}\bar{g} = \overline{fg}$ want

$R[X]/Rp[X] \cong (R/Rp)[X] \implies \bar{f}\bar{g} = \sum \bar{c_k} X^k = \sum \bar{0} X^k = \bar{0}$

$\Rightarrow (R/Rp)[X]$ heeft nuldelers, want $\bar{f}, \bar{g} \neq 0$. Maar in een UFD is elke Rp, voor p irred priem, dus R/Rp is domein, $\Rightarrow (R/Rp)[X]$ domein. Contradictie!

(waarom $\bar{f}, \bar{g} \neq \bar{0}$? omdat f, g primitief zijn, dus niet alle coëff hebben deler p.) □

Lemma 5.26 elke $f \in R[X]$ met $f \neq 0$ kan worden geschreven als

$$f = u \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_s \cdot g_1 \cdot \ldots \cdot g_t$$

waarbij $u \in R^* = R[X]^*$, $p_1, \ldots, p_s$ irreducibele elementen van R en $g_1, \ldots, g_t$ primitief in $R[X]$ en irreducibel in $K[X]$. Bovendien is deze schrijfwijze op eenheden van R na uniek.

Bewijs: zie volgende pagina.

Bewijs $K[X]$ is een UFD, dus $f = d g_1 g_2 \cdots g_t$ met $d \in K[X]^*$ en $g_1, g_2, \ldots g_t$ irreducibel. Deze schrijfwijze is wegens UFD op volgorde van factoren en eenheden uit $K[X]^* = K^*$ uniek bepaald. Schrijf daarom steeds $g_i = d_i g_i'$, $d_i \in K^*$ met g_i' primitief (lemma 5.25) dan kunnen we $d d_1 d_2 \ldots d_t \in K[X]^* = K^*$, dus kunnen we zelfs eisen dat $g_1, g_2, \ldots g_t$ allemaal primitief in $R[X]$ zijn.

omdat $g_1, \ldots g_t$ alle primitief zijn, is $g = g_1 g_2 \cdots g_t$ $\in R[X]$ dat in $R[X]$
wegens lemma 5.25 ook, dus nu krijgen we dat $f = (d d_1 \cdots d_t) \cdot g$ met $g \in R[X]$ primitief, en dan volgt wegens lemma 5.24 is $(d d_1 \ldots d_t) \in K^*$ uniek bepaald op eenheden van R, R^* na. Bovendien is $d d_1 \ldots d_t$ gelijk aan $\text{inh}(f)$, dus ihb $d d_1 \ldots d_t \in R$. Maar R is UFD, dus dan $d d_1 \cdots d_t = \underline{u p_1 p_2 \cdots p_s}$ voor $u \in R^*$, $p_1, \ldots p_t \in R$ irreducibel en dit product is op eenheden van R na uniek.

dus we vinden $f = u \cdot p_1 p_2 \cdots p_s g_1 \cdots g_t$ en de eenduidigheid volgt eruit dat als $u p_1 \cdots p_s g_1 \cdots g_t = v q_1 \cdots q_r h_1 \ldots h_n$, dan ~~...~~ volgt $u p_1 \cdots p_s$ ~~...~~ $= \text{inh}(f) = v q_1 \cdots q_r$ zodat wegens "R is UFD" op eenheid in R^* na deze factoren dezelfde zijn.
Maar dan volgt wegens lemma 5.24 dat $g_1 \cdots g_t = h_1 \cdots h_n$ en dit maakt dat deze twee producten op eenheid in R^* na uniek zijn, want alle polynomen zijn primitief. $\square$

Een voorbeeld: $f = 4X^2 + 8X + 4$
$= (2X+2)(2X+2)$ in $\mathbb{Q}[X]$,
maar we kunnen "de inhoud eruithalen" en verkrijgen zo primitieven
$= 2 \cdot 2 \cdot (X+1)(X+1)$ in $\mathbb{Z}[X]$
en dit is op eenheid na uniek, want ook:
$f = -2 \cdot 2 \cdot (-X-1)(X+1)$ oid.

Als we nu kunnen laten zien dat precies alle irreducibele elementen van $R[X]$ zijn: de irreducibele elementen van R en de primitieve polynomen van R die irreducibel zijn in $K[X]$, dan is de "unieke schrijfwijze" uit lemma 5.26 niet zomaar een schrijfwijze meer, maar een ontbinding in irred. factoren, die uniek is op volgorde en eenheden van $R^* = R[X]^*$ na $\Rightarrow$ $R[X]$ is een UFD.

(De grote stelling) voor R UFD is $R[X]$ UFD.

Bewijs: het volstaat aan te tonen dat de irreducibele elementen van $R[X]$ precies zijn:

1) $p \in R$ irreducibel, en
2) $g \in R[X]$ die primitief zijn in $R[X]$ en in $K[X]$ irreducibel.

Bewijs hiervan: "$\subset$" zij $f \in R[X]$ irreducibel en schrijf $f = u p_1 p_2 \cdots p_s g_1 g_2 \cdots g_t$ als in 5.26
we hebben $s+t \neq 0$ want f is geen eenheid
maar als $s+t \geq 2$ dan krijgen we een ontb. voor f in minstens 2 niet-eenheden, in tegenspraak met irreducibiliteit. dus $s=1, t=0$ of $s=0, t=1$, zodat f op eenheid na een $p \in R$ irred. of een $g \in R[X]$ primitief die in $K[X]$ irred. is.

omgekeerd, "$\supset$": zij $h \in R[X]$ met $h = p \in R$ irred zoals bij 1), of $h = g \in R[X]$ zoals in 2). h is geen eenheid in $R[X]^*$, want $R[X]^* = R^*$.
Als $h = f_1 f_2$, f_1, f_2 twee niet-eenheden, dan geeft dat een tegenspraak met de beweren eenduidigheid uit 5.26 voor het product h.
Oftewel, h kan niet geschreven worden als product van twee niet-eenheden in $R[X]$ en is geen eenheid
$\Rightarrow$ h heet irreducibel.

Dit bewijst 5.16.

Diverse gevolgen van stelling 5.16:

— (Gevolg 5.27) R UFD, $K = Q(R)$ $f \in R[X]$ primitief dan f irreducibel in $K[X]$ $\Leftrightarrow$ f irreducibel in $R[X]$

Bew $\Leftarrow$ elke $f \in R[X]$ is ofwel een irred. element van R ofwel een primitief polynoom in $R[X]$ dat irred. is in $K[X]$. Omdat f primitief is, en zelf geen eenheid, kan het niet in R^* liggen en dus als $f \in R$ dan $inh(f) = f \notin R^*$ dus is f niet primitief, contradictie. Dus volgt dat f irred. is in $K[X]$ (moet wel categorie 2) zijn). dus f is irred. in $K[X]$.

$\Rightarrow$ stel f is primitief in $R[X]$ en irred. in $K[X]$. Stel $f = g \cdot h$ met $g, h \in R[X]$. Omdat f irred. is in $K[X]$ volgt ofwel $g \in K[X]^* = R - \{0\}$ ofwel $h \in K[X]^*$. neem zvva $g \in K[X]$. dan volgt dat $g \in R$ dus $f = g \cdot h$ impliceert dat $g \mid inh(f)$ maar $inh(f) = u \in R^*$, dus $k \cdot g = u$ en dus $(u^{-1}k) g = 1 \Rightarrow g \in R^*$, dus f is irreducibel.

$\boxtimes$

5.28 (Lemma van Gauss) R UFD met $K = Q(R)$ en $f \in R[X]$ monisch ($a_n = 1$). Stel $f = g \cdot h$ in $K[X]$ met g, h monisch. Dan geldt $g, h \in R[X]$

— Bewijs wegens 5.24 (elke $f \in K[X]$ kan als $d \cdot f_0$, $f_0 \in R[X]$ primitief en $d \in K^*$ worden geschreven) schrijven we $g = d \cdot g_0$, $h = e \cdot h_0$ op deze manier. omdat g monisch is volgt uit $R[X] \ni g_0 = h^{-1} g$, $R[X] \ni h_0 = e^{-1} h$ dat $h^{-1}, e^{-1} \in R$, want de kopcoeff. van g_0 is dan $h^{-1} \cdot 1 \in R$ en van h_0 is $e^{-1} \cdot 1 \in R$ Dus schrijf $u = d^{-1}$, $v = e^{-1}$ dan $uv \cdot f = ug \cdot vh = g_0 \cdot h_0$. Omdat g_0 en h_0 primitief zijn in $R[X]$, is $uv \cdot f$ dat ook. maar uv deelt elke coëff van f dus ook deelt $uv \mid inh(f)$ $\Rightarrow$ uv is in R^*. Dus er is een $z \in R^*$ met

$z(uv) = (uv)z = 1 \Rightarrow (zu)\cdot v = 1$, $v \in R$
en $z \in R^*$ en $u \in R$ dus $zu \in R \Rightarrow zv = 1$ voor $z \in R$ en $v \in R$
$\Rightarrow v \in R^*$. Evenzo $u \in R^*$. Maar dan
zijn $g = u^{-1}(ug)$, met $u^{-1} \in R^*$ en $ug \in R$ en
$h = v^{-1}\cdot(vh)$ met $v^{-1} \in R^*$ en $vh \in R \Rightarrow$
$h, g \in R[X]$, wat te bewijzen was $\square$

Praktische methoden om polynomen te ontbinden.

5.29 bepalen van nulpunten. Als we zoeken naar een lineaire factor van $f \in K[X]$ voor K een lichaam, dan weten we uit 3.7 (K is domein) dat
f een factor $X-a$ heeft $\Leftrightarrow$ a is een nulpunt van f. Bovendien zijn in $K[X]$ alle lineaire polynomen op eenheid na van de vorm $X-a$.
immers $bX - c = bb^{-1}(bX - c) = b(X - b^{-1}c)$
mits $b \neq 0$, want dan is $b \in K^*$.

in K:
zoeken van lineaire factoren komt overeen met zoeken van nulpunten. Hierbij helpt:

(a) $f = aX^2 + bX + c$ met $a \neq 0$, dan voor $2 \neq 0$:
$$4a\cdot f = (2aX+b)^2 - (b^2 - 4ac)$$

f heeft dus nulpunt α in K $\Leftrightarrow$ $(2a\alpha + b)^2 = b^2 - 4ac$
$\Leftrightarrow$ $b^2 - 4ac$ is kwadraat in K.

! waarbij we nogmaals opmerken $2 \neq 0$ in K. In $\mathbb{F}_2$ gaat dit dus niet op!

(b) als K eindig is kan men alle $\alpha \in K$ proberen.
ihb over lichamen $\mathbb{F}_q$, q priem.

(c) als $K = \mathbb{Q}$, neem dan aan dat f primitief is in $\mathbb{Z}$, anders nemen we $f = d \cdot f_0$, dus $f_0 = d^{-1}f$ voor $d \in K^*$ en f_0 primitief in $\mathbb{Z}[X]$ waarbij f_0 een nulpunt α heeft desda $f(\alpha) = 0$.

stel $\frac{b}{c} \in \mathbb{Q}$ is een nulpunt van $f = a_n X^n + \dots + a_0$, $a_i \in \mathbb{Z}$, $a_n \neq 0 \neq a_0$ (als $a_0 = 0$ deel dan eerst (een aantal) keer door X). Dan volgt dat $(cX - b) \cdot g = f$ voor $g \in \mathbb{Q}[X]$, en omdat $cX - b$ primitief is (per aanname $\text{ggd}(b, c) = 1$) en dus een irreducibel element van $R[X]$ is dat $f \in R[X]$ deelt in $K[X]$, schrijf dan $uf = (cX - b)(ug)$ voor $ug \in R[X]$ (lemma 5.24) primitief en $u \in \mathbb{Q}^*$, dan is $uf^{\in R[X]}$ primitief want (lemma 5.25) $cX - b$ en ug zijn dat, dus u moet een eenheid $\rightarrow \{\pm 1\}$ in $\mathbb{Z}$ zijn $\Rightarrow$ $f = (cX - b) g$ voor $g \in \mathbb{Z}[X]$

nu vergelijkt men de hoogstegraadscoëff, dat impliceert dat $c \mid a_n$, en de laagstegraadcoëff, dat impliceert $-b \mid a_0$ dus $b \mid a_0$.

Vb voor $f = X^3 + 5X^2 - 3X + 7$, dan komen voor b alleen ± 7, ± 1 en voor c alleen ± 1 in aanmerking dus volgt dat nulpunten in $\mathbb{Q}$ alleen ± 7 kunnen zijn.

$$f(7) = 343 + 5 \cdot 49 - 3 \cdot 7 + 7$$
$$= 13 \cdot 49 - 2 \cdot 7 \neq 0$$
$$f(-7) = -7 \cdot 49 + 5 \cdot 49 - 3 \cdot 7 + 7$$
$$= -2 \cdot 49 - 2 \cdot 7 \neq 0$$

oftewel f heeft geen lineaire factoren. Maar dan heeft f ook geen kwadratische want $f = gh$, $gr(g) = 2$ impliceert $gr(h) = 1$ $\lightning$. Dus f is irreducibel.

5.30 Polynomen reduceren modulo priem p.

over $\mathbb{Z}[X]$: Als $f \in \mathbb{Z}[X]$ <u>monisch</u> is en er is een p zodat $(f \bmod p) \in \mathbb{F}_p[X]$ irred is, dan is f irred in $\mathbb{Z}[X]$ en (omdat f primitief is, wegens gevolg 5.27) ook in $\mathbb{Q}[X]$.
Immers, als $f = g \cdot h$ in $\mathbb{Z}[X]$ dan zou $\overline{f} = \overline{h} \cdot \overline{g}$ in $\mathbb{F}_p[X]$. Dit geldt triviaal voor monische polynomen omdat $p \nmid 1$ voor p priem. Als p wél een deler is van de kopcoëff dan geeft deze methode geen informatie, omdat dan de graad van $f \bmod p$ lager kan worden (als $p \mid a_n$ dan verdwijnt $a_n X^n$ want $a_n X^n \bmod p \longleftrightarrow \overline{a_n} X^n = \overline{0} X^n = \overline{0}$.) zodat een niet-triviale ontbinding $f = g \cdot h$ in $\mathbb{Z}[X]$ niet meer aanleiding hoeft te geven tot een niet-triviale ontb. in $\mathbb{F}_p$ omdat g of h door wegvallen van de kopcoëff in $\mathbb{F}_p[X]^* = \mathbb{F}_p - \{0\}$ kan komen te zitten (gaat van graad m naar graad 0)

als voorbeeld: $h = 2X^2 + 2X + 1$ en $g = X + 1$
dan $f = 2X^3 + 4X^2 + 3X + 1$, en $(f \bmod 2) = X + \overline{1}$ irred maar f <u>niet</u>! wat er gebeurt: $\overline{f} = X + 1$, $\overline{g} = X + 1$, $\overline{h} = 1 \in \mathbb{F}_p^*$ zodat $f = g \cdot h$ in $\mathbb{F}_2[X]$ "onopgemerkt" blijft. Het is voldoende om te eisen dat f een kopcoëff a_n heeft zodat $p \nmid a_n$ want dan kan p ook niet de kopcoëff van g en h delen en dus worden $\overline{g}$ en $\overline{h}$ niet opeens constante polynomen.
Om ook te garanderen dat f irred. in $\mathbb{Z}[X]$ is, mag f ook niet door constante polynomen $q \in \mathbb{Z}$ deelbaar zijn, oftewel f moet primitief zijn.
Als f monisch is, dan volgt wegens het (modus tollens van) lemma van Gauss dat f ook niet in $\mathbb{Q}[X]$ ontbonden kan worden, dus dat f irred. in $\mathbb{Q}[X]$ is.

Eisenstein: Dit is een soort veralgemenisering van reduceren modulo p.

5.31 Eisenstein-polynomen

Def Voor R UFD, $p \in R$ irred. en $f = a_nX^n + \ldots a_0 \in R[X]$, $n>0$ is f een Eisensteinpolynoom bij p als $p \nmid a_n$, $p \mid a_i$ $\forall i = 0, 1, \ldots n-1$, $p^2 \nmid a_0$ (maar $p \mid a_0$)

Prop (Kenmerk v. Eisenstein) zij $K = Q(R)$. Dan is f irred. in $K[X]$. als f primitief is, is f dus ook irred. in $R[X]$. (per 5.27)

Bew. Omdat p niet alle a_i deelt, geldt ook $p \nmid inh(f) =: d$ we kunnen het niet-primitieve geval dus overvoeren in het primitieve geval door $f = d \cdot f_0$ te beschouwen en het voor $f_0 \in R[X]$ te bewijzen. zvva nemen we f primitief.

Stel f is niet irred in $K[X]$ dus $\exists g, h \in K[X]$, met $gr(g) > 0$ $gr(h) > 0$ (anders zijn g, h constanten dus eenheden want $f \neq 0$). In $(R/pR)[X]$ geldt wegens $p \nmid a_n$ maar $p \mid a_i$ $\forall i = 0, \ldots n-1$, dat
$\bar{f} = \bar{a}_n X^n$, $\bar{a}_n \neq 0$ $\Rightarrow \bar{f} \neq 0$
Bovendien $f = g \cdot h$ dus $\bar{f} = \bar{g} \cdot \bar{h}$. En als voor g heeft kopcoeff c en h kopcoeff b geld $a_n = bc$ en dus $\bar{a}_n = \bar{b} \cdot \bar{c}$ en $\bar{a}_n \neq 0$ dus $\bar{b}, \bar{c}$ ook niet. dus voor $gr(g) = k > 0$ $gr(h) = l > 0$ geld nu $\bar{g} = \bar{c}X^k$, $\bar{h} = \bar{b}X^l$. Maar dan volgt dat alle andere coëff van g en h door p deelbaar waren, want deze vallen weg in $\bar{g}, \bar{h} \in R/pR$.
Dus: g had constante coeff deelbaar door p en h ook. Maar dan was door vergelijken van constante coeff. in $f = g \cdot h$, dus a_0 twee keer deelbaar door p, in tegenspraak met Eisensteincriterium.
Er volgt dat $f = g \cdot h$ niet kan. $\Rightarrow f \in K[X]$ irred.
Per primitiviteit van $f \in R[X]$ volgt dat f dat dan ook is in $R[X]$. $\square$

Vb vanwege alg. ringen is "Eisenstein" ook te gebruiken in $R[X,Y]$ voor R UFD.
Bekijk bijvoorbeeld X^2+Y^2+1. Dit is in $R[Y][X]$ een eisensteinpolynoom bij $p = Y^2+1$ en dus irreducibel in $(Q(R[Y]))[X]$ maar het is ook primitief want $ggd(1, Y^2+1) = 1$, dus het is irred. in $R[X,Y]$

5.34 Reciproke polynoom.

Def voor $f \in R[X]$, R domein en $f = a_0 + \dots + a_n X^n$ met $a_0 \neq 0$ $a_n \neq 0$ dan is het reciproke polynoom:

$$f^* = a_0 X^n + \dots + a_n$$

We zien $f^* = X^n f(\frac{1}{X})$. hieruit volgt:
als $f = g \cdot h$, dan $g^* \cdot h^*$ = welgedefinieerd ten eerste, want dan hebben ook g en h niet-nul constante coeff. en voor $gr(g) = m$, $gr(h) = \ell$ volgt $g^* = X^m g(\frac{1}{X})$, $h^* = X^\ell h(\frac{1}{X})$
dus omdat ev$_{\frac{1}{X}}$ een homom. is als R commutatief is, volgt $g(\frac{1}{X}) \cdot h(\frac{1}{X}) = (g \cdot h)(\frac{1}{X})$
zodat $g^* h^* = X^{m+\ell} (gh)(\frac{1}{X}) = X^n f(\frac{1}{X}) = f^*$
dus als f^* irred is, is f dat ook en vanwege $f^{**} = f$ volgt zelfs equivalentie.

Vb

5.35 Soms werkt het om coëff. te vergelijken, als bekend is welke graden de niet-triviale factoren van f moeten hebben (bijv. wanneer lineaire factoren uitgesloten zijn).

5.36 Lineaire substituties. Voor K een lichaam, $f \in K[X]$, $a \in K^*$, $b \in K$ en zij $g = f(aX+b)$ dus substitutie van $aX+b$ op de plaats van X.

Dan: f irred. in $K[X] \Leftrightarrow g$ irred. in $K[X]$

Bewijs: we hebben het ringhomom $K[X] \to K[X]$ door $\sum_i a_i X^i \mapsto \sum_i a_i (aX+b)^i$ met inverse $\sum_i a_i X^i \mapsto \sum_i a_i (a^{-1}X - a^{-1}b)^i$, het is dus een automorfisme van ringen.

Maar voor elk domein-automorfisme f $R \to R$ (R domein) geldt: $p \in R$ irred $\Leftrightarrow f(p)$ irred. immers als $p = g \cdot h$ voor $g, h \notin R^*$ dan volgt, omdat f eenheden in eenheden overvoert dus f^{-1} ook

namelijk, $u, v \in R$ eenheden ~~en~~ f homom, dan als $uv = vu = 1$ dan $f(u)f(v) = f(uv) = f(1) = 1$ en $f(v)f(u) = f(vu) = f(1) = 1$ dus $f(u), f(v)$ zijn eenheden. dus voor automorfismes geldt: als $g \notin R^*$, dan $f(g) \notin R^*$ anders is $f^{-1}(f(g)) \in R^*$ maar dat is $g \in R^*$ $\perp$.

dat g, h geen eenheden zijn dus is $f(p)$ ook niet irred. En de omkering volgt door f^{-1} te bekijken ∎

Vb $f = X^5 + 3X^4 + 2X^2 + 5X + 7 \in \mathbb{Q}[X]$ is monisch dus primitief. Alle rationale nulpunten zijn geheel en delen 7. $f(7) > 0$ duidelijk,

$f(-7) = -7 \cdot 7^4 + 3 \cdot 7^4 + 14 \cdot 7 + 5 \cdot 7 + 7$

$= -4 \cdot 7^4 + 20 \cdot 7 < 0$ duidelijk. Dus geen lin. factoren

in $\mathbb{F}_2[X]$ is $\bar{f} = X^5 + X^4 + X + 1$
$= (X^4+1)(X+1)$
$= (X^2+1)^2(X+1)$
$= (X+1)^5$

maar ~~als f~~ is ~~f~~ monisch, dus als f ontbonden kan worden in $\mathbb{Z}[X]$ dan moeten dit lineaire factoren zijn. Dus heeft f een nulpunt in $\mathbb{Z} \subset \mathbb{Q}$, contradictie. f is dus irreducibel.

Vb (huiswerkopgave) $f = X^5 - Y^5$, welke ontbindingen zijn er in $\mathbb{C}[X,Y]$ en $\mathbb{F}_5[X,Y]$?

— we zien dat X een nulpunt is van f in zowel $\mathbb{C}[X]$ als $\mathbb{F}_5[X]$. Er is dus een factor $Y - X \in (K[X])[Y]$.
Als we bovendien naar het binomium kijken, dan zien we $(Y-X)^5 = Y^5 - \bar{5}Y^4X + \overline{10}Y^3X^2 - \overline{10}Y^2X^3 + \bar{5}YX^4 - X^5$

en dan vallen in $\mathbb{F}_5[X,Y]$ de delers van 5 weg want $\bar{5} = \bar{0}$, en staat er $Y^5 - X^5$.
in $\mathbb{C}[X,Y]$ kan zoiets niet. Daar is
$X^5 - Y^5 = (X^4 + X^3Y + X^2Y^2 + XY^3 + Y^4)(X - Y)$
en de eerste factor, zeg g heeft geen nulpunt in $Y \in \mathbb{C}[Y]$
dus er is maar één factor $X - Y$. g heeft zelfs helemaal geen nulpunten in $\mathbb{C}[Y]$:
het reciproke polynoom is namelijk
$X^4Y^4 + X^3Y^3 + X^2Y^2 + XY + 1$ en
we zien dat voor elke $\alpha \in \mathbb{C}[Y]$ geldt
dat dit $\alpha^4Y^4 + \alpha^3Y^3 + \alpha^2Y^2 + \alpha Y + 1 = 0$
geeft, dus $(\alpha^4Y^4 + \dots + \alpha Y) = -1$,
links staat iets ~~met~~ zonder ~~een~~ constante term,
rechts staat alleen een constante term! Contradictie.
Geen lineaire termen (in X) dus, en in Y ook niet want
$g(X,Y) = g(Y,X)$ ("symmetrisch" polynoom!)