H6 Gehelen van Gauss (een bijzondere ring)

Dit is $\mathbb{Z}[i] = \{a+bi \,;\, a,b \in \mathbb{Z}\}$. We zien

$n \in \mathbb{Z},\ n = a^2+b^2,\ a,b \in \mathbb{Z} \iff n = (a+bi)(a-bi)$ in $\mathbb{Z}[i]$

We gaan in dit hoofdstuk laten zien dat $\mathbb{Z}[i]$ een PID (ihb een UFD) is. Ihb is elke $n \in \mathbb{Z}_{>0}$ te schrijven als unieke priemontbinding in $\mathbb{Z}[i]$.

Deze komt lang niet altijd overeen met die in $\mathbb{Z}$, bijv. $5 = 1^2+2^2 = (1+2i)(1-2i)$. We zullen zien dat $1 \pm 2i$, wel irred. zijn in $\mathbb{Z}[i]$. Bovendien,

Als $n = p_1^{n_1} \cdots p_t^{n_t}$ in $\mathbb{Z}_{>0}$ de priemontb, en we weten van elke p_j de priemontb. in $\mathbb{Z}[i]$, dan volgt hieruit per "UFD" dat de unieke priemfactorisatie van n in $\mathbb{Z}[i]$ bekend wordt.

St 6.1 (Eenheden van $\mathbb{Z}[i]$). a) $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$

b) $2 = -i \cdot (1+i)^2$ en $-i \in \mathbb{Z}[i]^*$ en $1+i$ irred.

c) als q priemgetal is en $q \equiv 3 \bmod 4$ dan is q irred. in $\mathbb{Z}[i]$

d) als p priemgetal is en $p \equiv 1 \bmod 4$ dan is er een $\pi \in \mathbb{Z}[i]$ zodat $p = \pi \cdot \overline{\pi}$ en $\pi \neq \pi \cdot u$ voor $u \in \mathbb{Z}[i]^*$ en $\pi, \overline{\pi}$ zijn beide irred. in $\mathbb{Z}[i]$

Bew a) definieer $N : \mathbb{Z}[i] \to \mathbb{Z}$ door $N(a+bi) = (a+bi)(a-bi) = a^2+b^2$, dan zien we $N(\alpha) = \alpha\overline{\alpha}$ en dus $N(\alpha\beta) = \alpha\beta\,\overline{\alpha\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = N(\alpha)N(\beta)$
en $N(1) = 1^2 = 1$
dus ~~als~~ $u \in \mathbb{Z}[i]^*$ en $uv = vu = 1$ alleen als $N(u)N(v) = N(v)N(u) = 1$ dus alleen als $N(u) \in \mathbb{Z}^*$ dus voor $u = a+bi$ alleen als $a^2+b^2 = \pm 1$. voor -1 is dit onzin, voor 1 alleen als $a=1, b=0$ of $a=0, b=1$.

b) dit reken je na: $-i(1+i)^2 = -i(1+2i-1) = 2$

Waarom is $1+i$ irred. in $\mathbb{Z}[i]$? Stel $\alpha\beta = i$ in $\mathbb{Z}[i]$ dan in $\mathbb{Z}$ $N(\alpha)N(\beta) = N(1+i) = 2$. Maar dan is ofwel $N(\alpha)$ ofwel $N(\beta)$ een eenheid in $\mathbb{Z}$ want 2 is irred. in $\mathbb{Z}$. en dat is dan wel $+1$ want $N(\alpha) \geq 0$ voor alle $\alpha \in \mathbb{Z}[i]$. dus α of β is eenheid.

c) schrijf $q = \alpha\beta$, dan $N(\alpha)N(\beta) = N(q) = q^2$ en neem aan $\alpha, \beta \notin \mathbb{Z}[i]^*$ dus $N(\alpha) > 1$, $N(\beta) > 1$.

dit kan alleen als $N(\alpha) = N(\beta) = q$ want q is irred. en $N(\alpha), N(\beta)$ zijn beide geen eenheid in $\mathbb{Z}$.

schrijf $\alpha = a+bi$, $a, b \in \mathbb{Z}$.

als a en b beide even zijn, dan is $N(\alpha) = a^2+b^2$ een 4-voud dus $0 \bmod 4$, contradictie met $q \equiv 3 \bmod 4$

als a en b beide oneven zijn, dan is $N(\alpha) =$ $(2k+1)^2 + (2\ell+1)^2 = 4(\ell^2+k^2) + 4(k+\ell) + 2 \equiv 2 \bmod 4$, contradictie

als a of b oneven is maar niet beide, dan zien we $N(\alpha) = a^2+b^2 =$ (neem zvva $a = 2k+1$, $b = 2\ell$) $4k^2+4k+1 + 4\ell^2 \equiv 1 \bmod 4$ contradictie.

Er zijn dus geen α, β zodat dit kan! Dus q is irred.

d) St 3.14: R domein, G og., eindig, van R^*. Dan is G cyclisch. Toegepast op lichaam dus domein $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ dan is $\mathbb{F}_p^*$ een groep van orde $p-1$

$p-1$ is deelbaar door 4, dus als $\alpha \in \mathbb{F}_p^*$ en $\langle\alpha\rangle = \mathbb{F}_p^*$ dus orde$(\alpha) = p-1$, dan bekijk $x = \alpha^{\frac{p-1}{4}} \in \mathbb{F}_p^*$

Dan orde$(x) = 4$ want als kleiner dan is orde$(\alpha) < p-1$ en als groter dan is orde$(\alpha) > p-1$. Dus volgt $x^4 = 1$ en dan $x^2 = -1 \in \mathbb{F}_p^*$ want $y^2 = 1$ in $\mathbb{F}_p^*$ geeft $y^2-1 = 0$ dat y nulpunt van $X^2-1 \in \mathbb{F}_p^*$ is en omdat $\mathbb{F}_p^*$ een domein is heeft dit polynoom hooguit 2 nulpunten en die vinden we ook als ± 1 maar $x^2 = 1$ kan niet wegens orde$(x) \neq 1$ dus $x^2 = -1$. Dan is $\phi: \mathbb{Z}[i] \to \mathbb{F}_p$ met $\phi: a+bi \mapsto \bar{a} + \bar{b}x$ een surjectief ringhomomorfisme.

we gebruiken nu (zonder cirkelredenering! Het bewijs van 6.12 staat los van dit bewijs) dat $\mathbb{Z}[i]$ een PID is, en vinden dat $\ker(\phi) = (\pi)$ voor een $\pi \in \mathbb{Z}[i] \overset{1^e \text{ is.mfiest.}}{\Longrightarrow} \mathbb{Z}[i]/(\pi) \cong \mathbb{F}_p$ en daarmee en 4.10 is (π) maximaal ideaal dus π irreducibel wegens St.5.8. Verder, $p \in \ker(\phi)$ dus $p = \pi\beta$ voor een $\beta \in \mathbb{Z}[i]$. Daar π geen eenheid kan zijn, anders $(\pi) = \mathbb{Z}[i]$ niet maximaal, is dit alleen een niet-triviale ontb. als $\beta \in \mathbb{Z}[i]^*$. Maar dan volgt $(\pi) = (\pi\beta) = (p)$, en dan krijgen we een tegenspraak, want $\mathbb{Z}[i]/(\pi)$ heeft p elementen en $\mathbb{Z}[i]/(p)$ heeft als representanten $S = \{a+bi \,;\, a = 0,1,..p-1,\ b = 0,1,..p-1\}$ dus orde $p^2 \neq p$. We concluderen $N(\beta) = N(\pi) = p$.
aha maar dan $\pi\bar{\pi} = p$, dus $\beta = \bar{\pi}$ wegens "UFD".

waarom is nu $\pi \neq \bar{\pi} u$ voor een $u \in \mathbb{Z}[i]^*$?
als $u = \pm 1$ en $\pi = a+bi$ dan levert dit

$a+bi = \pm a \mp bi$ dus ofwel $+1$: $b = 0$
-1: $a = 0$

maar dan $p = a^2$ of $p = b^2$, contradictie want p is priem.
en als $u = \pm i$, dan volgt $+i$: $a+bi = -b+ai \Rightarrow a = b$
$-i$: $a+bi = -b-ai \Rightarrow a = -b$

maar $a = \pm b$ geeft $p = 2a^2$ en dat kan niet want p is priem en oneven $\square$

6.5 (Gevolg) $n \in \mathbb{Z}_{>0}$ met priemontb. in $\mathbb{Z}$:

$$n = 2^k p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r} \quad q_1^{m_1} q_2^{m_2} \cdots q_s^{m_s} \quad , n_j, m_j > 0$$

en p_i q_j onderling verschillende priemgetallen
met $p_i \equiv 1 \bmod 4 \ \forall i$ $\quad q_j \equiv 3 \bmod 4 \ \forall j$

dan is n de som van twee kwadraten alleen als
m_j even is voor alle j

Bewijs $\Leftarrow$ is natuurlijk makkelijk:
neem dan $m_j = 2\ell_j$ $\forall j$, dan met $p_i = \pi_i\overline{\pi_i}$ $\forall i$ volgt:

$$n = 2^k \pi_1^{n_1}\overline{\pi}_1^{n_1}\cdots \pi_r^{n_r}\overline{\pi}_r^{n_r}\cdot q_1^{\ell_1}q_1^{\ell_1}\cdots q_s^{\ell_s}q_s^{\ell_s}$$

$$= (1+i)^k(1-i)^k\pi_1^{n_1}\overline{\pi_1}^{n_1}\cdots\pi_r^{n_r}\overline{\pi_r}^{n_r}\cdot q_1^{\ell_1}q_1^{\ell_1}\cdots q_s^{\ell_s}q_s^{\ell_s}$$

$$= \left((1+i)^k\pi_1^{n_1}\cdots\pi_r^{n_r}q_1^{\ell_1}\cdots q_s^{\ell_s}\right)\left(\overline{(1+i)}^k\,\overline{\pi_1}^{n_1}\cdots\overline{\pi_r}^{n_r}\,\overline{q_1}^{\ell_1}\cdots\overline{q_s}^{\ell_s}\right)$$

$$= N\Big(\underbrace{(1+i)^k\pi_1^{n}\cdots\pi_r^{n_r}q_1^{\ell_1}\cdots q_s^{\ell_s}}_{\text{noem }\alpha}\Big) = a^2+b^2 \quad \text{voor } a+bi=\alpha.$$

andersom, als $n = a^2+b^2$, dan $n = \alpha\overline{\alpha}$ voor $\alpha\in\mathbb{Z}[i]$ en dan is er een ontbinding van α en $\overline{\alpha}$ in $\mathbb{Z}[i]$ gegeven wegens "$\mathbb{Z}[i]$ UFD", zeg

$$\alpha = u\cdot p_1^{n_1}p_2^{n_2}\cdots p_r^{n_r}q_1^{m_1}q_2^{m_2}\cdots q_s^{m_s}$$

waarbij $p_1,\dots p_r$ een niet-nul imaginair deel hebben en $q_1,\dots q_s\in\mathbb{Z}$ liggen. Dat zijn de enige twee mogelijkheden: $\mathrm{Im}(p)=0$ of niet.
omdat $u\overline{u} = N(u) = 1$ volgt vanwege $\overline{q_i} = q_i$:

$$n = \alpha\overline{\alpha} = (p_1\overline{p_1})^{n_1}\cdots(p_r\overline{p_r})^{n_r}q_1^{2m_1}\cdots q_s^{2m_s}.$$

We moeten nu nog laten zien:
1) elke $p_j \equiv 1 \bmod 4$ of is 2 ($\Leftrightarrow 2 \bmod 4$)
2) elke $q_j \equiv 3 \bmod 4$.

Bewijs volgens de stelling wordt n geschreven als

$$n = 2^k p_1^{n_1} \cdots p_r^{n_r} q_1^{m_1} \cdots q_t^{m_t}$$

met $p_j \equiv 1 \bmod 4$, $q_j \equiv 3 \bmod 4$ $\forall j$.

Bovendien is n te schrijven als som van 2 kwadraten alleen als $n = \alpha\bar{\alpha}$ voor $\alpha \in \mathbb{Z}[i]$

"$\Rightarrow$" stel $n = \alpha\bar{\alpha}$ voor een $\alpha \in \mathbb{Z}[i]$

We schrijven α als priemontbinding in $\mathbb{Z}[i]$, en wel als volgt:

$$\alpha = u \cdot (1+i)^{\ell} (\pi_1^{a_1} \bar{\pi}_1^{b_1}) \cdots (\pi_{r'}^{n_{r'}} \bar{\pi}_{r'}^{n_{r'}}) q_1^{c_1} \cdots q_{t'}^{c_{t'}}$$

waarbij we de irreducibele factoren P indelen in:

1) p is $(1+i)$ (irred. wegens St. 6.3 b))
2) p heeft niet-nul imaginair deel. In dat geval schrijven we de factor $\bar{p}$ ernaast
3) p heeft geen imaginair deel. Dan is $\bar{p} = p$ en schrijven we p los op

nu volgt precies, omdat $p_j = \pi'_j \bar{\pi}'_j$ voor zekere $\pi'_j \in \mathbb{Z}[i]$, irreducibel en $u\bar{u} = 1$ dat (en omdat q_j irred. in $\mathbb{Z}[i]$ zijn)

$$\underbrace{(-i)^k (1+i)^{2k} \pi'^{n_1}_1 \bar{\pi}'^{n_1}_1 \cdots \pi'^{n_r}_r \bar{\pi}'^{n_r}_r q_1^{m_1} \cdots q_t^{m_t}}_{\text{priemontb. van } n \text{ in } \mathbb{Z}[i]} = n = \alpha\bar{\alpha}$$

$$= \underbrace{\underbrace{u\bar{u}}_{1} (1+i)^{\ell} \underbrace{(-i \cdot (1+i))^{\ell}}_{\overline{1+i} = -i \cdot (1+i) \text{ vandaar}} \pi_1^{a_1+b_1} \bar{\pi}_1^{a_1+b_1} \cdots \pi_{r'}^{a_{r'}+b_{r'}} \bar{\pi}_{r'}^{a_{r'}+b_{r'}} q_1'^{2c_1} \cdots q_{t'}'^{2c_{t'}}}_{\text{priemontb. van } \alpha\bar{\alpha} \text{ in } \mathbb{Z}[i]}$$

$$= (-i)^{\ell} (1+i)^{2\ell} \pi_1^{a_1+b_1} \bar{\pi}_1^{a_1+b_1} \cdots \pi_{r'}^{a_{r'}+b_{r'}} \bar{\pi}^{a_{r'}+b_{r'}} q_1'^{2c_1} \cdots q_{t'}'^{2c_{t'}}$$

hieruit hoeft niet te volgen dat de factoren 1-op-1 overeenkomen! Maar wél dat er op eenheden en volgorde na hetzelfde staat, en bovendien omdat

de π_j' en π_j zo gekozen waren dat zij
niet $(1+i)$ kunnen zijn en ook niet in $\mathbb{Z}$ liggen
en zij de enige irred. factoren waren met
deze eigenschap, volgt $r' = r$ en op volgorde
en eenheden na komen de $\pi_j, \overline{\pi_j}, \pi_j', \overline{\pi_j'}$ overeen.

Hetzelfde volgt nu voor de q_j en q_j'. Dus $t = t'$
en er is een $\sigma \in S_t$ met $u_1, \ldots u_t \in \{\pm 1, \pm i\} = \mathbb{Z}[i]^*$
zodat $q_j = u_j q'_{\sigma(j)}$ $\forall j = 1, \ldots t.$

maar dán volgt dus $q_j^{m_j} = (u_j q'_{\sigma(j)})^{2c_j}$ $\forall j$
en dan staat er aan beide zijden een irred. factoren ontb.

$$\underbrace{q_j q_j \cdots q_j}_{m_j \text{keer}} = \underbrace{u_j^{2c_j}}_{\in \mathbb{Z}[i]} \underbrace{q'_{\sigma(j)} \cdots q'_{\sigma(j)}}_{2c_j \text{ keer}}$$

dus moet wel gelden $m_j = 2c_j$ voor alle $j = 1, \ldots t$.
dus m_j is even voor alle $j = 1, \ldots t$.

$\Leftarrow$ omgekeerd, is eenvoudiger: stel m_j is even
voor alle $j = 1, \ldots t$. dan $\frac{m_j}{2} \in \mathbb{Z}_{>0}$ $\forall j$

Dan weten we wegens 6.3. b) c), d) dat we
n ook kunnen schrijven als

$$n = (1+i)^k (1-i)^k \pi_1^{n_1} \overline{\pi_1}^{n_1} \cdots \pi_r^{n_r} \overline{\pi_r}^{n_r} q_1^{\frac{m_1}{2}} q_1^{\frac{m_1}{2}} q_t^{\frac{m_t}{2}} q_t^{\frac{m_t}{2}}$$

voor $\pi_j \overline{\pi_j} = p_j$ en π_j irred (d)), q_j irred in $\mathbb{Z}[i]$ ((c))
en dit is een ontbinding in irred. factoren in $\mathbb{Z}[i]$.

maar we zien ook dat voor

$$\alpha = (1+i)^k \pi_1^{n_1} \cdots \pi_r^{n_r} q_1^{m_1/2} \cdots q_t^{m_t/2}$$

volgt $n = \alpha \overline{\alpha}$, QED

$\square$

VIb $32 = 2^5 = (1+i)^5 (1-i)^5$. neem $\alpha = (1+i)^5 =$
$1 + 5i - 10 - 10i + 5 + i = -4 - 4i$, dan zien we

$$32 = (-4)^2 + (-4)^2$$

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1

Euclidische ringen ($\Rightarrow$ domein)

Def 6.8 een domein R heet een Euclidische ring als er een functie $g : R - \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$ is met de volgende eigenschappen:

(E1) $g(a) \leq g(ab) \quad \forall a,b \in R \quad a \neq 0 \neq b$

(E2) $\forall a,b \in R, \ b \neq 0 \quad \exists q,r \in R \quad a = qb + r \ , \ r = 0 \ \vee \ g(r) < g(b)$

Er is dus een "deling met rest" mogelijk waarbij g de "grootte" van de rest bepaalt.

Vbd We zien als voorbeeld wegens 3.1 dat elk lichaam K heeft dat $K[X]$ Euclidisch is met $g = gr$. Niet voor elke ring is $R[X]$ Euclidisch, want deling met rest van polynomen gaat alleen goed wanneer de kopcoëfficiënt van a een eenheid in R is, wat voor een lichaam natuurlijk altijd geldt.

— Het blijkt dat Euclidische ringen (PID)'s zijn (de omkering geldt niet). Door een geschikte g voor $\mathbb{Z}[i]$ te zoeken kunnen we vervolgens aantonen dat $\mathbb{Z}[i]$ een (PID) is.

St 6.10 Een Eucl. ring R is een PID.

Bew R is al een domein. We hoeven alleen te laten zien dat een ideaal $I \subset R$ een hoofdideaal is.

Als $I = \{0\}$, is $I = (0)$ en zijn we klaar.
Als $I \neq \{0\}$ dan $I - \{0\} \neq \emptyset$. Bekijk daarom g op $I - \{0\}$. omdat $g(I - \{0\}) \subset \mathbb{Z}_{\geq 0}$ en $\mathbb{Z}_{\geq 0}$ is van onderen begrensd en discreet, volgt dat

$g\big|_{I-\{0\}}$ ergens zijn minimum aanneemt. Zij $b \in I - \{0\}$ zdd $g(b) = \min_{x \in I - \{0\}} g(x)$.

We laten zien dat $I = (b)$. "$\supset$" is duidelijk, want $b \in I$. En "$\subset$" volgt als volgt: zij $x \in I$, dan $x = 0$ of $x \neq 0$. Als $x = 0$ dan $x \in (b)$, en anders kunnen we wegens (E2) delen met rest naar $b \neq 0$:

$x = qb + r$ met $r = 0$ of $g(r) < g(b)$. Als $r \neq 0$, dan $g(r) < g(b)$ én $r = x - qb$, $x, qb \in I$ dus $r \in I - \{0\}$ maar dan neemt g dus niet zijn minimum aan in b op $I - \{0\}$ maar in r, contradictie!

We concluderen dat $r = 0$, en dus $x = qb \in (b)$ dus volgt $I \subset (b)$ en hiermee is het bewijs rond. $\square$

Opm Het bewijs van deze stelling is geheel analoog aan het bewijs dat $\mathbb{Z}$ een (PID) is (2.6 a Groepentheorie) of $K[X]$ (3.4) maar nu gebruiken we ipv $|\cdot| = g$ of $gr = g$ de algemene functie g.

St. 6.12 ($\mathbb{Z}[i]$ is Euclidisch): $\mathbb{Z}[i]$ is een Euclidische ring. hierbij nemen we $g = N$

Bewijs We controleren hiertoe de voorwaarden (E1) en (E2) op N:

(E1): voor $\alpha, \beta \in \mathbb{Z}[i]$, $\alpha, \beta \neq 0$ geldt $N(\alpha\beta) = N(\alpha)N(\beta)$ en $N(\alpha), N(\beta) \geq 1$, dus volgt
$N(\alpha\beta) = N(\alpha)N(\beta) \geq N(\alpha)$

(E2) Hiervoor bekijken we N uitgebreid naar $\mathbb{C}$. en $\mathbb{Z}[i] \subset \mathbb{C}$. Voor $\alpha, \beta \in \mathbb{Z}[i]$ en $\beta \neq 0$ moeten we $\gamma, \rho \in \mathbb{Z}[i]$ vinden zodat

$$\alpha = \gamma\beta + \rho \quad , \quad N(\rho) < N(\beta) \text{ of } \rho = 0$$

en $N(\beta) > 0$

aangezien $N(0) = 0$ kunnen we ook wel schrijven

$$\alpha = \gamma\beta + \rho \quad , \quad N(\rho) < N(\beta)$$

in $\mathbb{C}$ kunnen we delen door $\beta \neq 0$, n.l. krijgen we dan equivalent

$$\alpha/\beta = \gamma + \rho/\beta \quad \text{en} \quad N(\rho/\beta) < 1$$

oftewel, we zoeken $\gamma \in \mathbb{Z}[i]$ met $N(\alpha/\beta - \gamma) < 1$
en daaruit volgt dan $\rho = \alpha - \beta\gamma$, en deze voldoen.

$\frac{\alpha}{\beta} = u + vi$ voor $u, v \in \mathbb{R}$ (in feite $\mathbb{Q}$, n.l.

$$\frac{\alpha}{\beta} = \frac{a+bi}{c+di} = (a+bi)\left(\frac{c-di}{c^2+d^2}\right)$$

$$= \left(\frac{ac+bd}{c^2+d^2}\right) + \left(\frac{bc-ad}{c^2+d^2}\right)i \quad)$$

omdat $u, v \in \mathbb{R}$ tussen twee gehelen
in liggen en wel op hooguit $\frac{1}{2}$ afstand, kunnen we
precies $u', v' \in \mathbb{Z}$ vinden zodat $|u-u'| \leq \frac{1}{2}$ en
$|v-v'| \leq \frac{1}{2}$

Het blijkt dat $\gamma = u' + v'i$ voldoende is, n.l.

$$N(\alpha/\beta - \gamma) = N((u-u') + (v-v')i)$$
$$= (u-u')^2 + (v-v')^2$$
$$\leq \left(\tfrac{1}{2}\right)^2 + \left(\tfrac{1}{2}\right)^2 = \tfrac{1}{2} < 1$$

$\square$

We zien dat bijvoorbeeld wanneer u of v in $\frac{1}{2}\mathbb{Z}$ ligt,
dat dan de deling met rest niet uniek hoeft
te zijn zoals we van bijv. $\mathbb{Z}$ en $K[X]$ gewend
zijn.

→ Gevolg: $\mathbb{Z}[i]$ is een hoofdidealdomein.

Vbd deling met rest in $\mathbb{Z}[i]$: $\alpha = 5+i$ $\beta = 1+2i$
We bekijken $\alpha/\beta \in \mathbb{C}$, dat is $\frac{(5+i)(1-2i)}{1+4} =$
$\frac{7}{5} - \frac{9}{5}i$, dan werkt $\gamma = 1-2i$ volgens de stelling

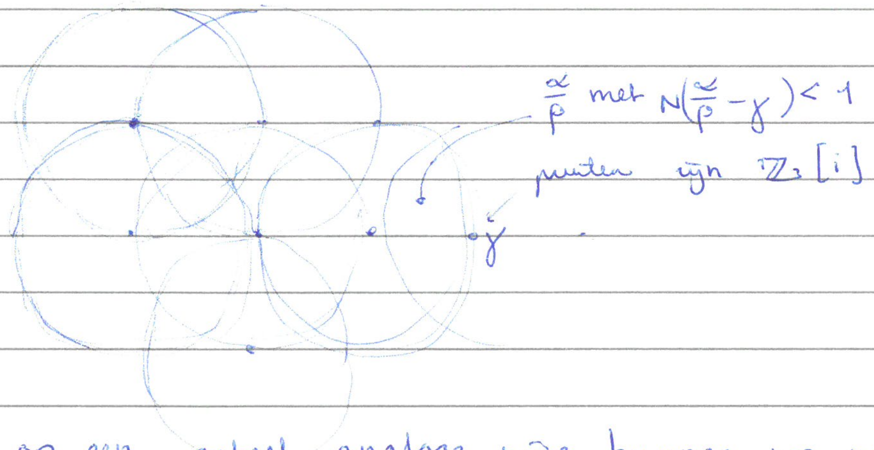
en $\rho = 5+i - (1-2i)(1+2i)$
$= i$ met $N(\rho) = 1 < 5 = N(\beta)$.

6.14 Het bewijs van st. 6.12 heeft de volgende meetkundige interpretatie: elke $\frac{\alpha}{\beta} \in \mathbb{Q}[i] \subset \mathbb{C}$

kan benaderd worden met een γ zodat
$N\left(\frac{\alpha}{\beta} - \gamma\right) = \left|\frac{\alpha}{\beta} - \gamma\right|^2 < 1$

oftewel we kunnen met inwendige cirkelschijven
$U_1(\gamma) = \{ z \in \mathbb{C} \mid |z-\gamma|^2 < 1 \}$ heel $\mathbb{C}$ overdekken.

We zien dat deling met rest zeker niet uniek is waar de cirkels elkaar overlappen!



op een geheel analoge wijze kunnen we nagaan dat de ring $\mathbb{Z}[\frac{1}{2}(1+\sqrt{-3})]$ euclidisch is met keuze $g = N$ en zo ook voor $\mathbb{Z}[\sqrt{-2}]$

— We kunnen ook concluderen dat een niet-PID ook geen Euclidische ring (ER) kan zijn:

Lichaam $\subset$ (ER) $\subset$ (PID) $\subset$ (UFD) $\subset$ Domein $\subset$ comm. Ring $\subset$ Ringen

En er zijn nog wel wat speciale definities hiertussen in.

Een alternatieve definitie van GGD in een PID.

— UFD - GGD: hadden we reeds gedefinieerd als : $a, b \in R - \{0\}$

$$ggd(a,b) = \prod_{p \in \mathcal{P}} p^{\min\{ord_p(a), ord_p(b)\}}$$

$ggd(a,0) = ggd(0,a) = a$ op eenheid na uniek

— PID - GGD: in elke PID geldt ook $(a,b) = (d)$ voor een $d \in R$. Definiëren we $ggd(a,b) = d$ dan is deze op eenheid na goedgedefinieerd, want $(d') = (d) \Leftrightarrow d' = hd,\ d = kd',\ h, d \in R$
$\Leftrightarrow d = khd \Leftrightarrow d = 0$ of $kh = 1$
$\Leftrightarrow d = d' = 0$ (want dan $(d) = \{0\} = (d')$) óf $h \in R^*$
$\Leftrightarrow d' = hd$ voor $h \in R^*$.

(Opgave) de UFD-ggd valt in een PID samen (op eenheid na) met de PID-ggd, dwz

$$(a,b) = \left(\prod_{p \in \mathcal{P}} p^{\min\{ord_p(a), ord_p(b)\}} \right)$$

Tip Het bewijs volgt de structuur van het bewijs van St. 5.15

Zij namelijk $a = u p_1^{n_1} \cdots p_t^{n_t}$, $b = v p_1^{m_1} \cdots p_t^{m_t}$ in irred. elementen en $\mu_j = \min\{n_j, m_j\}$ voor $j = 1, \ldots, t$, dus $ggd_{UFD}(a,b) = p_1^{\mu_1} \cdots p_t^{\mu_t}$, noem dit d.

We zien eenvoudig in dat $d \mid a$ en $d \mid b$, dus $(a,b) \subset (d)$ is triviaal. Zij nu $\begin{cases} a' = u p_1^{n_1 - \mu_1} \cdots p_t^{n_t - \mu_t} \\ b' = v p_1^{m_1 - \mu_1} \cdots p_t^{m_t - \mu_t} \end{cases}$
(dus $a = a'd$, $b = b'd$)

We gaan laten zien dat $(a') + (b') = R$, want dan volgt dat er $s, r \in R$ zijn met $sa' + rb' = 1$ en dus $sa + rb = (sa' + rb')d = d$, zodat $d \in (a,b)$ en dus $(d) \subset (a,b)$ ook bewezen is. We doen dit analoog aan 5.15:

- omdat R PID is, is er een $g \in R$ met $(a', b') = (g)$. Stel g is geen eenheid wegens UFD: er is een factorisatie!

Dan is er een irreducibel element $p \in R$ dat g deelt en dus $a' \in (g) \subset (p)$, $b' \in (g) \subset (p)$

dus $p \mid u p_1^{n_1-\mu_1} \cdots p_t^{n_t-\mu_t}$, $p \mid v p_1^{m_1-\mu_1} \cdots p_t^{m_t-\mu_t}$

wegens uniciteit van priemontbinding (of wegens: in een UFD is (p) priemideaal, al zeggen we daarmee hetzelfde) volgt $p = p_j$ voor één j uit $1,\dots,t$.

Dus volgt voor die p_j dat deze zowel in a' als in b' zit. Probleem: dan $n_j - \mu_j > 0$, $m_j - \mu_j > 0$ maar we hadden $\mu_j := \min\{n_j, m_j\} \in \{n_j, m_j\}$ dus ofwel $n_j - \mu_j = 0$ ofwel $m_j - \mu_j = 0$, en dat levert een tegenspraak.

We concluderen dat $g \in R^*$, dus $(a', b') = R \ni 1$ en dus volgt dat er $s, r \in R$ zijn met $sa' + rb' = 1$ en voor deze s, r geldt dan $sa + rb = d \Rightarrow (d) \subset (a, b)$

$\square$

De PID ($=$ UFD) – GGD berekenen in een Euclidische ring

Het Euclidisch algoritme, bekend in het geval van $\mathbb{Z}$, uit H1 Groepentheorie, kan worden uitgebreid naar alg. Euclidische ringen om een ggd "snel" uit te rekenen".

Bovendien is ook het uitgebreide Euclidische algoritme te generaliseren en stelt dit ons in staat r, s te vinden met $ra + sb = d$.

De generalisatie is grotendeels een invuloefening:

6.19 Zij R Euclidische ring met g de (E1),(E2)-functie $a, b \in R$ neem zvva $g(a) \geq g(b)$

noem $r_{-1} = a$, $r_0 = b$ en vind gegeven (r_{k-1}, r_k) steeds $r_{k+1} = r_{k-1} - q_k r_k$ met $g(r_{k+1}) < g(r_k)$ of $r_{k+1} = 0$

we zien steeds dat $(r_{k-1}, r_k) = (r_{k-1} - q_k r_k, r_k)$
zodra $r_{n+1} = 0$ zien we dus $(a,b) = (r_n, 0) = (r_n)$
en volgt $\operatorname{ggd}(a,b) = r_n$

Bovendien $\begin{pmatrix} r_k \\ r_{k+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix} \begin{pmatrix} r_{k-1} \\ r_k \end{pmatrix}$ voor $k = 0, \ldots n$

zodat $\begin{pmatrix} r_n \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{n-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_0 \end{pmatrix} \begin{pmatrix} r_{-1} \\ r_0 \end{pmatrix}$

in de eerste coordinaat kijken:
en zo vinden we s, r met $d = r_n = s r_{-1} + r r_0$
$= sa + rb$

$\square$

Vbd met $g = gr$ is $\mathbb{F}_5[X]$
een Euclidische ring. Zoeken we de ggd van

$$9X^5 + 3X^4 - X^2 + 2X, \qquad X^4 + 3X^2 - 8$$

dan vinden we: $9X^5 + 3X^4 - X^2 + 2X =$

$$(9X + 3)(X^4 + 3X^2 - 8) + (-27X^3 - 10X^2 + 74X + 24)$$

$X^4 + 3X^2 - 8 =$

$$\left(-\frac{1}{27}X + \frac{10}{27^2}\right)(-27X^3 - 10X^2 + 74X + 24)$$
$$+ \left(3 + \left(\frac{10}{27}\right)^2 + \frac{74}{27}\right)X^2 + \left(-\frac{740}{27^2} + \frac{24}{27}\right)X$$
$$- \frac{240}{27^2}$$

$-27X^3 - 10X^2 + 74X + 24 =$

$(X \quad \ldots$

oké je snapt het idee .. heel goed "uit te rekenen" Thx Euclides.

H7 : Symmetrische polynomen !

R commutatieve ring en $n \in \mathbb{Z}$, $n \geq 1$

Def $f \in R[X_1, \dots, X_n]$ heet <u>symmetrisch</u> als bij elke permutatie $\sigma \in S_n$, geldt
$$f(X_1, \dots, X_n) = f(X_{\sigma(1)}, \dots, X_{\sigma(n)})$$

Vbd $X_1^2 X_2 + X_2^2 X_1 + X_3^2 X_1 + X_3^2 X_2 + X_1^2 X_3 + X_2^2 X_3$

— Als we ~~de~~ polynoomring in een nieuwe variabele Z over $R[X_1, \dots X_n]$, dus $R[X_1, \dots, X_n][Z]$, beschouwen, en we bekijken
$$(Z - X_1)(Z - X_2) \dots (Z - X_n) \in R[X_1, \dots, X_n][Z]$$
dan werkt dit uit tot:

$$Z^n + \left(\sum_{i=1}^n -X_i\right) Z^{n-1} + (X_1X_2 + X_1X_3 + \dots + X_1X_n + X_2X_3 + \dots + X_2X_n + \dots + X_{n-1}X_n) Z^{n-2}$$
$$+ -\sigma_3 Z^{n-3} + \dots + (-1)^n \sigma_n$$

Hierbij zijn: $\sigma_t = \sum_{1 \leq i_1 < i_2 < \dots < i_t \leq n} X_{i_1} X_{i_2} \dots X_{i_t}$ voor $t = 1, \dots, n$

We zien dat de vorm van σ_t afhangt van t en impliciet van n, dus van de $R[X_1 \dots X_n]$ waarin we werken.

St 7.2 (Hoofdstelling over de symmetrische polynomen)

$f \in R[X_1 \dots X_n]$ symm. polynoom. Dan is f te schrijven als polynoom in $\sigma_1, \dots \sigma_n$ met coëff uit R. **Deze** schrijfwijze is bovendien <u>eenduidig</u>!

Bew Zij $f \neq 0$, anders zijn we klaar (n.l. kies $a_i = 0$ voor alle $i = 1, \dots n$). Orden de termen $r X_1^{a_1} X_2^{a_2} \dots X_n^{a_n}$ zodat $(a_1, a_2, \dots a_n)$ lexicografisch geordend zijn. Deze ordening is eenduidig want lexicografische ordening is totaal.

voor gedetailleerde uitleg zie verderop (*)

(dus $a_i > b_i$ en $a_1 = b_1, \ldots, a_{i-1} = b_{i-1}$ dan $(a_1, \ldots a_n) > (b_1, \ldots b_n)$)

de kopterm, zeg $r X_1^{c_1} X_2^{c_2} \cdots X_n^{c_n}$ heeft dan:

c_1 = de grootste a_1 die voorkomt

c_2 = de grootste a_2 die voorkomt bij alle termen met $a_1 = c_1$

c_3 = de grootste a_3 die voorkomt bij termen met $a_1 = c_1$, $a_2 = c_2$.

Bovendien, omdat f symmetrisch is, geldt zvva $c_1 \geq c_2 \geq c_3 \geq \cdots \geq c_n$. Anders verwisselen we twee X_i, X_j in f, en dan zou dit een term geven die vóór $r X_1^{c_1} \cdots X_n^{c_n}$ komt doordat c_i nu hoger is dan c_j, terwijl f nog steeds hetzelfde polynoom is!

dit is eigenlijke de sleutelstap vh bewijs. We hebben eenkt nodig dat f symm. is.

dus mag!

Bewering: $r \underbrace{\sigma_1^{c_1 - c_2}}_{\geq 0} \underbrace{\sigma_2^{c_2 - c_3}}_{\geq 0} \cdots \underbrace{\sigma_{n-1}^{c_{n-1} - c_n}}_{\geq 0} \underbrace{\sigma_n^{c_n}}_{\geq 0}$ heeft dezelfde kopterm als f in de huidige ordening.

σ_1 heeft kopterm X_1

σ_2 heeft kopterm $X_1 X_2$

$\vdots$

σ_n " ——— " $X_1 X_2 \cdots X_n$, dus

kopterm $(r \sigma_1^{c_1 - c_2} \cdots \sigma_n^{c_n}) = (r \cdot 1 \cdot 1 \cdot 1 \cdots 1) X_1^{c_1 - c_2} (X_1 X_2)^{c_2 - c_3} \cdots (X_1 \cdots X_n)^{c_n}$

want dit mag omdat 1 nooit een nuldeler is,

$= r X_1^{c_1} X_2^{c_2} \cdots X_n^{c_n}$

noem nu $f_1 = f - r \sigma_1^{c_1 - c_2} \cdots \sigma_n^{c_n}$

Vbd $X_1^2 X_2 + X_1 X_2 X_3 + X_2^2 X_1 + X_3^2 X_2 + X_3^2 X_1 + X_2^2 X_3 + X_1^2 X_3$

lexicografisch ordenen geeft:

$X_1^2 X_2 + X_1^2 X_3 + X_1 X_2^2 + X_1 X_2 X_3 + X_1 X_3^2 + X_2^2 X_3 + X_2 X_3^2$

$(2,1,0) > (2,0,1) > (1,2,0) > (1,1,1) > (1,0,2) > (0,2,1) > (0,1,2)$

(*) wat nu als er $i < j$ zijn met $c_i < c_j$? Permutatie van X_i en X_j levert hetzelfde polynoom op, want f

is symmetrisch (hiermee valt/staat het bewijs, dit is de belangrijkste stap!)
in deze term $rX_1^{c_1} \cdots X_n^{c_n}$ zijn nu X_i en X_j verwisseld
maar c_i en c_j niet, want we permuteren de variabelen
(anders zijn we gewoon aan het herschrijven en gebruiken we
niet eens dat f symmetrisch is!)

dus $rX_1^{c_1} \cdots X_j^{c_i} \cdots X_i^{c_j} \cdots X_n^{c_n}$ is deze term dan, en
we herschikken de nieuwe permutatie op nummers (X_i en X_j
worden nu herschikt/herschreven): $rX_1^{c_1} \cdots X_i^{c_j} \cdots X_j^{c_i} \cdots X_n$.
Nu klopt het weer, maar we zien iets geks:

- f met X_i en X_j gepermuteerd is hetzelfde polynoom als
f vóór deze permutatie.

- maar de macht van X_i in deze term $rX_1^{c_1} \cdots X_i^{c_j} \cdots X_j^{c_i} \cdots X_n$
is hoger dan die in de eerdere lexicografisch grotere
term. We hebben dus in hetzelfde polynoom f een
lexicografisch "eerdere" term gevonden dan de aanvankelijk door
ons gevonden lexicografisch "eerste" term $rX_1^{c_1} \cdots X_i^{c_i} \cdots X_j^{c_j} \cdots X_n$.

— merk op dat we echt nodig hebben dat
f symmetrisch is.

In een woordenboek bijvoorbeeld:

"aalbes" zou het eerste woord kunnen zijn, maar toch
'e'<'s'. Als een woordenboek alle permutaties van
"aalbes" zou bevatten, dan zou "aalbes" echter
niet vooraan kunnen staan, want dan zou
"aabels" vooraan staan omdat deze permutatie
bestaat. Het polynoom is het hele woordenboek,
de termen zijn woorden. Een woordenboek dat
alle permutaties van alle woorden bevat gaat
door elke permutatie in zichzelf over!

einde (*)

— We zetten het bewijs van 7.2 voort met $f_1 = f - r\sigma_1^{c_1-c_2} \cdots \sigma_n^{c_n}$

De som van twee symmetrische polynomen (in evenveel variabelen!) en het product is weer symmetrisch omdat in een commutatieve ring $ev_{(X_{i_1}, \dots X_{i_n})} : R[X_1 \dots X_n] \to R[X_1 \dots X_n]$ een homomorfisme is, dus als g, f symm is, desda $ev_{(X_{\sigma(1)}, \dots X_{\sigma(n)})}(f_{\text{of } g}) = f_{\text{of } g}$ voor alle $\sigma \in S_n$ dan is

$$\forall \sigma \in S_n : ev_{(X_{\sigma(1)} \dots X_{\sigma(n)})}(gf) = ev_{(X_{\sigma(1)} \dots X_{\sigma(n)})}(g) \, ev_{(X_{\sigma(1)} \dots X_{\sigma(n)})}(f)$$

$$= gf \quad \text{dus } gf \text{ dat ook}$$

en evenzo $ev_{(X_{\sigma(1)} \dots X_{\sigma(n)})}(g+f) = ev_{..}(g) + ev_{..}(f) = g+f$

dus $g+f$ dat ook.

dus we kunnen de termen van f_k op elk moment lexicografisch ordenen, concluderen $c_1^{(k)} \geq c_2^{(k)} \dots c_n^{(k)}$ voor kopterm $r^{(k)} X_1^{c_1^{(k)}} \dots X_n^{c_n^{(k)}}$ en daarmee $c_1^{(k)} - c_2^{(k)} \geq 0 \ \dots \ c_{n-1}^{(k)} - c_n^{(k)} \geq 0$ zodat we van f^k af kunnen trekken $r^{(k)} \sigma_1^{c_1^{(k)} - c_2^{(k)}} \dots \sigma_n^{c_n^{(k)}}$

We moeten nu alleen laten zien dat dit proces op een bepaald moment $f^T = 0$ voor $T \in \mathbb{Z}_{>0}$ oplevert.

Hiertoe bekijken we de totale graad $\text{totgr}(f)$
(zie H1 als je deze kwijt bent)

We zien namelijk $\text{totgr}(\sigma_t) = t$, zodat

$$\text{totgr}(r\sigma_1^{c_1-c_2} \dots \sigma_n^{c_n}) = (c_1 - c_2) + 2(c_2 - c_3) + 3(c_3 - c_4) + \dots + nc_n$$
$$= c_1 + c_2 + c_3 + \dots + c_n \leq \text{totgr}(f)$$

want $X_1^{c_1} X_2^{c_2} \dots X_n^{c_n}$ komt voor, maar of het de hoogste totale macht heeft weten we niet
($X_1^1 X_2^1 X_3^1 X_4^1$ komt lexicografisch later dan $X_1^2 X_2^1$)
($X_n^{100000} < X_1^1$ is hier geen goed tegenvoorbeeld want we moeten wel als eerste term $c_1 \geq c_2 \geq \dots \geq c_n$ kiezen, of in andere woorden als X_n^{100000} erin zit dan X_1^{100000} ook)

dus i.h.b. $\text{totgr}\left(r^{(k)}\sigma_1^{c_1^{(k)}-c_2^{(k)}}\cdots\sigma_n^{c_n^{(k)}}\right) \le \text{totgr}(f_k)$

en daaruit volgt $\text{totgr}(f_{k+1}) = \text{totgr}\left(f_k - r^{(k)}\sigma_1^{c_1^{(k)}-c_2^{(k)}}\cdots\sigma_n^{c_n^{(k)}}\right)$
$\le \text{totgr}(f_k)$

dus $\text{totgr}(f) \ge \text{totgr}(f^1) \ge \dots$

bovendien (en hier is de lexicografische ordening onze grote tweede troef!) is de nieuwe kopterm van f_{k+1} altijd lexicografisch later dan die van f_k, dus kunnen we (omdat er maar een eindig aantal $c_1, c_2, \dots c_n \in \mathbb{Z}_{\ge 0}$ met $\sum_i c_i = \text{totgr}(f_k)$ is) nooit langer dan dat aantal (Partitiegetal $P(n, K)$ met $K = \text{totgr}(f_k)$) stappen "blijven hangen" op $\text{totgr}(f_k)$, immers cyclen door machtsindexes $(c_1, \dots c_n)$ is niet mogelijk omdat we de lexicografische ordening aflopen.

oftewel, uiteindelijk treedt er een $T \in \mathbb{N}_1$ op met $\text{totgr}(f_T) = 0$

——— hiermee is existentie aangetoond, immers dan

$$f = \sum_{1 \le k \le T} r^{(k)} \sigma_1^{c_1^{(k)}-c_2^{(k)}} \sigma_2^{c_2^{(k)}-c_3^{(k)}} \cdots \sigma_{n-1}^{c_{n-1}^{(k)}-c_n^{(k)}} \sigma_n^{c_n^{(k)}}$$

Nu nog Uniciteit!!

Vbd $X_1^2X_2 + X_1^2X_2^2 + X_1X_2^2$ heeft:

lexicografisch $X_1^2X_2^2 + X_1^2X_2 + X_1X_2^2$, neem $1\sigma_1^{\overset{2-2}{0}}\sigma_2^{\overset{2}{2}} = (X_1+X_2)^0(X_1X_2)^2$

dan $X_1^2X_2^2 + X_1^2X_2 + X_1X_2^2 - (X_1^2X_2^2) = X_1^2X_2 + X_1X_2^2$

$X_1^2X_2 + X_1X_2^2$, neem $1\sigma_1^{\overset{2-1}{1}}\sigma_2^{\overset{1}{1}} = (X_1+X_2)(X_1X_2)$

dan geeft dit 0, dus:

$$X_1^2X_2 + X_1^2X_2^2 + X_1X_2^2 = (X_1X_2)^2 + (X_1+X_2)(X_1X_2)$$

□

——— Uniciteit: we moeten aantonen: als $g_1 \ne g_2$, $g_1, g_2 \in R[T_1, \dots T_n]$ (n variabelen-polynomen over R), dan zijn $g_1(\sigma_1, \dots \sigma_n)$ en $g_2(\sigma_1, \dots \sigma_n)$ verschillend! Schrijf $g = g_1 - g_2$. We werken over een commutatieve ring dus evaluatie is homom. Het is

– daarmee voldoende aan te tonen: $\left\{\begin{array}{l}\text{als } g \in R[T_1, \ldots T_n],\ g \neq 0 \text{ dan} \\ g(\sigma_1, \ldots, \sigma_n) \neq 0.\end{array}\right.$

Bewijs hiervan: elke term in g is van de vorm

$$rT_1^{a_1-a_2} T_2^{a_2-a_3} \ldots T_n^{a_n}$$

worden geschreven (waarbij a_i uniek bepaald zijn door a_n, dan a_{n-1} = "macht van T_{n-1}" $+ a_n \geq a_n$, .. etc.)

Bekijk dan nu de lexicografische ordening van deze termen, geordend op $(a_1, \ldots a_n)$ lexicografisch. De eerste term schrijven we dus als

$$rT_1^{c_1-c_2} \ldots T_n^{c_n}.$$

Substitueren we $T_j \rightsquigarrow \sigma_j$ voor $j = 1, \ldots, n$ dan geeft deze eerste term een polynoom met lexicografische kopterm van

$$r\underbrace{\sigma_1^{c_1-c_2}}_{X_1^{c_1-c_2}} \underbrace{\sigma_2^{c_2-c_3}}_{X_1^{c_2-c_3}X_2^{c_2-c_3}} \ldots \underbrace{\sigma_n^{c_n}}_{X_1^{c_n}X_2^{c_n}\ldots X_n^{c_n}}, \text{ dat is}$$

is eerste term uit $\sigma_2^{c_2-c_3}$

en dat is $r(X_1^{c_1-c_2})(X_1^{c_2-c_3}X_2^{c_2-c_3})(X_1^{c_3-c_4}X_2^{c_3-c_4}X_3^{c_3-c_4}) \ldots (X_1^{c_{n-1}-c_n}X_2^{c_{n-1}-c_n} \ldots X_{n-1}^{c_{n-1}-c_n}) \cdot (X_1^{c_n} \ldots X_n^{c_n})$

$$= r X_1^{c_1} X_2^{c_2} \ldots X_n^{c_n}$$

maar voor elke $r' T_1^{c'_1-c'_2} \ldots T_n^{c'_n}$ waarbij $(c'_1, \ldots c'_n)$ lexicogr. later komt voor deze term geldt dat de kopterm bij substitutie, $r'X_1^{c'_1} \ldots X_n^{c'_n}$ nooit gelijk aan $-r T_1^{c_1} \ldots T_n^{c_n}$ kan zijn want $(c'_1 \ldots c'_n)$ is lexicografisch <u>strikt</u> later dan $(c_1, \ldots c_n)$ <u>per aanname</u>. Dus de term $rX_1^{c_1} \ldots X_n^{c_n}$ <u>blijft</u>, zodat $g(\sigma_1, \ldots \sigma_n) \neq 0$ $\square$

— Toepassingen van symm. polynomen

Stelling: zij R' comm. ring en $R \subset R'$ deelring en zij $h \in R[X]$ monisch irreducibel van graad n zodat in $R'[X]$: $f = (X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n)$

Zij nu $g \in R[X_1, X_2, \ldots X_n]$ symmetrisch polynoom, dan is $g(\alpha_1, \ldots \alpha_n) \in R$

(een symmetrische uitdrukking van $\alpha_1 \ldots \alpha_n$ ligt in de kleinere ring)

Bew de H.S. van de symm. polynomen zegt: er zijn de $R[X_1 .. X_n] \ni \sigma_1, \ldots \sigma_n$ symmetrische elementaire polynomen, en er is een $h \in R[Y_1, \ldots, Y_n]$ met $g = h(\sigma_1, \ldots \sigma_n)$

dus $\alpha_1, \ldots \alpha_n$ invullen geeft $g(\alpha_1, \ldots, \alpha_n) = h(\sigma_1(\alpha_1, \ldots, \alpha_n), \ldots, \sigma_n(\alpha_1, \ldots \alpha_n))$

Anderzijds is f te schrijven als

$f = X^n - b_1 X^{n-1} + b_2 X^{n-2} + \cdots + (-1)^{n-1} b_{n-1} X + (-1)^n b_n$
met $b_j \in R$
en $f = (X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n) = H(\alpha_1, \ldots \alpha_n)$
met $H \in R[X_1, \ldots X_n, X]$ door $H = (X - X_1)(\cdots)(X - X_n)$
en $H \overset{def}{=} X^n - \sigma_1 X^{n-1} + \cdots + (-1)^{n-1}\sigma_{n-1} X + (-1)^n \sigma_n$
, dus $b_j = \sigma_j(\alpha_1, \ldots, \alpha_n)$ voor $j = 1, \ldots n$

$\Rightarrow$ $g(\alpha_1, \ldots, \alpha_n) = h(\sigma_1(\alpha_1, \ldots, \alpha_n), \ldots, \sigma_n(\alpha_1, \ldots, \alpha_n))$
enerzijds, anderzijds
$\sigma_1(\alpha_1, \ldots, \alpha_n) = b_1, \quad \ldots \quad \sigma_n(\alpha_1, \ldots, \alpha_n) = b_n \in R$

$\Rightarrow$ $g(\alpha_1, \ldots, \alpha_n) = h(b_1, \ldots b_n)$ en $h \in R[X_1, \ldots X_n]$
en $b_1, \ldots b_n \in R$

een polynomiale uitdrukking in R van elem. van R
dus $h(b_1, \ldots, b_n) \in R$, dus $g(\alpha_1, \ldots, \alpha_n) \in R$

Vbd een toepassing : $f = X^3 + aX^2 + bX + c \in \mathbb{Q}[X]$
$f = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3) \in \mathbb{C}[X]$

dan zien we $a = -\sigma_1(\alpha_1, \alpha_2, \alpha_3) = -(\alpha_1+\alpha_2+\alpha_3)$
en $b = \sigma_2(\alpha_1, \alpha_2, \alpha_3) = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3$
en $c = -\sigma_3(\alpha_1, \alpha_2, \alpha_3) = -\alpha_1\alpha_2\alpha_3$

$\Rightarrow -(\alpha_1+\alpha_2+\alpha_3) \in \mathbb{Q}$
$\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3 \in \mathbb{Q}$
$\alpha_1\alpha_2\alpha_3 \in \mathbb{Q}$

en stelling zegt bijvoorbeeld : $\alpha_1^2 + \alpha_2^2 + \alpha_3^2 \in \mathbb{Q}$

en dat begrijpen we, want $\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = a^2 - 2b$

Vbd $aX^2 + bX + c = 0 \qquad a \neq 0$

heeft dubbele nulpunten wanneer discriminant
$\Delta = b^2 - 4ac = 0$

Algemeen $f = X^n + b_{n-1}X^{n-1} + \cdots + b_0$ in een domein
in de uitbreiding $f = (X-\alpha_1)\cdots(X-\alpha_n)$

en zij $\Delta = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (\alpha_i - \alpha_j)$

dan f dubbel nulpunt $\Leftrightarrow \exists i \neq j \; \alpha_i = \alpha_j$ (we werken in een domein, geen nuldelers
$\Leftrightarrow \Delta = 0$

Maar Δ is een symm. uitdrukking in $\alpha_1, \ldots \alpha_n$
dus te schrijven in $\sigma_1(\alpha_1, \ldots, \alpha_n) = -b_{n-1}$
$\sigma_2(\alpha_1, \ldots \alpha_n) = b_{n-2}$
$\vdots$
$\sigma_n(\alpha_1, \ldots \alpha_n) = (-1)^n b_0$

dus Δ is te berekenen zonder dat we $\alpha_1, \ldots \alpha_n$ weten!

Vb $\Delta(X^2+aX+b) = a^2-4b$

$\Delta(X^3+aX^2+bX+c) = a^2b^2-4b^3-4ac-27c^2+18abc$

op de middelbare: uit Δ komt een formule voor de nulpunten. Kan dit ook voor hogeregraads?

Alg $f \in K[X]$ met $\mathrm{char}(K) \neq 2,3$ (we willen straks gaan delen door 2,3), K lichaam

aanname: $\exists \omega \in K$ $\omega \neq 1$ met $\omega^3 = 1$

neem $f = X^3+aX^2+bX+c$. en zij $\alpha_1, \alpha_2, \alpha_3 \in K$ de nulpunten.

We gaan kijken naar
$$A_1 = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3$$
$$A_2 = \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3 \quad \in K[\alpha_1,\alpha_2,\alpha_3]$$

(123): $A_1 \rightsquigarrow \omega A_1$

$A_2 \rightsquigarrow \omega^2 A_2$

(23) $A_1 \rightsquigarrow A_2$

$A_2 \rightsquigarrow A_1$

dit is hoe A_1, A_2 wijzigen onder permutaties $(123), (23)$

omdat $(123), (23)$ heel S_3 voortbrengen, volgt: A_1A_2 en $A_1^3+A_2^3$ zijn symmetrisch:

want onder (123) $A_1A_2 \rightsquigarrow \omega A_1\omega^2A_2 = A_1A_2$

(23) $A_1A_2 \rightsquigarrow A_2A_1 = A_1A_2$

$\Rightarrow$ onder heel S_3 $A_1A_2 \rightsquigarrow A_1A_2$

en onder (123) $A_1^3+A_2^3 \rightsquigarrow \omega^3A_1^3+\omega^6A_2^3 = A_1^3+A_2^3$

(23) $A_1^3+A_2^3 \rightsquigarrow A_2^3+A_1^3 = A_1^3+A_2^3$

$\Rightarrow$ onder heel S_3 $A_1^3+A_2^3 \rightsquigarrow A_1^3+A_2^3$

zij dus $A := A_1A_2$, $B = \dfrac{A_1^3+A_2^3}{2}$ symm.

dus ik kan A, B uitdrukken in a, b, c

met het delen zoals in de hoofdstelling:

$$A_1^3 + A_2^3 = -2a^3 + 9ab - 27c$$
$$A_1 A_2 = a^2 - 3b$$

$\Delta = 4B^2 - 4A^3$

! merk nu op: $(T - A_1^3)(T - A_2^3) = \overline{T^2 - 2BT + A^3}$

we weten de nulpunten van deze tweedegraads:

dus

$$A_1^3 = B + \sqrt{B^2 - A^3} \qquad A_2^3 = B - \sqrt{B^2 - A^3}$$

dus $A_1 = \sqrt[3]{B + \sqrt{B^2 - A^3}}$ $\quad A_2 = \sqrt[3]{B - \sqrt{B^2 - A^3}}$

$\omega^3 = 1 \quad \omega \neq 1 \Rightarrow \frac{\omega^3 - 1}{\omega - 1} = 0 \Rightarrow \omega^2 + \omega + 1 = 0$

dus
$$\begin{aligned} A_1 + A_2 &= 2\alpha_1 + (\omega + \omega^2)\alpha_2 + (\omega + \omega^2)\alpha_3 \\ &= 2\alpha_1 - \alpha_2 - \alpha_3 \\ &= 3\alpha_1 - (\alpha_1 + \alpha_2 + \alpha_3) = 3\alpha_1 + a \\ \Rightarrow \alpha_1 &= (A_1 + A_2 - a)/3 \end{aligned}$$

en de andere α_2, α_3 op dezelfde manier.