H3

St. 3.1 (Unieke deling met rest voor polynomen)
R ring, $f, g \in R[X]$ met:

- $g \neq 0$
- kopcoëfficiënt van g ligt in R^*

Dan bestaan er unieke $q, r \in R[X]$ met
- $f = qg + r$
- $r = 0$ of $gr(r) < gr(g)$

(neemt men $gr(0) = -\infty$ dan is dit geval niet apart nodig)

Bew noem $n = gr(f)$ $m = gr(g)$
We bewijzen met inductie naar n, bij vaste g.

IB als $n < m$, neem $q = 0$ en $f = g$.
IH als het geldt voor alle $n' < n$, $n \geq m$, dan
IS laat f $gr(f) = n$ hebben. Zij a de kopcoëff van f en b die van g. $b \in R^*$, dus er is een $b^{-1} \in R$. $\tilde{f} = f - (ab^{-1}X^{n-m})g$
Dan heeft $(ab^{-1}X^{n-m}) \cdot g$ graad n en kopcoëff. a.
Dus $\tilde{f}$ heeft geen hogere machten dan n, en voor X^n is de coëfficiënt $a - a = 0$, dus $gr(\tilde{f}) < n$.
Pas IH toe, we vinden dan $\tilde{q}, \tilde{r}$ met
$$\tilde{f} = \tilde{q}g + \tilde{r}. \Rightarrow f = \tilde{f} + (ab^{-1}X^{n-m}) \cdot g = (\tilde{q} + ab^{-1}X^{n-m})g + \tilde{r}$$
dus neem $q = \tilde{q} + ab^{-1}X^{n-m}$, $r = \tilde{r}$ dan zijn we klaar met existentie

Uniciteit: stel $f = qg + r$, $f = \hat{q}g + \hat{r}$
voor $q, \hat{q}, r, \hat{r} \in R[X]$ en $gr(r), gr(\hat{r}) < gr(g)$

$$f - f = 0 \quad \text{dus} \quad \hat{q}g + \hat{r} - (qg + r) = 0$$
$$\Rightarrow (\hat{q} - q)g = r - \hat{r}$$
Als $\hat{q} \neq q$, dan, omdat de kopcoëfficiënt van g een eenheid is, ~~is~~ het ~~geen~~ nuldeler dus

kan niet wegvallen. $\Rightarrow$ linkerzijde heeft graad m. maar rechterzijde heeft hoogstens graad $m-1$ ↯ $\Rightarrow q = \hat{q}$

maar dan is de linkerzijde het nulpolynoom,

$0 = r - \hat{r} \Rightarrow \hat{r} = r$. dus r, q zijn uniek ▲

opm R domein $\Rightarrow$ $R[X]$ domein (H.1)

Gevolg K lichaam $\Rightarrow$ elke ideaal $I \subset K[X]$ is een hoofdideaal

Bew K is een lichaam, dus K is een domein, dus $K[X]$ domein, dus we kunnen delen met rest in $K[X]$. Zij I ideaal van $K[X]$ en $g \in I$, $g \neq 0$ en de graad van g minimaal. We willen bewijzen $I = (g)$, dus $I \subset (g)$. Zij $f \in I$. Doordat g als kopcoëff. $k \in K$ heeft en $K - \{0\} = K^*$ en $k \neq 0$, hebben we dat k een eenheid is, dus deel uniek met rest
$f = qg + r$, $q, r \in K[X]$. Dan $r = f - qg$
en $f \in I$, $g \in I$ dus $qg \in I$, dus $f - qg \in I \Rightarrow r \in I$.
en tevens $r = 0$ of $\overset{r \neq 0}{gr(r)} \overset{\text{en}}{<} gr(g)$. Als $\overset{r \neq 0}{gr(r)} < gr(g)$ dan was g niet het polynoom $\neq 0$ van kleinste graad in I, contradictie. Dus $r = 0 \Rightarrow f \in (g)$
dus $I \subset (g)$ en $g \in I$ dus $(g) \subset I \Rightarrow I = (g)$ $\square$

We hebben "K lichaam nodig" om te verzekeren dat g kopcoëff eenheid heeft. Immers in $\mathbb{Z}[X]$ is $2 \notin \mathbb{Z}^*$ dus $(2X, X^2)$ of $(2, X)$ etc zijn geen hoofdidealen: 2 heeft minimale graad maar ligt niet in $\mathbb{Z}^*$, en geen enkel const polynoom ligt hier in $\mathbb{Z}^*$

Opm We kunnen uit een polynoom dus een functie $R \to R$ construeren. Maar merk op dat voorzichtigheid geboden is omdat in niet-commutatieve ringen evaluatie geen homomorfisme hoeft te zijn.

Bovendien kunnen twee verschillende polynomen dezelfde functie induceren. Denk aan $X^2 - \bar{1} \in (\mathbb{Z}/3\mathbb{Z})[X]$ en $X^2 + \bar{2}$, beide induceren ze $\bar{0} \mapsto \bar{2}$, $\bar{1} \mapsto \bar{0}$ $\bar{2} \mapsto \bar{0}$

St. 3.5 R commutatieve ring $\alpha \in R$, $f \in R[X]$

Dan is er een $q \in R[X]$ met

$$f = q(X-\alpha) + ev_\alpha(f)$$
$$= q(X-\alpha) + f(\alpha)$$

Bew zie dat voor $g = X - \alpha$ geldt dat kopcoëff $1 \in R^*$ is, dus pas unieke deling met rest toe:

$$f = q(X-\alpha) + r$$

Nu geldt dat evaluatie op $R[X] \to R$ een homom. is wegens "R commutatief" $\Rightarrow$

$$ev_\alpha(f) = ev_\alpha(q(X-\alpha) + r)$$
$$= ev_\alpha(q)\, ev_\alpha(X-\alpha) + ev_\alpha(r)$$
$$= 0 + ev_\alpha(r)$$
$$= ev_\alpha(r)$$

maar $gr(r) < gr(g) = 1$, dus r is een constant polynoom $\Rightarrow ev_\alpha(r) = r \in R$

dus $r = ev_\alpha(f) = f(\alpha)$

$$\Rightarrow f = q(X-\alpha) + ev_\alpha(f) \qquad \Diamond$$

Vb In het duale lichaam $(K[\varepsilon])[X]$, evaluatie in ε en $f = \varepsilon X^2 - 5 + X^4 - X^5$:

$$X - \varepsilon \,/\, -X^5 + X^4 + \varepsilon X^2 - 5 \,\backslash\, -X^4 + (1-\varepsilon)X^3 + \varepsilon X^2 + \varepsilon X$$

$-X^5 + \varepsilon X^4$

$(1-\varepsilon)X^4 + \varepsilon X^2 - 5$

$(1-\varepsilon)X^4 - \varepsilon X^3$

$\varepsilon X^3 + \varepsilon X^2 - 5$

εX^3

$\varepsilon X^2 - 5$

εX^2

-5

$$\Longrightarrow f = (-X^4 + (1-\varepsilon)X^3 + \varepsilon X^2 + \varepsilon X)(X-\varepsilon) - 5$$

en idd $f(\varepsilon) = 0 - 5 + 0 - 0$
$= -5$

St. 3.6 R domein $\alpha_1, .. \alpha_n \in R$ n <u>verschillende</u> nulpunten voor $f \in R[X]$.
Dan is er een $q \in R[X]$ met $f = q(X-\alpha_1)\cdots(X-\alpha_n)$

Bew Met inductie naar n:

IB $n=1$: dit is St. 3.5 toegepast op commutatieve ring R met $ev_{\alpha_1}(f) = 0$, dus $f = q(X-\alpha_1) + 0$.

IH Stel voor een $n \geq 1$ geldt dat als $\alpha_1, .. \alpha_{n-1}$ nulpunten van f zijn, dan $f = q(X-\alpha_1)\cdots(X-\alpha_{n-1})$

IS {neem nu $\alpha_1, .. \alpha_n$ nulp. van f
wegens 3.5 geldt $f = q(X-\alpha_n)$ voor $q \in R[X]$.
Bovendien $ev_{\alpha_i}(f) = 0 \Longrightarrow ev_{\alpha_i}(q(X-\alpha_n)) = 0 \Longrightarrow$
$ev_{\alpha_i}(q)\cdot(\alpha_i - \alpha_n) = 0$. $\alpha_i \neq \alpha_n$ ("verschillend")
dus $\alpha_i - \alpha_n \neq 0$. Wegens R domein dus ook $ev_{\alpha_i}(q) = 0$ want er zijn geen nuldelers.
Pas dan IH toe op q met $n-1$ verschillende nulpunten, dan $q = \tilde{q}(X-\alpha_1)\cdots(X-\alpha_{n-1})$
$\Rightarrow f = q(X-\alpha_n) = \tilde{q}(X-\alpha_1)\cdots(X-\alpha_n)$ QED. $\square$

St 3.7 (Gevolg voor de graad vh polynoom)
Zij R domein en $f \in R[X]$, $f \neq 0$.
Dan heeft f in R hooguit $gr(f)$ verschillende nulpunten.

3.8 (Gevolg voor gelijkheid van polynomen) R een domein, als $f, g \in R[X]$ en $f(\alpha_1) = g(\alpha_1) \ldots f(\alpha_{n+1}) = g(\alpha_{n+1})$ maar $gr(f), gr(g) \leq n$
Dan zijn f, g gelijk in $R[X]$

Immers $f-g$ heeft graad $\leq n$ maar $n+1$ nulpunten, dus $f-g = 0 \Rightarrow f = g$

Opm Het is essentieel dat R domein is, anders kan $f \in R[X]$ wellicht meer nulpunten hebben, doordat nuldelers "cancelen" tijdens evaluatie
VB in $(\mathbb{Z}/8\mathbb{Z})[X]$ heeft $X^2 - \bar{1}$ de nulpunten van $(X-\bar{1})(X+\bar{1}) \leftarrow \left\{ \begin{matrix} \bar{3} \\ \bar{1} \\ \bar{7} \end{matrix} \right.$ $\bar{5}$ waarbij $\bar{3}, \bar{5}$ nuldelers geven

maar..

is er een $q \in (\mathbb{Z}/8\mathbb{Z})[X]$ met

$X^2 - \bar{1} = q(X - \bar{5})$? Stelling 3.5 zegt van wel

Omdat $\bar{1}$ eenheid is moet $gr(q) = 1$ zijn, anders wordt de graad rechts te hoog en als q constant juist te klein.

Dus $X^2 - \bar{1} = (\bar{a} X + \bar{b})(X - \bar{5})$
$= \bar{a} X^2 - \bar{5}\bar{b} + (\bar{b} - \bar{5}\bar{a}) X$

$\Rightarrow \bar{a} = \bar{1}$

$\Rightarrow X^2 - \bar{5}\bar{b} + (\bar{b} - \bar{5}) X = X^2 - \bar{1}$

$\Rightarrow \bar{b} - \bar{5} = \bar{0} \Rightarrow b = \bar{5}$?

maar dan $X^2 - \overline{25} = X^2 - \bar{1}$

dit klopt inderdaad, dus $X^2 - \bar{1}$ is óók $(X - \bar{5})^2$

Dus er is geen unieke ontbinding in lineaire polynomen.. tegenintuïtief

St. 3.10 $p \in \mathbb{Z}_{>0}$ priemgetal. Dan

$$X^p - X = \prod_{a \in \mathbb{F}_p} (X - a) \quad \text{in } \mathbb{F}_p[X]$$

Bewijs De kleine st. van Fermat (Groepentheorie) gaf dat voor p priem,

$a^p \equiv a \mod p$ dus

equivalent $a^p = a \quad \forall a \in \mathbb{F}_p$

equivalent $\forall a \in \mathbb{F}_p \; ev_a(X^p - X) = \bar{0}$

en $\mathbb{F}_p$ is domein (lichaam!)

$\Rightarrow X^p - X$ is van de vorm $q \prod_{a \in \mathbb{F}_p} (X - a)$

maar $\mathbb{F}_p$ is domein, dus de graad van $\prod_{a \in \mathbb{F}_p} (X - a)$ is $\# \mathbb{F}_p = p$ maar dan moet q constant polynoom zijn, en $q \in \mathbb{F}_p$

maar dan is de kopcoëff van $q \prod_{a \in \mathbb{F}_p} (X - a)$ precies $q \bar{1}^p = q$ en die van $X^p - X$ is $\bar{1} \Rightarrow q = 1$

dus $X^p - X = \prod_{a \in \mathbb{F}_p} (X - a)$ ◊

3.12 (Gevolg: st. van Wilson) p priemgetal, dan

$$(p-1)! \equiv -1 \mod p$$

hier gebruiken we dat er unieke deling met rest is

deel door X:

Bew $X^p - X = \prod_{a \in \mathbb{F}_p} (X - \bar{a})$ in $\mathbb{F}_p$,

$$= \prod_{a=0}^{p-1} (X - \bar{a}) = X \prod_{a=1}^{p-1} (X - \bar{a})$$

$$X^{p-1} - \bar{1} = \prod_{a=1}^{p-1} (X - \bar{a})$$

vanwege $\mathbb{F}_p$ commutatief is er het evaluatie homom $ev_{\bar{0}}$.

$$ev_{\bar{0}}(X^{p-1} - \bar{1}) = ev_{\bar{0}}\left(\prod_{a=1}^{p-1}(X - \bar{a})\right) = \prod_{a=1}^{p-1} ev_{\bar{0}}(X - \bar{a})$$

$$\bar{0}^{p-1} - \bar{1} = \prod_{a=1}^{p-1}(\bar{0} - \bar{a}) = (-\bar{1})^{p-1} \prod_{a=1}^{p-1} \bar{a}$$

$$\bar{0} - \bar{1} = (-\bar{1})^{p-1}\,\overline{(p-1)!}$$

voor $p = 2$ is $p-1$ oneven dus $(-\bar{1})^{p-1} = -\bar{1} \overset{\text{in } \mathbb{F}_2}{=} \bar{1}$

voor $p \neq 2$ is $p-1$ even dus $(-\bar{1})^{p-1} = \bar{1}$

$$\Rightarrow -\bar{1} = \overline{(p-1)!} \Rightarrow (p-1)! \equiv -1 \mod p \qquad \square$$

Nu komt een belangrijke stelling over Eindige ondergroepen van R^* (de multiplicatieve eenhedengroep in R) als R een domein is.

Eerst volgt een lemma uit Groepentheorie:

3.13 Zij G eindige Abelse groep

(i) $x, y \in G$, orde(x), orde$(y) < \infty$ (dwz $\in \mathbb{N}_{>0}$)
stel orde(x), orde(y) zijn relatief priemgetallen (onderling ondeelbaar, copriem etc.)
Dan orde(xy) = orde(x) orde(y)

(ii) G eindige groep, dus alle $g \in G$ hebben eindige orde (immers $g^{\#G} = e$ dus orde$(g) \mid \#G$)
Zij $a \in G$ elem. met orde$(a) = \max\{\text{orde}(g) : g \in G\}$
Dan $\forall g \in G$ orde$(g) \mid$ orde(a)

Bew. (i) Zij orde$(x) = m$ orde$(y) = n$. en orde$(xy) = t$

Dan $(xy)^{mn} = x^{mn}y^{mn} = (x^m)^n (y^n)^m$

$= e^n e^m = e$

$\Rightarrow t \mid mn$

Anderzijds, $(xy)^t = e$ dus

$e = (xy)^{mt} = x^{mt}y^{mt} = y^{mt} \Rightarrow n \mid mt$

$e = (xy)^{nt} = x^{nt}y^{nt} = x^{nt} \Rightarrow m \mid nt$

maxggd$(m,n) = 1 \Longrightarrow n \mid t$, $m \mid t$

dus $mn =$ kgv$(m,n) \mid t \Rightarrow mn \mid t$

samen met $t \mid mn \Longrightarrow mn = t$

(ii) neem a, m zoals in de stelling

Neem $b \in G$ willekeurig. Zij $n =$ orde(b)

Zij p een priemgetal en schrijf

orde$(a) = p^i m$ met $p \nmid m$,

orde$(b) = p^j n$ met $p \nmid n$. Dan is te bewijzen dat $j \leq i$, dan immers deelt (voor elke p) orde$(b) \mid$ orde(a)

uit orde$(a) = p^i m$ volgt orde$(a^{p^i}) = m$ want $p^i m$ is het kleinste getal zodat $a^{p^i m} = e$, dus m is het kleinste getal zodat $(a^{p^i})^m = e$. Evenzo orde$(b^{p^j}) = n$ en orde$(a^m) = p^i$, orde$(b^n) = p^j$

ggd$(m, p^j) = 1 \Rightarrow$ orde$(b^n a^{p^i}) = mp^j$

maar mp^i is de maximale orde dus

$mp^j \mid mp^i \Longrightarrow p^j \mid p^i \Rightarrow j \leq i$ QED $\diamond$

3.14 $G \subset R^*$ o.g en $\# G$ eindig, R domein
Dan is G cyclisch

Bew R is commutatief, dus R^* abels, dus G ook.
Neem $a \in G$ met maximale orde, $\text{orde}(a) = M$
Wegens het lemma 3.13 geldt $\forall b \in G$ $\text{orde}(b) \mid M$
dus $\forall b \in G$ $ev_b(X^M - 1) = 0$

Dan volgt ook wegens 3.7 dat (R domein)
$X^M - 1$ niet meer dan M nulpunten kan
hebben. Dus $\# G \leq M$. Maar ook
$M \mid \# G \implies M = \# G$, dus a brengt
heel de groep G voort.

Def $b \in R^*$ met $\text{orde}(b) < \infty$ noemt men
eenheidswortels.

3.16 p priem, dan is $\mathbb{F}_p^*$ cyclisch en $\# \mathbb{F}_p^* = p-1$

Want $\mathbb{F}_p$ is commutatief dus $\mathbb{F}_p^*$ abels,
dus cyclisch $\Leftarrow$ $\mathbb{F}_p$ is lichaam dus domein, pas 3.14
toe. $\mathbb{F}_p$ is lichaam dus $\mathbb{F}_p^* = \mathbb{F}_p - \{\bar{0}\}$
$\implies \# \mathbb{F}_p^* = \# \mathbb{F}_p - 1 = p-1$ □

3.17 Differentiëren zonder analyse.

Zij vanaf nu tot eind H3 R een
commutatieve ring

Zij $f \in R[X]$ en beschouw het polynoom
in twee variabelen $f(X,Y) - f(X) \in R[X,Y]$

We zien dat $ev_0^Y : (R[X])[Y] \to R[X]$ door $f(X+Y) \mapsto f(X,0)$
voor zo'n polynoom het nulpolynoom $0 \in R[X]$
oplevert.

Wegens 2.13 geldt dus

$$f(X+Y) - f(X) \in Y R[X,Y] = (Y)$$

$\Rightarrow f(X+Y) - f(X) = Y \cdot H(X,Y)$
voor een $H \in R[X,Y]$ uniek

Def We definiëren de <u>afgeleide</u> van f dan door

$f' = ev_0^Y(H) = H(X,0) \in R[X]$

We kunnen dit, omdat delen door $Y \in R[X,Y]$ dus zeker kan (met rest 0) en $R[X,Y]$ is commutatief, als

$$f' = \left(\frac{f(X+Y) - f(X)}{Y} \right) \Big|_{Y=0}$$

Notatie Andere notatiewijzen: $\frac{d}{dX} f$ of $\frac{\partial}{\partial X} f$

als $f \in R[X, \tilde{X}, \cdots]$

St. 3.18 R commutatieve ring, dan $\forall f, g \in R[X]$:

(i) $(f+g)' = f' + g'$

$(fg)' = f'g + g'f$

(ii) Voor $f = \sum_{k=0}^{n} a_k X^k$ is $f' = \sum_{k=1}^{n} k a_k X^{k-1}$ $\quad ka_k = \overbrace{a_k + \cdots + a_k}^{k \text{ termen}}$

Bew (i) zij $f(X+Y) - f(X) = Y \cdot H_1$ $\quad g(X+Y) - g(Y) = Y H_2$

Dan $(f+g)(X+Y) - (f+g)(X) =$

$(f(X+Y) + g(X+Y)) - (f(X) + g(X)) =$

$(f(X+Y) - f(X)) + (g(X+Y) - g(X)) =$

$Y H_1 + Y H_2 =$

$Y(H_1 + H_2)$

$\Rightarrow (f+g)' = H_1(X,0) + H_2(X,0) = f' + g'$

en $(fg)(X+Y)-(fg)(X) = f(X+Y)g(X+Y) - f(X)g(X)$

$= f(X+Y)\ g(X+Y) - f(X)g(X+Y) + f(X)g(X+Y) - f(X)g(X)$
$= (f(X+Y)-f(X))\,g(X+Y) + f(X)(g(X+Y)-g(X))$
$= YH_1 g(X+Y) + f(X)\cdot Y H_2 = Y(H_1 g(X+Y) + f(X)H_2)$

deel door Y, substitueer daarna $Y=0$:

$= H_1(X,0)\underbrace{g(X+0)}_{=g(X)=g} + f(X)H_2(X,0) = f'g + fg'$

(ii) Eerst met inductie naar $k>0$ dat $(a_k X^k)' = k a_k X^{k-1}$

en merken op dat voor $k=0$, $(a_0)(X+Y)-(a_0)(X)$
$= a_0 - a_0 = 0 = Y\cdot 0 \Longrightarrow (a_0)' = 0$.

IB voor $k=1$: $(a_1X^1)(X+Y)-(a_1X^1)(X)$
$= a_1X + a_1Y - a_1X = a_1Y$
$\Rightarrow (a_1X^1)' = \left(\frac{a_1Y}{Y}\right)\Big|_{Y=0} = a_1\big|_{Y=0} = a_1$

IH stel $k-1\geq 1$, $(r_1 X^{k-1})' = (k-1)r X^{k-2}$. Dan
IS bewijzen we het voor k:

$$(a_kX^k)' = ((a_kX^{k-1})\cdot X)' \overset{(i)}{=} (a_kX^{k-1})'X + (a_kX^{k-1})X'$$

$X' = (1X)' = 1$ wegens IB
$(a_kX^{k-1})' = (k-1)a_k X^{k-2}$ wegens IH:

$$(a_kX^k)' = (k-1)a_kX^{k-2}\cdot X + a_kX^{k-1}\cdot 1$$
$$= (k-1)a_kX^{k-1} + 1a_kX^{k-1}$$
$$= k a_k X^{k-1}$$

uit (i) volgt dat "je de som kunt nemen". $\square$

Opm. We kunnen f' ook definiëren als in (ii). Maar dan volgen andere eigenschappen wat minder makkelijk, bijvoorbeeld:

Def R commutatieve ring, dan heet $\alpha\in R$ een nulpunt van $f\in R[X]$ als $f(\alpha)=0$
Wegens 3.5 of 3.6 dan $f = q(X-\alpha)$ voor $q\in R[X]$

Def Kunnen we zelfs schrijven $f = q(X-\alpha)^2$
Dan heet α een dubbel of meervoudig nulpunt van f.

St 3.20 R commutatieve ring, $f \in R[X]$, $\alpha \in R$.
Dan is α een dubbel nulpunt van f
$\Longleftrightarrow$ α is een nulpunt van f'

Bew Schrijf volgens de deling-met-reststelling

$$f = q(X-\alpha)$$

α is dubbel nulpunt $\Longleftrightarrow$ $q(X-\alpha) = \hat{q}(X-\alpha)^2$
$\Longleftrightarrow$ $q = \hat{q} \cdot (X-\alpha)$ $\exists \hat{q} \in R[X]$
$\Longleftrightarrow$ $ev_\alpha(q) = 0$ oftewel $q(\alpha) = 0$

En α nulpunt van f' $\Leftrightarrow$ $f'(\alpha) = 0$
Stel dat we kunnen bewijzen $f'(\alpha) = q(\alpha)$,
dan zijn we klaar want dan

$$f = \hat{q}(X-\alpha)^2 \Leftrightarrow q(\alpha) = 0 \Leftrightarrow f'(\alpha) = 0.$$

Bewijs: pas (i) uit st. 3.18 toe:

$$f = q(X-\alpha) \Rightarrow f' = q'(X-\alpha) + q(X-\alpha)'$$
$$= q'(X-\alpha) + q$$
$$\Rightarrow f'(\alpha) = q'(\alpha)(\alpha-\alpha) + q(\alpha)$$
$$= 0 + q(\alpha) = q(\alpha)$$

en we zijn klaar. $\square$