EINDIGE LICHAMEN

door

H.W. Lenstra Jr.

1. LICHAMEN

Een *lichaam* is een verzameling K waarin voor elk tweetal elementen a en b een *som* $a + b$ en een *product* $a \cdot b$, beide weer tot K behorend, gedefinieerd zijn, en dat verder een *nul-element* 0 en een *eenheidselement* 1 bevat, zodanig dat voor alle a, b en c uit K geldt:

$(a + b) + c = a + (b + c)$

$a + b = b + a$

$0 + a = a$

Elke a heeft een *tegengestelde* $-a$, die weer tot K behoort, met

$a + (-a) = 0$

$(a \cdot b) \cdot c = a \cdot (b \cdot c)$

$a \cdot b = b \cdot a$

$1 \cdot a = a$

elke $a \neq 0$ heeft een *inverse* $a^{-1} \in K$ met

$a \cdot (a^{-1}) = 1$

$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

$0 \neq 1$

Bekende voorbeelden zijn het lichaam der rationale getallen, het lichaam der reële getallen en het lichaam der complexe getallen.

Wij zullen ons bezig houden met *eindige lichamen*, dat zijn lichamen met slechts eindig veel elementen. Deze nemen een aparte plaats in in de

theorie der lichamen: veelgebruikte argumenten zoals "een polynoom f van de de graad n heeft hoogstend n nulpunten dus er is een $x \in K$ met $f(x) \neq 0$" zijn voor eindige lichamen niet correct, maar hier staat tegenover dat men beschikt over *tel-argumenten*: overwegingen die berusten op het tellen van het aantal elementen in een deelverzameling. Bij de opbouw van de theorie zullen we ons voornamelijk van dit soort argumenten bedienen.

Zij p een priemgetal (1 is geen priemgetal). Het "lichaam der gehele getallen modulo p" bestaat uit de p getallen 0, 1, ..., p-1; deze getallen worden opgeteld en vermenigvuldigd als gewone gehele getallen, behalve dat men de uitkomst steeds vervangt door de rest bij deling door p, om weer in de verzameling {0, 1, ..., p-1} terecht te komen. Voor p = 7 heeft men bijvoorbeeld $4+5 = 2$, want 9 geeft rest 2 bij deling door 7, en $4 \cdot 5 = 6$, want 20 geeft rest 6 bij deling door 7. Het is niet moeilijk na te gaan dat men op deze manier inderdaad een lichaam krijgt; het gegeven dat p een priemgetal is gebruikt men om het bestaan van inversen te bewijzen: voor $0 < a < p$ geldt $(a,p) = 1$ dus er zijn gehele getallen x, y met $x \cdot a + y \cdot p = 1$; zetten we $x = q \cdot p + r$ met q geheel en $0 \leq r < p$, dan is r de inverse van a. We geven dit lichaam aan met $\mathbb{F}_p$.

Zo zien we dat er voor elk priemgetal p een eindig lichaam met p elementen bestaat. De vraag of er meer eindige lichamen bestaan, en hoeveel elementen deze hebben, wordt beantwoord door de volgende stelling.

STELLING 1. *Ieder eindig lichaam heeft* p^n *elementen waar* p *een priemgetal en* n *een geheel getal* ≥ 1 *is. Omgekeerd bestaat er bij elk priemgetal* p *en elk geheel getal* $n \geq 1$ *een eindig lichaam met* p^n *elementen. Twee eindige lichamen met evenveel elementen zijn isomorf.*

Hier noemen we twee lichamen K_1 en K_2 *isomorf* als er een 1-1 afbeelding van K_1 op K_2 bestaat die de optelling en de vermenigvuldiging respecteert. De laatste zin van stelling 1 zegt dus dat de structuur van een eindig lichaam volledig bepaald wordt door zijn aantal elementen.

Het bewijs van stelling 1 wordt in de paragrafen 2 en 4 gegeven.

2. HET AANTAL ELEMENTEN VAN EEN EINDIG LICHAAM.

Laat K een eindig lichaam zijn. Voor een positief geheel getal n geven we de som $1 + 1 + \ldots + 1$, die uit n termen 1 bestaat, aan met $\overline{n}$; dit is een element van K. Verder zetten we $\overline{0} = 0 \in K$. kennelijk geldt

$$\overline{n} + \overline{m} = \overline{n + m}$$

$$\overline{n} \cdot \overline{m} = \overline{n \cdot m}.$$

Aangezien K eindig is zijn er gehele getallen n, m met

$$n > m \geq 0, \qquad \overline{n} = \overline{m}$$

dus

$$n - m > 0. \qquad \overline{n - m} = 0$$

Zij p het kleinste positieve gehele getal met $\overline{p} = 0$. We tonen aan dat p een priemgetal is. Stel namelijk $p = a \cdot b$ met $0 < a < p$ en $0 < b < p$, dan

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b} = \overline{p} = 0, \qquad \overline{a} \neq 0, \ \overline{b} \neq 0$$

en dit is een tegenspraak daar in een lichaam een product alleen 0 is als een der factoren 0 is. Verder $p \neq 1$ want $\overline{1} \neq 1$ want $\overline{1} = 1 \neq 0$.

De deelverzameling $D = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\} \subset K$ bevat kennelijk p verschillende elementen, en de optelling en vermenigvuldiging in D worden gegeven door

$$\overline{n} + \overline{m} = \overline{n + m} = \overline{s}, \text{ waar}$$

$$s = (\text{rest van } n + m \text{ bij deling door } p),$$

$$\overline{n} \cdot \overline{m} = \overline{t}, \text{ waar}$$

$$t = (\text{rest van } n \cdot m \text{ bij deling door } p).$$

Hieruit volgt dat D met de optelling en vermenigvuldiging van K zelf een lichaam vormt, dat isomorf is met het in §1 gedefinieerde lichaam $\mathbb{F}_p$.

CONCLUSIE: elk eindig lichaam K bevat een deellichaam isomorf met $\mathbb{F}_p$, voor

zeker priemgetal p. Men noemt p de *karakteristiek* van K.

In het vervolg zullen we $\mathbb{F}_p$ zelf als deellichaam van K beschouwen, d.w.z. we identificeren $\mathbb{F}_p$ en D.

Met behulp van lineaire algebra bewijzen we nu dat het aantal elementen van K gelijk is aan p^n, voor zekere $n \geq 1$. Noem elementen $a_1,\ldots,a_k$ uit K *lineair onafhankelijk over* $\mathbb{F}_p$ als

$$c_1 \cdot a_1 + c_2 \cdot a_2 + \ldots + c_k \cdot a_k \neq 0$$

voor alle $c_1,\ldots,c_k \in \mathbb{F}_p$, behalve voor $c_1 = c_2 = \ldots = c_k = 0$. Zij nu $\{a_1,\ldots,a_n\} \subset K$ lineair onafhankelijk over $\mathbb{F}_p$ met n zo groot mogelijk. Men gaat dan eenvoudig na dat $\{a_1,\ldots,a_n\}$ een *basis* van K over $\mathbb{F}_p$ is, dat wil zeggen: elke $b \in K$ kan op precies één manier geschreven worden als

$$b = c_1 \cdot a_1 + c_2 \cdot a_2 + \ldots + c_n \cdot a_n, \quad \text{met} \quad c_1,\ldots,c_n \in \mathbb{F}_p .$$

Aangezien elke coëfficient c_1 precies p waarden kan aannemen zijn er p^n mogelijkheden voor b, dus K heeft p^n elementen.
Hiermee is de eerste bewering van stelling 1 bewezen.

3. IRREDUCIBELE POLYNOMEN OVER EEN EINDIG LICHAAM.

Zij K een eindig lichaam. Met K[X] geven we de verzameling polynomen in X met coëfficienten uit K aan; dit zijn uitdrukkingen van het type

(3.1) $$f = c_0 + c_1 \cdot X + c_2 \cdot X^2 + \ldots + c_k \cdot X^k, \text{ met } c_0,\ldots,c_k \in K,\ k \geq 0;$$

hier moet men X niet als een variabele zien maar als een formeel symbool. Twee polynomen worden op de gebruikelijke wijze opgeteld en vermenigvuldigd; in $\mathbb{F}_5[X]$ geldt bijvoorbeeld

$$(1 + 2X) + (4 + X + 3X^2) = 3X + 3X^2$$

$$(1 + 2X) \cdot (4 + X + 3X^2) = 4 + 4X + X^3.$$

Merk op dat K[X] géén lichaam is: de meeste polynomen hebben geen inverse.

Als in (3.1) geldt $c_k \neq 0$ dan noemen we k de *graad* van f, notatie gr(f), en c_k heet dan de *kopcoëfficient* van f. Het nulpolynoom (d.w.z.: alle $c_i = 0$) heeft geen kopcoëfficient en graad $-\infty$. Een polynoom met kopcoëfficient 1 heet *monisch*. Een polynoom van graad >0 heet *irreducibel* als het niet geschreven kan worden als product van twee polynomen die elk een lagere graad hebben.

Met behulp van een staartdeling kan men bij elk tweetal polynomen f en g, met $g \neq 0$, een *quotiënt* $h \in K[X]$ en een *rest* $r \in K[X]$ bepalen waarvoor geldt $f = h.g + r$ en $gr(r) < gr(g)$. Uitgaande van deze delingsalgoritme kan men, geheel analoog aan het geval van de gehele getallen, de "stelling van de eenduidige priemfactorontbinding" bewijzen:
elk monisch polynoom uit K[X] kan geschreven worden als product van een eindig aantal monische *irreducibele* polynomen uit K[X], en deze schrijfwijze is eenduidig op de volgorde der factoren na. (De beperking tot *monische* polynomen komt overeen met de beperking tot *positieve* gehele getallen)

We zijn nu geinteresseerd in het *aantal* monische irreducibele polynomen van gegeven graad n in K[X]. De overeenkomstige vraag voor de gehele getallen ("hoeveel priemgetallen zijn er onder een gegeven grens?") pleegt men te benaderen met behulp van de zeta-functie van Riemann:

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}, \qquad s \in \mathbb{R}, \quad s>1;$$

de "clou" van deze benadering is de productontwikkeling

$$\sum_{n=1}^{\infty} n^{-s} = \prod_{p} (1 + p^{-s} + p^{-2s} + p^{-3s} + \ldots) \tag{3.2}$$

(het product rechts loopt over alle priemgetallen p) die men bewijst door het product uit te werken en op te merken dat de stelling van de eenduidige priemfactorontbinding garandeert, dat men dan voor elk positief geheel getal n één term n^{-s} krijgt. Men kan (3.2) dus beschouwen als een analytische vertaling van de stelling van de eenduidige priemfactorontbinding.

Hetzelfde idee voert voor K[X] veel sneller tot het doel. Zij k een reële variabele en beschouw het oneindige product

$$\prod_f (1 + t^{gr(f)} + t^{2gr(f)} + t^{3gr(f)} + \ldots)$$

waar f loopt over alle monische irreducibele polynomen in K[X].
Het is niet moeilijk te bewijzen dat het product convergeert voor $|t| < \frac{1}{q}$, waar q het aantal elementen van K is (gebruik dat er hoogstens q^k monische irreducibele polynomen van de graad k in K[X] zijn). Werkt men het product uit dan vindt men analoog aan (3.2)

$$(3.3) \qquad \prod_f (1 + t^{gr(f)} + t^{2gr(f)} + \ldots) = \sum_g t^{gr(g)}$$

waar g loopt over alle monische polynomen in K[X]. Het aantal monische polynomen $g = c_0 + c_1X + \ldots + c_{n-1}X^{n-1} + X^n$ van graad n is q^n, want voor elke c_i zijn er q mogelijkheden. Dus

$$\sum_g t^{gr(g)} = \sum_{n=0}^{\infty} q^n t^n = \frac{1}{1 - qt}$$

Definiëren we

x(k) = (aantal monische irreducibele polynomen van graad k in K[X])

dan vinden we voor het linkerlid van (3.3):

$$\prod_f \frac{1}{1 - t^{gr(f)}} = \prod_{k=1}^{\infty} \left(\frac{1}{1 - t^k}\right)^{x(k)}$$

dus (3.3) wordt

$$\prod_{k=1}^{\infty} \left(\frac{1}{1 - t^k}\right)^{x(k)} = \frac{1}{1 - qt}$$

en hieruit moeten we x(k) oplossen.

Neem aan beide zijden de logaritmische afgeleide (d.w.z.: eerst de logaritme, en dan de afgeleide naar t), dan vinden we

$$-\sum_{k=1}^{\infty} x(k) \cdot \frac{k.t^{k-1}}{1 - t^k} = \frac{-q}{1 - q^t}$$

dus

$$\sum_{k=1}^{\infty} k.x(k).\frac{t^k}{1 - t^k} = \frac{qt}{1 - qt} = \sum_{n=1}^{\infty} q^n t^n.$$

Het linker lid is gelijk aan

$$\sum_{k=1}^{\infty} (k.x(k). \sum_{j=1}^{\infty} t^{jk}) = \sum_{n=1}^{\infty} (\sum_{k|n} k.x(k))\ t^n$$

(hier is jk vervangen door n; met $\sum_{k|n}$ bedoelen we sommatie over de positieve gehele getallen k die een deler van n zijn). We concluderen

$$\sum_{n=1}^{\infty} (\sum_{k|n} k.x(k))\ t^n = \sum_{n=1}^{\infty} q^n t^n, \quad \text{voor } t \in \mathbb{R}, \ |t| < \frac{1}{q},$$

en een coëfficientenvergelijking levert

$$\sum_{k|n} k.x(k) = q^n, \qquad \text{voor } n \geq 1. \tag{3.4}$$

Hieruit volgt kennelijk $n.x(n) \leq q^n$, dus

$$n.x(n) = q^n - \sum_{k\ n,\ k \neq n} k.x(k) \geq q^n - \sum_{k=1}^{n-1} k.x(k)$$

$$\geq q^n - \sum_{k=1}^{n-1} q^k = q^n - \frac{q^n - q}{q - 1} > 0 \quad ,$$

oftewel $x(n) > 0$,

(3.5) CONCLUSIE. Zij K een eindig lichaam en $n \geq 1$ een geheel getal. Dan bevat K[X] tenminste één monisch irreducibel polynoom van de graad n.

We merken nog op dat men met behulp van de "omkeerformule van Moebius" uit (3.4) de volgende uitdrukking voor x(n) kan afleiden:

$$x(n) = \frac{1}{n} \sum_{k|n} \mu(\tfrac{n}{k})\, q^k$$

waar μ de *Moebiusfunctie* is:

$\mu(1) = 1$

$\mu(p_1 \ldots p_r) = (-1)^r$ als $p_1, \ldots, p_r$ verschillende priemgetallen zijn,

$\mu(m) = 0$ voor andere m.

In het bijzonder:

$x(1) = q$ $\qquad$ $x(4) = (q^4 - q^2)/4$

$x(2) = (q^2 - q)/2$ $\qquad$ $x(5) = (q^5 - q)/5$

$x(3) = (q^3 - q)/3$ $\qquad$ $x(6) = (q^6 - q^3 - q^2 + q)/6$

VOORBEELD. Voor $K = \mathbb{F}_2$ vinden we:

n	x(n)	irreducibele polynomen van de graad n.
1	2	X, $1 + X$
2	1	$1 + X + X^2$
3	2	$1 + X + X^3$, $1 + X^2 + X^3$
4	3	$1 + X + X^4$, $1 + X^3 + X^4$, $1 + X + X^2 + X^3 + X^4$.

4. CONSTRUCTIE VAN EINDIGE LICHAMEN.

In deze paragraaf bewijzen we de twee laatste uitspraken van stelling 1. We maken daarbij gebruik van de resultaten van paragraaf 3. We merken op dat men uitgaande van de theorie der splijtlichamen een veel korter

bewijs kan geven (vgl. §5).

In paragraaf 1 hebben we het lichaam $\mathbb{F}_p$ geconstrueerd door *gehele getallen* modulo een *priemgetal* te beschouwen. Geheel analoog hieraan gaan we nu een lichaam van *polynomen* modulo een *irreducibel polynoom* construeren.

Laat K een eindig lichaam zijn, en $f \in K[X]$ een irreducibel polynoom van de graad k. Het "lichaam K[X] modulo f", notatie $K[X]/(f)$, is de verzameling

$$\{c_0 + c_1.x + \ldots + c_{k-1}.x^{k-1} \mid c_0,\ldots,c_{k-1} \in K\} =$$
$$= \{g(x) \mid g \in K[X],\ gr(g) < k\}$$

waarin men twee elementen optelt en vermenigvuldigt als gewone polynomen, behalve dat men de uitkomst steeds vervagt door de rest bij deling door f. Bovendien hebben we X door x vervangen, om verwarring tussen elementen van K[X] en van $K[X]/(f)$ te voorkomen.

Evenals in paragraaf 1 is na te gaan dat op deze manier inderdaad een lichaam verkregen wordt; de voorwaarde "f is irreducibel" garandeert weer het bestaan van inversen. Het aantal elementen van dit lichaam is q^k, als q het aantal elementen van K is.

De tweede bewering van stelling 1 is nu gemakkelijk te bewijzen: zij p een priemgetal en $n \geq 1$ een geheel getal; wegens (3.5) bestaat er een irreducibel polynoom $f \in \mathbb{F}_p[X]$ van de graad n, dus bovenstaande constructie (met $K = \mathbb{F}_p$) levert ons het verlangde lichaam met p^n elementen.

VOORBEELD: $p^n=4$. Hier hebben we een irreducibel polynoom $f \in \mathbb{F}_2[X]$ van graad 2 nodig. Er is slechts één zo'n polynoom, nl. $f = 1 + X + X^2$, zie §3. Een lichaam van vier elementen wordt dus gevormd door {0, 1, x, 1+x} met de volgende optel- en vermenigvuldigtabel:

+	0	1	x	1+x
0	0	1	x	1+x
1	1	0	1+x	x
x	x	1+x	0	1
1+x	1+x	x	1	0

×	0	1	x	1+x
0	0	0	0	0
1	0	1	x	1+x
x	0	x	1+x	1
1+x	0	1+x	1	x

VOORBEELD $p^n = 9$. Een monisch irreducibel polynoom van graad 2 in $\mathbb{F}_3[X]$ is $1 + X^2$ (er zijn nog twee andere). De verzameling $\{a + b.x \mid a, b \in \mathbb{F}_3\}$ is een lichaam van 9 elementen, met de volgende optelling en vermenigvuldiging:

$$(a + b.x) + (c + d.x) = (a + b) + (c + d).x$$

$$(a + b.x) \,.\, (c + d.x) = (ac - bd) + (ad + bc).x$$

voor $a, b, c, d \in \mathbb{F}_3$. Merk op dat deze complexe getallen $a + bi$ en $c + di$, met $a, b, c, d \in \mathbb{R}$, op dezelfde manier opgeteld en vermenigvuldigd worden.

Laat K een eindig lichaam van karakteristiek p zijn (d.w.z. $\mathbb{F}_p \subset K$) en $a \in K$ een vast gekozen element. Als $f = \sum_{i=0}^{k} c_i X^i \in \mathbb{F}_p[X]$ een polynoom is dan wordt met $f(a)$ het element $\sum_{i=0}^{k} c_i a^i$ van K bedoeld. Omdat K eindig is zijn er zeker twee polynomen $f_1 \neq f_2$ in $\mathbb{F}_p[X]$ met $f_1(a)=f_2(a)$, dus er is ook een polynoom $f \in \mathbb{F}_p[X]$, $f \neq 0$, met $f(a) = 0$ (namelijk $f = f_1 - f_2$). Deel f door zijn kopcoëfficient, dan mogen we aannemen dat f monisch is. Onder alle monische polynomen $f \in \mathbb{F}_p[X]$ met $f(a) = 0$ noemen we degeen die de *kleinste* graad heeft het *kanonieke polynoom van* a *over* $\mathbb{F}_p$. Het is gemakkelijk in te zien dat er niet *twee* monische polynomen $g_1 \neq g_2$ van minimale graad zijn met $g_1(a) = g_2(a) = 0$: immers, $g = (g_1 - g_2)/(\text{kopcoëfficient})$ zou een nog lagere graad hebben.

Zij $f \in \mathbb{F}_p[X]$ het kanonieke polynoom van a over $\mathbb{F}_p$, en $k = gr(f)$. We noemen k de *graad* van a over $\mathbb{F}_p$; deze is ≥ 1. Het polynoom f is *irreducibel*, want uit $f = g.h$, met $gr(g) < k$ en $gr(h) < k$, zou de tegenspraak

$$g(a).h(a) = f(a) = 0, \qquad g(a) \neq 0, \quad h(a) \neq 0$$

volgen.

De deelverzameling

$$\{g(a) \mid g \in \mathbb{F}_p[X], \; gr(g) < k\} =$$
$$= \{c_0 + c_1.a + \ldots + c_{k-1}.a^{k-1} \mid c_0, \ldots, c_{k-1} \in \mathbb{F}_p\} \subset K$$

heeft kennelijk precies p^k elementen, en de optelling en vermenigvuldiging worden in deze deelverzameling gegeven door

$g(a) + h(a) = s(a)$, waar

$s = (\text{rest van } g + h \text{ bij deling door } f) \in \mathbb{F}_p[X]$,

$g(a).h(a) = t(a)$, waar

$t = (\text{rest van } g.h \text{ bij deling door } f) \in \mathbb{F}_p[X]$.

We zien dus dat deze deelverzameling zelf een lichaam vormt, dat isomorf is met het lichaam $\mathbb{F}_p[X]/(f)$.

(4.1) CONCLUSIE Zij K een eindig lichaam van karakteristiek p, en $a \in K$. Zij f het kanonieke polynoom van a over $\mathbb{F}_p$, van graad k. Dan bevat K een deellichaam van p^k elementen

$$\{c_0 + c_1.a + \ldots + c_{k-1}.a^{k-1} \mid c_0,\ldots,c_{k-1} \in \mathbb{F}_p\}$$

dat isomorf is met het lichaam $\mathbb{F}_p[X]/(f)$. We geven dit deellichaam aan met $\mathbb{F}_p(a)$.

Zij p^n het aantal elementen van K. Als in paragraaf 2 kunnen we nu een *basis* $\{a_1,\ldots,a_m\}$ van K over $\mathbb{F}_p(a)$ vormen. Het aantal elementen van K blijkt dan $(p^k)^m = p^{km}$ te zijn; dus $p^n = p^{km}$. en k is een deler van n.

(4.2) CONCLUSIE. Zij K een eindig lichaam met p^n elementen, en $a \in K$. Dan is er een irreducibel monisch polynoom $f \in \mathbb{F}_p[X]$, waarvan de graad k een deler van n is, met $f(a) = 0$.

Een gegeven polynoom $f \in \mathbb{F}_p[X]$ van graad k kan echter niet meer dan k nulpunten hebben. Dus (4.2) impliceert dat het aantal elementen van K niet groter kan zijn dan

$$\sum_{k \mid n} k.\ (\text{aantal monische irreducibele } f \in \mathbb{F}_p[X] \text{ van graad } k)$$

oftewel

$$(4.3) \qquad p^n \leq \sum_{k \mid n} k.x(k)$$

met

$$x(k) = (\text{aantal monische irreducibele } f \in \mathbb{F}_p[X] \text{ van graad } k).$$

Volgens (3.4) (met $q = p$, want $\mathbb{F}_p$ heeft p elementen) geldt in (4.3) het gelijkheidsteken. Dat betekent dat we de redenering kunnen omdraaien, en we vinden:

(4.4) CONCLUSIE. Zij k een eindig lichaam met p^n elementen. Dan heeft elk monisch irreducibel polynoom $f \in \mathbb{F}_p[X]$, waarvan de graad k een deler van n is, k verschillende nulpunten in K. Bovendien is f het kanonieke polynoom van elk dezer nulpunten over $\mathbb{F}_p$.

Hiermee kunnen we de laatste bewering van stelling 1 direct bewijzen. Laten K en K' twee lichamen zijn die allebei p^n elementen hebben. Zij $f \in \mathbb{F}_p[X]$ monisch en irreducibel van graad n (zo'n f bestaat wegens (3.5)). Wgens (4.4) zijn er elementen $a \in K$ en $a' \in K'$ die allebei f als kanoniek polynoom over $\mathbb{F}_p$ hebben. De deellichamen $\mathbb{F}_p(a) \subset K$ en $\mathbb{F}_p(a') \subset K'$ hebben wegens (4.1) elk p^n elementen, dus moeten gelijk zijn aan K resp. K'. Oftewel: K en K' zijn beide isomorf met het lichaam $\mathbb{F}_p[X]/(f)$, dus ook isomorf met elkaar. Hiermee is stelling 1 volledig bewezen.

Een lichaam met q elementen (q een macht van een priemgetal) geeft men aan met $\mathbb{F}_q$. Uit (4.4) volgt gemakkelijk dat $\mathbb{F}_r$ isomorf is met een deellichaam van $\mathbb{F}_q$ dan en slechts dan als q een macht van r is.

Uit onze benadering volgt ook direct de "stelling van het primitieve element" voor eindige lichamen: elk eindig lichaam $\mathbb{F}_q$ van karakteristiek p bevat een element a met $\mathbb{F}_q = \mathbb{F}_p(a)$.

5. PRIMITIEVE WORTELS.

Zij $\mathbb{F}_q$ een eindig lichaam, en $a \in \mathbb{F}_q$, $a \neq 0$. Als b de elementen van $\mathbb{F}_q$ ongelijk aan 0 doorloopt, doet a.b dat ook, alleen niet noodzakelijk in dezelfde volgorde. Hier volgt uit

$$\prod_{b\neq 0} b = \prod_{b\neq 0} (a.b)$$

(beide producten lopen over alle elementen $b \neq 0$ van $\mathbb{F}_q$). Deel aan beide zijden door $\prod_{b\neq 0} b$, dan vinden we

$$1 = a^{q-1}, \qquad \text{voor } a \neq 0,$$

dus

(5.1) $\qquad a^q = a \quad$ voor alle $a \in \mathbb{F}_q \quad$ (ook voor $a = 0$).

Het polynoom $X^q - X$ heeft dus alle elementen van $\mathbb{F}_q$ als nulpunten. Omdat $X^q - X$ graad q heeft volgt hieruit de formule

(5.2) $\qquad X^q - X = \prod_a (X - a)$

(in $\mathbb{F}_q[X]$). Hier loopt a over alle elementen van $\mathbb{F}_q$.

VOORBEELD. Toegepast op het lichaam $\mathbb{F}_p$ levert (5.1) de "kleine stelling van Fermat": $n^p - n$ is deelbaar door p voor elk geheel getal n en elk priemgetal p. Bijvoorbeeld $2^7 - 2 = 7 \times 18$.
Voor $\mathbb{F}_p$ levert (5.2), gedeeld door X:

$$X^{p-1} - 1 = \prod_{i=1}^{p-1} (X - i) \qquad (\text{in } \mathbb{F}_p[X]).$$

Vergelijking van de constante coëfficient geeft de "stelling van Wilson": $(p - 1)\,! \equiv -1 \bmod p$, voor p priem. Voorbeeld: $6! + 1 = 7 \times 103$.

STELLING 2. *Elk eindig lichaam* $\mathbb{F}_p$ *bevat een "primitieve wortel", d.w.z. een element* $a \neq 0$ *zodanig dat elk element* $b \in \mathbb{F}_q$ *een macht van* a *is:* $b = a^n$ *voor zeker geheel getal* n.

Voor het bewijs van deze stelling hebben we het begrip *orde* nodig. We zeggen dat een element $b \neq 0$ orde d heeft, als $b^d = 1$ terwijl $b^i \neq 0$ voor $1 \leq i \leq d-1$; hier is d een positief geheel getal. Het is niet moeilijk in te zien dat b een nulpunt van $X^t - 1$ is dan en slechts dan als de

orde van b een *deler* van t is. Aangezien elke $b \in \mathbb{F}_q$, $b \neq 0$, een nulpunt van $X^{q-1} - 1$ is, volgt

$$\text{orde } (b) \text{ deelt } q - 1, \qquad \text{voor alle } b \in \mathbb{F}_q,\ b \neq 0.$$

Voor een deler d van $q - 1$ definiëren we:

$$y(d) = (\text{aantal } b \in \mathbb{F}_q,\ b \neq 0, \text{ met orde } (b) = d).$$

Dan geldt

$$\sum_{d \mid q-1} y(d) = q - 1,$$

en algemener, als t een deler is van $q - 1$:

$$\sum_{d \mid t} y(d) = (\text{aantal nulpunten van } X^t - 1 \text{ in } \mathbb{F}_q) = t,$$

de laatste gelijkheid omdat $X^t - 1$ een deler is van het polynoom $X^{q-1} - 1 = \prod_{a \neq 0} (X - a)$. Zetten we

$$z(d) = (\text{ aantal } b \in \mathbb{C},\ b \neq 0, \text{ met orde } (b) = d)$$

($\mathbb{C}$ is het lichaam der complexe getallen) dan vinden we evenzo

$$\sum_{d \mid t} z(d) = (\text{aantal nulpunten van } X^t - 1 \text{ in } \mathbb{C}) = t$$

want $X^t - 1$ heeft in $\mathbb{C}$ de t nulpunten $e^{2\pi ij/t}$, $j = 1, 2, \ldots, t$.
We concluderen

$$\sum_{d \mid t} y(d) = \sum_{d \mid t} z(d), \qquad \text{voor elke deler t van } q - 1.$$

Hieruit leidt men met inductie naar t direct af

$$y(t) = z(t), \qquad \text{voor elke deler } t \text{ van } q - 1.$$

In het bijzonder

$$y(q - 1) = z(q - 1).$$

Maar $z(q - 1) \geq 1$, want $e^{2\pi i/(q-1)}$ is een complex getal van orde $q - 1$. Dus er geldt ook $y(q - 1) \geq 1$, oftewel: $\mathbb{F}_q$ bevat een element $a \neq 0$ van orde $q - 1$. Voor deze a moeten de $q - 1$ elementen $1, a, a^2, \ldots, a^{q-2}$ alle verschillend zijn, dus

$$\{1, a, a^2, \ldots, a^{q-2}\} = \{b \in \mathbb{F}_q \mid b \neq 0\}$$

Hiermee is stelling 2 bewezen.

VOORBEELD: $\mathbb{F}_7$ heeft de primitieve wortel 3, want

$$1 = 3^0, \quad 2 = 3^2, \quad 3 = 3^1, \quad 4 = 3^4, \quad 5 = 3^5, \quad 6 = 3^3$$

in $\mathbb{F}_7$. Ook 5 is een primitieve wortel in $\mathbb{F}_7$.

OPMERKING. Uit (5.2) is gemakkelijk in te zien dat $\mathbb{F}_q$ het splijtlichaam van $X^q - X$ over $\mathbb{F}_p$ is, als $q = p^n$. Dit is in feite de gebruikelijke manier om het lichaam $\mathbb{F}_q$ te construeren, en de eenduidigheid ervan te bewijzen. We verwijzen hiervoor naar de leerboeken (van der Waerden, Algebra I).

6. GALOISTHEORIE VOOR EINDIGE LICHAMEN.

Zij $\mathbb{F}_q$ een eindig lichaam van karakteristiek p. Voor alle $a \in \mathbb{F}_p$ geldt wegens (5.1)

$$(a + 1)^p = a + 1 = a^p + 1$$

dus het polynoom

$$(X + 1)^p - X^p - 1 \in \mathbb{F}_q[X]$$

heeft de p elementen van $\mathbb{F}_p$ als nulpunten. Maar de graad van het polynoom is kennelijk kleiner dan p. Dit is alleen mogelijk als we met het nulpolynoom te maken hebben, dus

$$(X + 1)^p = X^p + 1.$$

Substitueer nu $\frac{a}{b}$ voor X, met $a, b \in \mathbb{F}_q$, $b \neq 0$, en vermenigvuldig met b^p, dan vinden we

$$(a + b)^p = a^p + b^p,$$

een formule die natuurlijk ook voor b = 0 geldt. Ook

$$(a.b)^p = a^p.b^p,$$

dus de afbeelding $F : \mathbb{F}_q \to \mathbb{F}_q$, gedefiniëerd door $F(x) = x^p$, respecteert zowel de optelling als de vermenigvuldiging. Verder is F een 1-1-afbeelding want uit $a^p = b^p$ volgt $(a - b)^p = a^p - b^p = 0$ dus a = b. We concluderen dat F een *automorfisme* van $\mathbb{F}_q$ is, het zogenaamde *Frobeniusautomorfisme*.
Er volgt ook dat elk element van $\mathbb{F}_q$ een p-de macht is: eindige lichamen zijn *volkomen*.

STELLING 3. *Zij* $\mathbb{F}_q$ *een eindig lichaam van karakteristiek* p, *met* $q = p^n$. *Dan heeft* $\mathbb{F}_q$ *precies* n *automorfismen, namelijk de machten van* F:

$$F^i(x) = x^{(p^i)}, \qquad 0 \leq i < n.$$

BEWIJS. Uit het voorgaande volgt direct dat F^i voor alle i een automorfisme van $\mathbb{F}_q$ is. Verder $F^i \neq F^j$ voor $0 \leq i < j < n$, want het polynoom $X^{p^j} - X^{p^i}$ kan wegens $p^j < q$ niet alle elementen van $\mathbb{F}_q$ als nulpunten hebben. Rest te bewijzen dat dit alle automorfismen zijn.

Zij G een automorfisme van $\mathbb{F}_q$, en a een primitieve wortel (stelling 2). Dan geldt $G(a) = a^m$ voor zekere m met $1 \le m \le q-1$. Elk element $x \neq 0$ uit $\mathbb{F}_q$ is een macht a^j van a, dus

$$G(x) = G(a^j) = G(a)^j = a^{mj} = x^m.$$

Schrijven we $m = \ell.p^i$, met $(\ell,p) = 1$ en $0 \le i \le n-1$, dan vinden we voor alle $x \in \mathbb{F}_q$

$$G(x) = x^{(\ell.p^i)} = F^i(x^\ell).$$

Omdat G en F^i automorfismen zijn volgt

$$F^i(x^\ell + 1) = F^i(x^\ell) + F^i(1) = G(x) + G(1)$$
$$= G(x + 1) = F^i((x + 1)^\ell)$$

en omdat F^i 1-1 is concluderen we

$$x^\ell + 1 = (x + 1)^\ell, \qquad \text{voor alle } x \in \mathbb{F}_q.$$

Het polynoom

$$(X + 1)^\ell - X^\ell - 1$$

heeft dan meer nulpunten dan zijn graad, dus moet het nulpolynoom zijn. Voor $\ell = 1$ klopt dit, en in dit geval geldt $G = F^i$, zoals verlengd. Het geval $\ell > 1$ treedt niet op, want net binomium van Newton levert

$$(X + 1)^\ell - X^\ell - 1 = \overline{\ell}.X^{\ell-1} + (\text{lagere graads termen}) \in \mathbb{F}_p[X]$$

voor $\ell > 1$, en dit is wegens $(\ell,p) = 1$ niet het nulpolynoom. Hiermee is stelling 3 bewezen. □

Is $\mathbb{F}_r \subset \mathbb{F}_q$ een deellichaam, met $r = p^k$ en $k|n$, dan bestaat $\mathbb{F}_r$ precies uit de nulpunten van $X^{p^k} - X$ in $\mathbb{F}_q$, en hieruit volgt dat F^i beperkt

tot $\mathbb{F}_r$ gelijk is aan de identieke afbeelding dan en slechts dan als i deelbaar is door k.

De zogenaamde "hoofdstelling van de Galoistheorie" laat zich aan de hand van bovenstaande gegevens voor het geval van eindige lichamen direct verifiëren.

7. EEN COMBINATORISCH PROBLEEM.

Eindige lichamen bewijzen hun nut in de getaltheorie en de combinatoriek. In paragraaf 5 hebben we een paar toepassingen in de getaltheorie gezien, in deze paragraaf zullen we een combinatorisch probleem oplossen met behulp van een eindig lichaam.

Stel dat men elk van de vijftien zijden en diagonalen van een zeshoek in één van de kleuren rood en blauw trekt. Dan zijn er onder die 15 lijnstukken drie van dezelfde kleur die een driehoek vormen, zoals men gemakkelijk bewijst. Bovendien is dit het best mogelijke resultaat, want het is niet lastig de 10 zijden en diagonalen van een *vijf*hoek elk rood of blauw te kleuren zonder dat er een dergelijke zgn "monochromatische driehoek" ontstaat: kleur de zijden rood en de diagonalen blauw.

Voor *drie* kleuren ligt de zaak iets lastiger. Trekt men elk van de 136 zijden en diagonalen van de zeventienhoek in een der kleuren geel, rood en blauw, dan ontstaat weer een monochromatische driehoek; zie Pythagoras, jaargang 12, pp. 136-137. Maar het is hier veel minder duidelijk dat dit resultaat niet verbeterd kan worden. We staan dus voor het probleem om de zijden en diagonalen van een *zestienhoek* elk geel, blauw of rood te kleuren zodanig dat er onder die 120 lijnstukken geen drie van dezelfde kleur zijn die de drie zijden van een driehoek zijn.

Bij de oplossing maken we gebruik van het lichaam $\mathbb{F}_{16}$. Een irreducibel monisch polynoom van de graad 4 in $\mathbb{F}_2[X]$ wordt gegeven door $f = 1 + X + X^2 + X^3 + X^4$ (zie §3). Wegens (4.4) bevat $\mathbb{F}_{16}$ een element x waarvan het kanonieke polynoom over $\mathbb{F}_2$ gelijk is aan f, en $\mathbb{F}_{16}$ is isomorf met het lichaam $\mathbb{F}_2[X]/(f)$: elk element van $\mathbb{F}_{16}$ kan op precies één manier worden geschreven als $c_0 + c_1.x + c_2.x^2 + c_3.x^3$, met $c_i \in \mathbb{F}_2$. Bij wijze van korte notatie geven we dit element aan met $c_0c_1c_2c_3$ (een soort "x-tallig stelsel"); bijvoorbeeld 0 = 0000, 1 = 1000, x = 0100.

Merk op dat in $\mathbb{F}_{16}$ geldt $1 + 1 = 0$, dus ook $a + a = (1 + 1).a = 0.a = 0$ voor alle $a \in \mathbb{F}_{16}$, oftewel $a = -a$: "plus" en "min" vallen samen.

Zij $H \subset \mathbb{F}_{16}$ da verzameling machten van x:

$$x = 0100$$
$$x^2 = 0010$$
$$x^3 = 0001$$
$$x^4 = 1 + x + x^2 + x^3 = 1111$$
$$x^5 = 1000 = 1.$$

De orde van x is 5; dit klopt met §5, want 5 deelt 16 - 1 = 15.
Laat $a = 1 + x = 1100$, en zij $aH = \{a.h \mid h \in H\}$; de elementen van aH zijn 0110, 0011, 1110, 0111 en 1100. Tenslotte zetten we $b = 1 + x^2 = 1010$ en $bH = \{b.h \mid h \in H\} = \{0101, 1101, 1001, 1011, 1010\}$.
De drie verzamelingen H, aH en bH bevatten samen 15 elementen. Elk element $\neq 0$ van $\mathbb{F}_{16}$ zit dus in precies één der verzamelingen H, aH en bH.

Beschouw nu een zestienhoek waarvan de hoekpunten genummerd zijn met de elementen van $\mathbb{F}_{16}$. De zijden en diagonalen van deze zestienhoek kleuren we als volgt: als $s, t \in \mathbb{F}_{16}$ twee verschillende hoekpunten zijn, dan $s + t = s - t \neq 0$, dus $s + t$ zit in precies één der verzamelingen H, aH en bH; kleur nu het lijnstuk van s naar t *geel* als $s + t \in H$, *blauw* als $s + t \in aH$, en *rood* als $s + t \in bH$. De kant van 1100 naar 0101 wordt dus rood, want $1100 + 0101 = 1001 \in b.H$.

We beweren dat er zo geen monochromatische driehoek ontstaat. Een manier om dit te bewijzen is de zestienhoek volledig te tekenen en elk van de 560 driehoeken te controleren. Iets sneller is de volgende manier. Stel dat $s, t, u \in \mathbb{F}_{16}$ de drie hoekpunten van een monochromatische driehoek zijn; dan is er een element $c \in \{1, a, b\}$ zodat $s + t$, $s + u$ en $t + u$ alle drie tot cH behoren: $c = 1$ als de driehoek geel is, $c = a$ als hij blauw is en $c = b$ als hij rood is. Maar de drie elementen $s + t$, $s + u$ en $t + u$ hebben als som

$$(s + t) + (s + u) + (t + u) = (s + s) + (t + t) + (u + u) = 0.$$

Dus cH bevat drie verschillende elementen met som 0. Delen we door c, dan zien we dat ook H drie verschillende elementen met som 0 bevat. Aangezien de som van alle vijf elementen van H nul is:

$$1 + x + x^2 + x^3 + x^4 = 0$$

concluderen we dat de twee overblijvende elementen van H eveneens samen 0 zijn: $x^j + x^i = 0$ voor zekere i,j met $0 \leq i < j \leq 4$. Hieruit volgt $x^j = -x^i = x^i$.
Dit is een tegenspraak, want H bestaat uit vijf *verschillende* elementen. Hiermee is het probleem opgelost. (Vergelijk R.E.Greenwood & A.M.Gleason, Canadien Journal of Mathematics, vol. 7 (1955), pp. 1-7).

Dit voorbeeld is typerend voor het gebruik van eindige lichamen in de combinatoriek: men introduceert een lichaamsstructuur waarvan in de vraagstelling in het geheel niet gerept wordt, om aldus de beschikking te krijgen over methoden uit de algebra.