H12 Eindige lichamen

Def. Een lichaam K heet eindig als $\#K \in \mathbb{N}_{\geq 1}$, oftewel Als K eindig is als verzameling.

Het blijkt dat er niet voor elk eindige getal een eindig lichaam bestaat. Bovendien geldt dat wanneer er een eindig lichaam is met, zeg q, elementen, dat dan dat lichaam op isomorfie na eenduidig bepaald is.

Net zoals met groepen kan men eindige lichamen dus classificeren.

St.12.1

1. Als K een eindig lichaam zou zijn, dan zou moeten volgen dat het een aantal elementen heeft dat een priemmacht is, dwz $\#K = p^n$ voor $p>0$ priem en $n \geq 1$ geheel. Bovendien zou dan $\text{char}(K) = p$ zijn

2. Als $q = p^n$ een priemmacht is zoals hierboven beschreven, d.w.z $n \geq 1$ geheel $p>0$ priem, dan is er een eindig lichaam met p^n elementen. En dit lichaam is op isomorfie na eenduidig bepaald.

— We hebben existentie en eenduidigheid van $\mathbb{F}_p$, p priem, al per constructie $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$

— We willen hiermee zeggen: eindige lichamen bestaan alleen voor priemmachten, en als ze bestaan, dan ligt hun structuur volledig vast door hun aantal elementen!

Bew • 1. Stel K is een eindig lichaam. Dan kan van K het karakteristiek niet 0 zijn, anders zou K een deellichaam K_0 hebben dat isomorf is met $\mathbb{Q}$, maar $\mathbb{Q}$ is oneindig terwijl $K_0 \subset K$ eindig zal zijn.
$\Rightarrow \text{char}(K) = p$ voor p priem. Nu nog aantonen "$\#K = p^n$" voor een $n \geq 1$ geheel.
Omdat K als deellichaam $K_0 \cong \mathbb{F}_p$ bevat, en beide zijn eindig met, zeg $\#K = q$, en we weten $\#K_0 = p$.

volgt dus, wanneer $[K:K_0] = n \geq 1$, ook wel stelling $[K:\mathbb{F}_p] = n$ geschreven, dat er een K_0-basis van n elementen $e_1 .. e_n \in K$ zijn voor K over K_0. Dus elke $\alpha \in K$ correspondeert met een unieke lineaire combinatie $\lambda_1 e_1 + .. + \lambda_n e_n$ op $e_1 .. e_n$ met $\lambda_1 .. \lambda_n \in K_0$ op p^n manieren te kiezen. Elke lineaire combi levert een andere $\alpha \in K$ wegens lineaire onafhankelijkheid, en dit zijn ook alle $\alpha \in K$ wegens opspannendheid $\Rightarrow \# K = p^n$ met $n \geq 1$ $\square$

2. Zij p priem, $n \geq 1$ geheel, en zij $q = p^n$.
We gaan kijken naar het wegens H.11 bestaande ontbichaam van $X^q - X \in \mathbb{F}_p$ over $\mathbb{F}_p$, dus $\Omega_{\mathbb{F}_p}^{X^q - X} =: K$
Als we kunnen laten zien $\# K = q$, zijn we klaar.

We vinden in $K \supseteq \alpha_1 .. \alpha_q$ met $(X^q - X) = \prod_{i=1}^{q} (X - \alpha_i)$
Deze $\alpha_1 .. \alpha_q$ zijn de niet noodzakelijk verschillende q nulpunten van $X^q - X$ in K. noem $A = \{\alpha_1 .. \alpha_n\}$.
We gaan aantonen: (i) $\alpha_i ..$ zijn wel alle verschillend, en $\# A = q$
(ii) A is deellichaam van K

(i) stel $\exists_{i \neq j} \alpha_i = \alpha_j$, dus $X^q - X$ heeft een dubbel nulpunt dan volgt dat $[X^q - X]'(\alpha_i) = 0$, de afgeleide (algebraïsche) van $X^q - X$ in α_i is nul. maar
$\mathbb{F}_p \Rightarrow [X^q - X]' = q \cdot X^{q-1} - 1$ en $q = p^n = 0$ in $\mathbb{F}_p$
dus dit is het -1 polynoom, wat nooit 0 wordt door evaluatie. $\perp$ $\Rightarrow$ alle α_i verschillend, $\# A = q$

(ii) zij $\beta, \gamma \in A$. Dan $\beta^q = \beta$, $\gamma^q = \gamma$. We gaan een algemeen toepasbaar lemma bewijzen voor we verdergaan:

Lemma Zij $\varphi : L \to L$ een homomorfisme van lichamen (endomorfisme). Dan is $FP(\varphi) = \{x \in L : \varphi(x) = x\}$ een deellichaam van L

Bew als eerst: $\varphi(1) = 1$ dus $1 \in FP(\varphi)$. als $x, y \in FP(\varphi)$ dan $\varphi(x) = x$ $\varphi(y) = y$ dus $\varphi(x-y) = \varphi(x) - \varphi(y) = x - y \Rightarrow x - y \in FP(\varphi)$

en als $y \neq 0$ dan $\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1} = xy^{-1} \Rightarrow xy^{-1} \in FP(\varphi)$ □

dit lemma, toegepast op $x \mapsto x^q$, $K \to K$. Dit is omdat $\mathbb{F}_p \subset K$, dus $\mathbb{F}_p$ is priemlichaam van K, het frobeniushomom. n keer toegepast, $F^n : (x \mapsto x^p)^n = x \mapsto x^{p^n} = x^q$ en frobenius was endomorfisme voor lich. met $\text{Char}(K) = p$. Dus we vinden $A = FP(F^n)$ deellichaam van K, met q elementen.

nu moeten we nog aantonen $A = K$. Maar dit is niet zo moeilijk meer. Waarom is dit nodig, als we al een A hebben gevonden dat een lichaam is met q elementen? Omdat we zeker willen zijn dat het echt bestaat. Gelijkheid met een ontb. lichaam $\Omega_{\mathbb{F}_p}^{X^q - X}$ legt dit bestaan onomstotelijk vast.

Omdat $\alpha_1, .. \alpha_q \in A$, volgt $\mathbb{F}_p(\alpha_1, .. \alpha_n) \subset A$, maar dan $\Omega_{\mathbb{F}_p}^{X^q - X} \subset A \subset \Omega_{\mathbb{F}_p}^{X^q - X} \Rightarrow A = \Omega_{\mathbb{F}_p}^{X^q - X}$

— ! Tenslotte nog eenduidigheid. Stel L is ook een lichaam van q elementen dan willen we een isomorfisme $L \cong K := \Omega_{\mathbb{F}_p}^{X^q - X}$ aantonen, oftewel dat L een ontb. lichaam is van $X^q - X$ over $\mathbb{F}_p$.

— $\# L = q = p^n$, dus L heeft $\text{Char}(L) = p$. Zij $L_0 \cong \mathbb{F}_p$ priemlichaam. Verder geldt $\# L^* = q - 1$, en wegens 3.14 is dan elke $\alpha \in L^*$ van orde delend $q-1$, dus $\alpha^{q-1} = 1$, dus $\alpha^q - \alpha = 0$ Dit betekent dat L^* $q-1$ elem. bevat die verschillende nulpunten van $X^q - X \in L[X]$ zijn, en $0 \in L$ voldoet ook. Dus $X^q - X$ heeft alle $\leq q$ de nulpunten (q) in L, dus $X^q - X = \prod_{\alpha \in L} (X - \alpha)$. Er volgt $\Omega_{\mathbb{F}_p}^{X^q - X} \cong \Omega_{L_0}^{X^q - X} \subset L$. Maar elke kleinere verzameling $S \subsetneq L$ heeft minder dan q elementen en mist dus één van de $\alpha \in L$, dus mist een nulpunt van $X^q - X$, dus kan niet $\Omega_{L_0}^{X^q - X}$ zijn.

$\Rightarrow \Omega_{L_0}^{X^q - X} \subsetneq L$ kan niet dus $\Omega_{L_0}^{X^q - X} = L$

$\Rightarrow \Omega_{\mathbb{F}_p}^{X^q - X} \cong L$ □

we schrijven dus op isomorfie na eenduidig $\mathbb{F}_{p^n}$ voor eindige lich.

Gevolg 12.4 Zij q macht v.e. priemgetal p en $q>1$, dan is $\mathbb{F}_q$ het ontbindingslichaam van $X^q - X$ over $\mathbb{F}_p$ en in $\mathbb{F}_q$ geldt $X^q - X = \prod_{\alpha \in \mathbb{F}_q} (X - \alpha)$

Bewijs Dit is gegeven in het voorgaande bewijs:

Stelling 12.5 Voor elke priemmacht $q>1$ is de groep $\mathbb{F}_q^*$ cyclisch met orde $q-1$.

Bew $\# \mathbb{F}_q^* = q-1$ want $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$, en wegens 3.14 is $\mathbb{F}_q^*$ cyclisch. □

Def Een element $\alpha \in \mathbb{F}_q^*$ dat $\mathbb{F}_q^*$ voortbrengt heet een primitieve wortel van $\mathbb{F}_q$ multiplicatieve orde is $q-1$ (niet zomaar een deler van $q-1$ maar $q-1$ zelf).

Stelling 12.6 zij q een priemmacht van p. Dan is er een $\alpha \in \mathbb{F}_q$ met $\mathbb{F}_p(\alpha) = \mathbb{F}_q$.

Bew. neem een existente (wegens 5.12) primitieve wortel α uit $\mathbb{F}_q^*$. Dan volgt $\alpha, \alpha^2, \ldots \alpha^{q-1}, 1 \in \mathbb{F}_p(\alpha)$ en $0 \in \mathbb{F}_p(\alpha)$ dus $\mathbb{F}_q \subset \mathbb{F}_p(\alpha)$, en natuurlijk $\mathbb{F}_p(\alpha) \subset \mathbb{F}_q$ omdat $\alpha \in \mathbb{F}_q$. Dus $\mathbb{F}_p(\alpha) = \mathbb{F}_q$ □

Stelling 12.7 Zij q een priemmacht van p dan is er een monisch irred. polynoom $f \in \mathbb{F}_p[X]$ met $\mathbb{F}_q \cong \mathbb{F}_p[X]/(f)$

Bew neem $\alpha \in \mathbb{F}_q^*$ primitieve wortel en zij $f^{\alpha}_{\mathbb{F}_p}$ het minimumpolynoom, dat is monisch en irreduibel. Wegens g.o.(c) volgt $\mathbb{F}_p(\alpha) \cong \mathbb{F}_p[X]/(f^{\alpha}_{\mathbb{F}_p})$
Dus neem $f = f^{\alpha}_{\mathbb{F}_p}$, dan $\mathbb{F}_q = \mathbb{F}_p(\alpha) \cong \mathbb{F}_p[X]/(f)$ □

Vb realiseer $\mathbb{F}_8$ door : $\mathbb{F}_8 = \mathbb{F}_2[X]/(f)$ waar $f = X^3+X^2+1 \in \mathbb{F}_2[X]$.
schrijf $\alpha := X \bmod (f)$, dan $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$
en elke $p \in \mathbb{F}_8$ schrijven we uniek op de basis $\{1, \alpha, \alpha^2\}$.

Zij nu $\gamma \in \mathbb{F}_8 - \mathbb{F}_2$, dan volgt $\gamma^n = 1 \iff n \mid 8-1, n \neq 1$
$\iff n = 7$. dus elke $\gamma \in \mathbb{F}_8 - \mathbb{F}_2$ is primitieve wortel van $\mathbb{F}_8$.
Dus $\langle \gamma \rangle = \mathbb{F}_8^*$, waaruit via 12.6 volgt $\mathbb{F}_2(\gamma) = \mathbb{F}_8$
voor elke $\gamma \in \mathbb{F}_8 - \mathbb{F}_2$. Maar dan moet gelden voor $f^{\gamma}_{\mathbb{F}_2}$
dat $gr(f^{\gamma}_{\mathbb{F}_2}) = [\mathbb{F}_8 : \mathbb{F}_2] = \log_2(8) = 3$.

Het blijkt dat er maar 2 3degraads irred. mon. pol. zijn over $\mathbb{F}_2$ namelijk X^3+X^2+1 en X^3+X+1

1. als $\gamma^3+\gamma^2+1 = 0$, bekijk dan eens het product in $\mathbb{F}_8[X]$: $(X-\gamma)(X-\gamma^2)(X-\gamma^4) = (X^2-(\gamma+\gamma^2)X+\gamma^3)(X-\gamma^4)$
$= X^3 - (\gamma+\gamma^2+\gamma^4)X^2 + (\gamma^3+\gamma^6+\gamma^5)X + \gamma^7$
opm: $-1 = 1$
we zien $-(\gamma^4+\gamma^2+\gamma) = \gamma(\gamma^3+\gamma^2+1) - \gamma^3 - \gamma^2 = 0 + 1 = 1$
$\gamma^6+\gamma^5+\gamma^3 = \gamma^3(\gamma^3+\gamma^2+1) = 0, \gamma^7 = 1$
dus hier staat precies $f^{\gamma}_{\mathbb{F}_2}$. We hebben daarmee precies de nulpunten van $f^{\gamma}_{\mathbb{F}_2}$ in $\mathbb{F}_8$ gevonden.

2. als $\gamma^3+\gamma+1 = 0$, dan is $(\gamma^2)^3+\gamma^2+1 = \gamma^6+\gamma^2+1$
$= \gamma^3(\gamma^3+\gamma+1) + \gamma^4+\gamma^3+\gamma^2+1 = \gamma(\gamma^3+\gamma+1)+\gamma^3+\gamma+1$
$= 0$, dus ook $f^{\gamma}_{\mathbb{F}_2}(\gamma^2) = 0$. maar dan is
$\gamma^3 = \gamma^2$ ook een nulpunt van $f^{\gamma}_{\mathbb{F}_2}$, dus volgt dat
γ'^2, omdat $\gamma'^2 \notin \mathbb{F}_2$ waar $\gamma'^2 = \gamma^4$ en $7 \nmid 4$, en $\gamma \neq 0$.
dus geldt ook $f^{\gamma}_{\mathbb{F}_2}(\gamma^4) = 0$ door toepassing van
$\gamma' \in \mathbb{F}_8 - \mathbb{F}_2$, $f^{\gamma'}_{\mathbb{F}_2}(\gamma'^8) = 0 \Longrightarrow f^{\gamma'}_{\mathbb{F}_2}(\gamma'^2) = 0$ wat in het voorgaande aangetoond was.
wederom zijn γ, γ^2 en γ^4 steeds de nulpunten van $f^{\gamma}_{\mathbb{F}_2}$ in $\mathbb{F}_8$.

Eindige lichamen van verschillende grootte kunnen (op isomorfie na) in elkaar liggen: onder welke voorwaarden $\mathbb{F}_q \subseteq \mathbb{F}_r$ (op $\cong$ na), gaan we nu uitzoeken.

Stelling 12.9 voor q en r twee priemmachten zijn de volgende drie uitspraken equivalent:

a. $\mathbb{F}_q$ is isomorf met deellichaam van $\mathbb{F}_r$
b. r is een macht van q
c. er is een priemgetal p met $q = p^m$ en $r = p^n$ waarbij $m \mid n$

Bewijs.

b. $\Rightarrow$ c. als $r = q^k$, $k \geq 1$ geheel, dan zij $q = p^m$ voor dus een priem p. we zien dan $q^k = p^{km}$, dus $r = p^{km}$ is de unieke priemontb. van r, en r is een p-macht p^n met $n = km$ dus $m \mid n$.

c. $\Rightarrow$ b. als er een p is met $q = p^m$ en $r = p^n$, $m \mid n$, dan volgt $q = p^m$, $r = p^{km}$ voor $km = n$ in $\mathbb{Z}$, alle ≥ 1 geheel, en daarmee $r = (p^m)^k = q^k$, dus r is een macht van q.

a. $\Rightarrow$ b. $\mathbb{F}_r$ is een e.d. v.r. over $\mathbb{F}_q$ en dus vinden we zoals in 12.1 een basis $\{e_1, \ldots e_n\}$ voor $\mathbb{F}_r$ over $\mathbb{F}_q$ en is $n = [\mathbb{F}_r : \mathbb{F}_q] \geq 1$ geheel, zodat elke $\alpha \in \mathbb{F}_r$ uniek corresponderet met één van de q^n lineaire combinaties $\lambda_1 e_1 + \ldots + \lambda_n e_n$ over $\{e_1 \ldots e_n\}$. Dit bewijst $r = q^n$, $n \geq 1$ geheel.

G. $\Rightarrow$ a. als r een macht is van q (dit is het meest technische deel vd stelling)

Zij M het ontb. lichaam van $(X^q - X)(X^r - X)$ over $\mathbb{F}_p$. En zij $F : M \to M : X \mapsto X^p$ het Frobenius-automorfisme (immers M heeft karakteristiek lichaam $\mathbb{F}_p$, en omdat F injectief is en M eindig, want een eindige uitbr. van een eindig lichaam, is F bijectief, vgl. 8.5)

Omdat alle nulpunten van $X^q - X$, $X^r - X$ ook in M liggen, zijn $\mathbb{F}_r$, $\mathbb{F}_q$ op isomfie na deellichamen van M.

voor $\alpha \in M$ geldt bovendien, omdat $\mathbb{F}_q = \{\alpha \in M : \alpha^q = \alpha\}$ dat $\alpha \in \mathbb{F}_q \iff \alpha^{p^k} = \alpha \iff F^k(\alpha) = \alpha$ en evenzo $\alpha \in \mathbb{F}_r \iff F^m(\alpha) = \alpha$. Zij nu, per aanname, $q = p^k$ en $r = p^m$, dan met $k \mid m$ volgt: $m = dk$ ✓

als $\alpha \in \mathbb{F}_q$ dan $\alpha = F^k(\alpha) = F^k(\underbrace{F^k(\alpha)}_{\text{want } \alpha}) = \dots = F^{dk}(\alpha) = F^m(\alpha) \Rightarrow \alpha \in \mathbb{F}_r$ □

Opm. Als $K \subseteq \mathbb{F}_r$ en $\mathbb{F}_q \cong K$, dan is K ook uniek: het bestaat namelijk uit <u>de</u> q unieke nulpunten van $X^q - X$ in $\mathbb{F}_r$.

Stelling 12.11 zij $q > 1$ priemmacht. en zij $n \geq 1$ geheel. Dan is

$$X^{q^n} - X = \prod_{f \in \mathcal{M}} f \quad \text{in } \mathbb{F}_q[X]$$

waarbij $\mathcal{M}$ de verzameling van monische irreducibele polynomen $f \in \mathbb{F}_q[X]$ is waarbij $gr(f) \mid n$

Bew. **Bekijk de uitbreiding $\mathbb{F}_{q^n} \supset \mathbb{F}_q$. Dat is een uitbreiding wegens St. 12.9. (b. ⇒ a.)**
Er geldt dat $\mathbb{F}_{q^n} = \Omega_{\mathbb{F}_q}^{X^{q^n} - X}$ en voor elke $m \geq 1$ geheel geldt $\mathbb{F}_{q^m}$ is een deellichaam van $\mathbb{F}_{q^n}$ alleen als $m \mid n$. Dus als $\alpha \in \mathbb{F}_{q^n}$ nulpunt van $X^{q^m} - X$ is dan $\alpha \in \mathbb{F}_{q^m}$ en α is dan het nulpunt van een irred. mon. polynoom $f \in \mathcal{M}$ (want $m = gr(f)$ =, wegens $\mathbb{F}_{q^m} \cong \mathbb{F}_q[X]/(f)$)

Dus in $\mathbb{F}_q[X]$ moeten alle $f \in \mathcal{M}$, <u>mits</u> voor deze f geldt: $f = f_{\mathbb{F}_{q^m}}^{\alpha}$ en $\alpha^{q^n} - \alpha = 0$, delers zijn van $X^{q^n} - X$.
Maar $f = f_{\mathbb{F}_q}^{\alpha}$ voor een α met $\alpha \in \mathbb{F}_{q^m}$, $m := gr(f)$ want elk mon. irred. polynoom kunnen we een nulpunt geven met de uitbr. $\mathbb{F}_q[X]/(f) \ni (X \bmod f) = \alpha$.
Bovendien geldt voor die α dan weer dat $\alpha \in \mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$ omdat $\mathbb{F}_{q^m}$ isomorf is met deellichaam van $\mathbb{F}_{q^n}$ als $m \mid n$

dat betekent, aangezien alle $\alpha \in \mathbb{F}_{q^n}$ nulpunten zijn van $X^{q^n} - X$ (zie 12.1), dat α een nulpunt is van $X^{q^n} - X$ en dus dat, wegens $f = f^{\alpha}_{\mathbb{F}_q}$ en f mon. irred en $\alpha^{q^n} - \alpha = 0$ volgt $f \mid X^{q^n} - X$.

dus nu zien we dat álle $f \in M$ minstens een keer delers zijn van $X^{q^n} - X$. Als we nu aantonen dat het er niet meer kunnen zijn, volgt de ontbinding:

- stel er is een $f \in M$ met f deelt tweemaal $X^{q^n} - X$. Dan is in $\mathbb{F}_{q^n}$, α een dubbel nulpunt van $X^{q^n} - X$, waar α een nulpunt van f is. Maar dan is de afgeleide van $X^{q^n} - X$ in α gelijk aan 0, terwijl $[X^{q^n} - X]' = q^n X^{q^n - 1} - 1 = 0 \cdot X^{q^n - 1} - 1 = -1$ overal. Dus dit kan niet

- Stel er is een andere factor in de ontbinding in irred. factoren in $\mathbb{F}_q[X]$ van $X^{q^n} - X$ onvermeld gebleven, zeg g. Maar dan is g dus monisch en irreducibel (dat kunnen we zo kiezen) en $g \mid X^{q^n} - X$. Zij nu $\operatorname{gr}(g) = r$. $r \neq n$ anders was $g \in M$ al vermeld geweest. Echter, $g \mid X^{q^n} - X$ dus alle r nulpunten van g in $\mathbb{F}_{q^r} \ni \alpha_1, \ldots \alpha_r \notin \mathbb{F}_q$ zijn nulpunten van $X^{q^n} - X$, dus $\in \mathbb{F}_{q^n}$ maar als $\alpha_1, \ldots \alpha_m \in \mathbb{F}_{q^n}$, dan ligt ook $\mathbb{F}_q(\alpha_1, \ldots \alpha_r) \subset \mathbb{F}_{q^n}$ maar dan $\mathbb{F}_{q^m} \subset \mathbb{F}_{q^n}$ terwijl $r \nmid n$ tegenspraak.

Oftewel, zonder enig telargument vinden we dat alleen $f \in M$ delen in van $X^{q^n} - X$ en precies één keer, zodat in totaal

$$X^{q^n} - X = \prod_{f \in M} f$$

□

St. 12.14 Zij p priem en $n \in \mathbb{Z}_{\geq 1}$. Dan is de automorfismen groep $\mathrm{Aut}(\mathbb{F}_{p^n}) = \{ f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n} , f \text{ isomorfisme} \}$ een cyclische groep van orde n, en $\mathrm{Aut}(\mathbb{F}_{p^n}) = \langle F \rangle$ waar F het Frobenius automorfisme is.

Bewijs.
1. laat zien dat $\mathrm{orde}(F) = n$
2. laat zien dat $\# \mathrm{Aut}(\mathbb{F}_{p^n}) \leq n$
3. concludeer dat $\cdots \leq \langle F \rangle \leq \cdots$ zodat $\langle F \rangle = \mathrm{Aut}(\mathbb{F}_{p^n})$ en dus is de groep cyclisch en van orde n.

1. voor alle $x \in \mathbb{F}_{p^n}$ geld $x^{p^n} - x = 0$, want $\mathbb{F}_{p^n} \cong \mathrm{SF}_{\mathbb{F}_p}^{X^{p^n}-X}$ en dus $F^n(x) = (x^p)^n = x = \mathrm{id}(x) \ \forall x \in \mathbb{F}_{p^n}$, dus $F^n = \mathrm{id}$. Hiermee $\mathrm{orde}(F) \mid n$.
Echter, als $F^k = \mathrm{id}$, dan dus $x^{p^k} = x \ \forall x \in \mathbb{F}_{p^n}$ dus alle $x \in \mathbb{F}_{p^n}$ zijn nulpunten van $X^{p^k} - X \neq 0$ maar dat kan wegens 3.7 alleen als $\mathrm{gr}(\cdots) \geq p^n$ dus $p^k \geq p^n \Rightarrow k \geq n$. Dus n is de kleinste waarvoor $F^n = \mathrm{id}$, zodat $\mathrm{orde}(F) = n$ per definitie

2. Schrijf $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$ voor $\alpha^{\in \mathbb{F}_{p^n}}$ met minimumpolynoom f, dus van graad n en $f = \sum_{i=1}^{n} a_i X^i$. $\forall i \ a_i \in \mathbb{F}_p$.

Bovendien is elke $\sigma \in \mathrm{Aut}(\mathbb{F}_{p^n})$ $\sigma|_{\mathbb{F}_p} = \mathrm{id}$, omdat $\sigma(1) = 1$ per definitie, en elke $y \in \mathbb{F}_p$ is te schrijven als $y = \underbrace{1 + \cdots + 1}_{\text{hoogstens } p-1 \text{ 1's}}$ dus $\sigma(y) = \sigma(1 + \cdots + 1) = \sigma(1) + \cdots + \sigma(1) = 1 + \cdots + 1 = y$, overal steeds hetzelfde aantal termen. Hieruit volgt $\sigma(a_i) = a_i \ \forall i$.

Dus : $0 = \sigma(f(\alpha)) = \sigma\left(\sum_{i=1}^{n} a_i \alpha^i\right) = \sum_{i=1}^{n} \sigma(a_i)\sigma(\alpha)^i = \sum_{i=1}^{n} a_i \sigma(\alpha)^i$
$= f(\sigma(\alpha))$

Dus voor elke $\sigma \in \mathrm{Aut}(\mathbb{F}_{p^n})$ volgt dat $\sigma(\alpha)$ nulpunt is van f, en $f \neq 0$, $\mathrm{gr}(f) = n$. Dus wegens 3.7 volgt weer dat $\# \mathrm{Aut}(\mathbb{F}_{p^n}) \leq n$, en dit voltooit het bewijs $\square$

Een lichaamstheoretisch gevolg van deze Groepentheoretische stelling is weer :

12.15 Zij $f \in \mathbb{F}_p$ monisch en irreducibel, p priemgetal en zij α een nulpunt van f in een uitbr. van $\mathbb{F}_p$. Dan geldt in $\mathbb{F}_p(\alpha)$:

$$f = \prod_{i=0}^{n-1} (X - \alpha^{p^i})$$

Bewijs elke $F^i(\alpha)$ is anders voor $i = 0, \dots n-1$ doordat F orde n heeft, en bovendien is elke F^i een automorfisme zodat $F^i(\alpha)$ een nulpunt van f is. We vinden zo dus n verschillende nulpunten van f, nl. $\alpha, F(\alpha), F^2(\alpha) \dots F^{n-1}(\alpha)$. En dit zijn ze wegens 3.7 allemaal gezien $\operatorname{gr}(f) = n$.

Dus volgt dat voor elke $i = 0, \dots n-1$, $X - F^i(\alpha) = X - \alpha^{p^i}$ een factor is van f in $\mathbb{F}_p(\alpha)$ (aangezien $\alpha^{p^i} \in \mathbb{F}_p(\alpha)$ voor alle i.)

$\Rightarrow$ de ontbinding $f = \prod_{i=0}^{n-1} (X - \alpha^{p^i})$ □

Vbd in $\mathbb{F}_8$: neem $X^3 + X^2 + 1 \in \mathbb{F}_2[X]$ mon. irreducibel, dan heeft het een nulpunt $\gamma \in \mathbb{F}_8$ (allemaal zelfs) en in $\mathbb{F}_2(\gamma)$ is het $(X-\gamma)(X-\gamma^{2^1})(X-\gamma^{2^2}) =$
$(X-\gamma)(X-\gamma^2)(X-\gamma^4)$