A&S
HC9

stelling:

(i) Stel $|\mathbb{F}| < \infty$ dan $|\mathbb{F}| = p^n$, p priem

(ii) $\forall p, \forall n \geq 1 \; \exists \mathbb{F}$ met $|\mathbb{F}| = p^n$, $\mathbb{F}$ is 'uniek'

(i) stel $|\mathbb{F}| < \infty$ dan $\text{char}(\mathbb{F}) = p$, $1 \in \mathbb{F}$, $1, \underbrace{1+1}_{2}, \ldots, \underbrace{1+\ldots+1}_{(p-1)\times}, \underbrace{1+\ldots+1}_{p} = 0$

dus $\mathbb{Z}_p \subset \mathbb{F}$

Beschouw $(\mathbb{F}, \mathbb{Z}_p)$

- $\mathbb{F}$ is optelgroep
- $\forall \lambda \in \mathbb{Z}_p, \alpha \in \mathbb{F}: \lambda\alpha \in \mathbb{F}$,

$(\lambda+\mu)\alpha = \lambda\alpha + \mu\alpha$ $\quad 1\cdot\alpha = \alpha$

$\lambda(\alpha+\beta) = \lambda\alpha + \lambda\beta$ $\quad \alpha, \beta \in \mathbb{F}$

$(\lambda\mu)\alpha = \lambda(\mu\alpha)$ $\quad \lambda, \mu \in \mathbb{Z}_p$

Conclusie: $\mathbb{F}$ is vectorruimte over $\mathbb{Z}_p$ dus heeft basis over $\mathbb{Z}_p$: $(\alpha_1 \ldots \alpha_n)$ $\alpha_i \in \mathbb{F}$

$(\mathbb{R}^2, \mathbb{R}) \Rightarrow \langle \binom{1}{0}, \binom{0}{1} \rangle$

$(\mathbb{R}^3, \mathbb{R}) \Rightarrow \langle \binom{1}{0}, \binom{0}{1}, \binom{0}{0} \rangle$

$\forall \alpha \in \mathbb{F} \; \exists! \; a_1, \ldots, a_n \in \mathbb{Z}_p$

$\alpha = \sum_{j=1}^{n} a_j \alpha_j \quad n = \dim_{\mathbb{Z}_p}(\mathbb{F})$

dus $|\mathbb{F}| = p^n$

(ii) Route

$p(x) \in \mathbb{F}_p[x]$ irreducibel: $\mathbb{F}_p[x]/\langle p(x) \rangle = \mathbb{E}$

$\mathbb{Z}_2[x]/\langle x^2+x+1 \rangle = \{ ax+b+\langle p(x) \rangle \mid a, b \in \mathbb{Z}_2 \}$

(basis: $\{1, x\}$) $\Rightarrow \dim = 2$

Via splijtlichamen nl. $\mathbb{Z}_2[x]/\langle x^2+x+1 \rangle$ is splijtlichaam van $x^4 - x \in \mathbb{Z}_2[x]$

$\mathbb{E} \supset \mathbb{Z}_2$ en bevat alle nulpunten van $x^4 - x$, en is zo klein mogelijk

$(ax+b+\langle p(x) \rangle)^3 = a^3x^3 + 3a^2x^2b + 3axb^2 + b^3 + \langle p(x) \rangle$

$= a + a(x+1)b + axb + b + \langle p(x) \rangle$

$(\forall (a,b) \neq (0,0)) \quad = a + ab + b + \langle p(x) \rangle = 1 + \langle p(x) \rangle$

$x^2 - x + 1$
$x^3 = x^2 + x$
$= x + 1 + x$
$= 1$

$\mathbb{E} \supset \mathbb{Z}_p$, $\mathbb{E}$ splijtlichaam van $x^q - x \in \mathbb{Z}_p[x]$ met $q = p^n$

$\mathbb{R}[x]/\langle x^2+1 \rangle \sim \mathbb{C}$

$f(x) \in \mathbb{F}[x]$, zij $p(x) \in \mathbb{F}[x]$ een irreducibele factor van $f(x)$
en beschouw $\mathbb{E} = \mathbb{F}[x]/\langle p(x)\rangle \supset \mathbb{F}$
dan: $p(x+\langle p(x)\rangle) = \langle p(x)\rangle \; (= 0 \in \mathbb{E})$
want: $= p_0 + p_1(x+\langle p(x)\rangle) + \dots + p_m(x+\langle p(x)\rangle)^m$
$= \underbrace{p_0 + p_1 x + p_2 x^2 + \dots + p_m x^m}_{p(x)} + \langle p(x)\rangle = \langle p(x)\rangle$

dus $f(x)$ heeft nulpunt in $\mathbb{E}$
$f(x) = (x-a)\tilde{f}(x)$ met $gr.\tilde{f}(x) < gr.f(x)$
met inductie op gr. $f(x)$ volgt: $\exists\, \mathbb{K} \supset \mathbb{F}$ waarin $f(x)$ splijt.

Splijtlichaam is nu: $\bigcap \mathbb{K}$
$\mathbb{K} \supset \mathbb{F}$
$f(x)$ splijt in $\mathbb{K}$

Stel $p(x) \in \mathbb{F}[x]$, irreducibel en stel $a \in \mathbb{E} \supset \mathbb{F}$ met $p(a) = 0$
dan: $\mathbb{F}[x]/\langle p(x)\rangle \sim \mathbb{F}(a)$ (kleinste lichaam dat $\mathbb{F}$ omvat waarin a zit)
$\varphi(f(x) + \langle p(x)\rangle) = f(a)$ surjectief & homomorfisme

Stel $\varphi(f(x)+\langle p(x)\rangle) = 0$
dan: $f(a) = 0$ $\quad A = \{g(x) \mid g(a) = 0\}$ is ideaal.
$p(x) \in A \Rightarrow \langle p(x)\rangle \subset A$, $1 \notin A$, maar $\langle p(x)\rangle$ is maximaal
dus $\langle p(x)\rangle = A$
$f(x) \in \langle p(x)\rangle \Rightarrow f(x) + \langle p(x)\rangle = \langle p(x)\rangle$

$\mathbb{C} \sim \mathbb{R}(i)$
$x^2 - 2 \in \mathbb{Q}[x]$
$\Rightarrow \mathbb{Q}(\sqrt{2})$

Stel nu dat $\mathbb{F} \subset \mathbb{E}_i$, $i = 1,2$ en $a_i \in \mathbb{E}_i$, $p(a_i) = 0$
dan $\mathbb{F}(a_1) \sim \mathbb{F}(a_2)$ want $\mathbb{F}(a_i) = \mathbb{F}[x]/\langle p(x)\rangle$
Met inductie naar graad $f(x)$ volgt dat splijtlichamen van $f(x)$ isomorf zijn

existentie: gegeven $q = p^n$ beschouw $\mathbb{E}$ splijtlichaam van $x^q - x$
dan $|\mathbb{E}| \leq q = p^n$
Andersom: als $|\mathbb{K}| = p^n$. $\forall a \in \mathbb{K}^* = \mathbb{K} \setminus \{0\}$, $a^{q-1} = 1$, dus ook $a^q - a = 0$, ook voor $a = 0$ $\Rightarrow$ $\mathbb{K}$ splijtlichaam van $x^q - x$
$\Rightarrow \mathbb{K} \sim \mathbb{E}$