# 0.1 Campi finiti

Sia  $\mathbb{K}$  un campo e sia  $\chi_{\mathbb{K}} \colon \mathbb{Z} \to \mathbb{K}$  definita come  $\chi_{\mathbb{K}}(n) = \sum_{i=1}^{n} 1_{\mathbb{K}}$  per  $n \geq 0$  (si intende che  $\chi_{\mathbb{K}}(0) = 0_{\mathbb{K}}$ ) e  $\chi_{\mathbb{K}}(-n) = -\chi_{\mathbb{K}}(n)$ . Allora,  $\chi_{\mathbb{K}}$  è un omomorfismo di anelli, quindi  $\operatorname{Im}(\chi_{\mathbb{K}}) \subseteq \mathbb{K}$  è un dominio di integrità, da cui  $\ker(\chi_{\mathbb{K}}) \triangleleft \mathbb{Z}$  è un ideale primo.

#### Definizione

Se  $\ker(\chi_{\mathbb{K}}) = \{0\}$ , allora  $\mathbb{K}$  si dice di caratteristica 0, e si scrive  $\operatorname{char}(\mathbb{K}) = 0$ . Se  $\ker(\chi_{\mathbb{K}}) \neq \{0\}$ , esiste un primo p tale che  $\ker(\chi_{\mathbb{K}}) = p\mathbb{Z}$ ; in questo caso,  $\mathbb{K}$  si dice di caratteristica p, e si scrive  $\operatorname{char}(\mathbb{K}) = p$ .

Fatto (lo chiamerò Lemma 2.3.3): Sia K un campo finito. Allora  $\chi_K$  non può essere iniettivo, quindi K è di caratteristica p per un primo p.

(In realtà è una definizione) Se K è un campo di caratteristica  $p \neq 0$ ,  $K_0 = \text{Im}(\chi_k) \subseteq K$  è un campo detto campo primo di K, ed è isomorfo a  $\mathbb{Z}/p\mathbb{Z}$ .

#### Teorema 2.3.4

Siano E, F campi finiti tali che |E| = |F|. Allora,  $E \simeq F$ 

Dimostrazione. Sia |E| = |F| = q. Per il Fatto,  $\operatorname{char}(E) = p_1$  e  $\operatorname{char}(F) = p_2$  per  $p_1, p_2$  primi. Poiché  $E_0 \subseteq E$ , detto  $n_1 = |E| : E_0|$ , si ha che  $|E| = p_1^{n_1}$ . Analogamente, poiché  $F_0 \subseteq F$ , detto  $n_2 = |F| : F_0|$  si ha che  $|F| = p_2^{n_2}$ . Dunque  $p_1 = p_2 = p$  e  $n_1 = n_2 = n$ . La dimostrazione dell'isomorfismo continua dopo (dannazione è un sacco disorganizzato negli appunti

Questo teorema non è valido per i gruppi e per gli anelli. Infatti, nei gruppi  $|S_3| = |\mathbb{Z}/6\mathbb{Z}| = 6$ , ma uno è abeliano e l'altro no, quindi  $S_3 \not\simeq \mathbb{Z}/6\mathbb{Z}$ . Negli anelli,  $\mathbb{Z}/4\mathbb{Z} \not\simeq \mathbb{F}_2[x]/\langle x^2 \rangle$  perché uno ha gruppo additivo ciclico e l'altro no.

Osservare come questo dice che ogni campo finito ha cardinalità  $p^n$  per un primo  $p \in n > 1$ . In realtà questo è un se e solo se, cioè, per ogni  $p^n$  esiste un campo di ordine  $p^n$ . Due strade: considerare lo splitting field E di  $x^{p^n} - x$  su  $\mathbb{Z}/p\mathbb{Z}$  e mostrare che  $|E| = p^n$ , oppure costruire un polinomio irriducibile f(x) di grado n in  $\mathbb{F}_p[x]$  e considerare il quoziente  $\mathbb{F}_p[x]/\langle f \rangle$ .

Da questo segue anche che se E, F sono campi finiti tali che |E| = |F| = q, allora  $E^{\times} \simeq \mathbb{Z}/(q-1)\mathbb{Z}$  (questo perché se G è un gruppo abeliano il cui esponente è  $\exp(G) = |G|$ , significa che G è ciclico).

## Proposizione 2.3.5

Sia  $A\subseteq K^{\times}$  sottoanello di K campo,  $|A|<\infty.$  Allora, A è un gruppo ciclico.

Dimostrazione. Sia  $n = \exp(A)$ , e sia  $f = x^n - 1$ . Allora,  $A \subseteq Z_f(K)$  (sta indicando con  $Z_f(K)$  qualcosa che ha a che fare con gli zeri...) da cui  $|A| \le \deg^*(f) = n = \exp(A)$ . Poiché  $\exp(A) \mid |A|$ , deve essere  $|A| = \exp(A)$ , cioè A è ciclico.

Conclusione dimostrazione 2.3.4: Sia  $\psi_q = (x^{q-1} - 1)x$ . Allora  $Z_{\psi_q}(E) = E$  e  $Z_{\psi_q}(F) = F$ , quindi  $\psi_q(x) = \prod_{\lambda \in E} (x - \lambda) = \prod_{\mu \in F} (x - \mu)$ . Dunque,  $E/E_0$  e  $F/F_0$  sono campi di spezzamento di  $\psi_q \in \mathbb{F}_p[x]$ . Dunque, per il punto (b) del Teorema 2.3.1 sappiamo che  $E \simeq F$ .

Notare come questo dimostra che non è ambiguo denotare con  $\mathbb{F}_p$  il campo di cardinalità p primo, perché esso è effettivamente l'unico!

## Lezione del 12/11/2019 (appunti grezzi)

#### Definizione

Sia  $\mathbb{K}$  un campo con char $(\mathbb{K}) = p$ . Allora, la mappa  $F : \mathbb{K} \to \mathbb{K}$  definita come  $F(x) = x^p$  è un omomorfismo di campi detto omomorfismo di Frobenius.

Osserviamo che tale mappa è effettivamente un omomorfismo. Infatti,  $F(0_K) = 0_K$ ,  $F(1_K) = 1_K$  e  $F(x+y) = \sum_{k=0}^p \binom{p}{k} x^k y^{p-k} = x^p + y^p = F(x) + F(y)$  perché  $\binom{p}{k}$  è divisibile per p se 0 < k < p. Infine, è evidente che  $F(xy) = (xy)^p = x^p y^p = F(x) F(y)$ .

(Diventerà un Lemma) Osserviamo anche che F è iniettiva, e se  $|\mathbb{K}| < \infty$  è pure un automorfismo. Infatti, sappiamo che  $\ker(F) \lhd \mathbb{K}$ , ed essendo  $1 \not\in \ker(F)$ ,  $\ker(F) = \{0_K\}$  perché gli unici ideali di un campo sono  $\{0_K\}$  e K. Dunque F è iniettiva. Se vale anche  $|K| < \infty$ , essendo F iniettiva su un insieme finito, è chiaramente anche suriettiva, da cui è biettiva e quindi un automorfismo.

## Proposizione

Sia K un campo finito,  $p = \operatorname{char}(K)$  e  $K_0 = \operatorname{Im} \chi_K$ . Se  $|K| = p^n$ ,  $n = |K: K_0|$ , allora  $\operatorname{ord}(F) = n$ , dove  $\operatorname{ord}(F) = n$  è l'ordine di F pensata come elemento di  $\operatorname{Sym}(K)$ .

Dimostrazione. Sappiamo che  $K/K_0$  è campo di spezzamento di  $x^{p^n}-x$ , cioè K è l'insieme degli zeri di  $x^{p^n}-x$ , il che è vero se e solo se  $z^{p^n}=F^n(z)=z$  per ogni  $z\in\mathbb{K}$ . Dunque,  $F^n=\operatorname{id}_K$ . Resta da verificare che n è effettivamente il minimo intero positivo per cui  $F^k$  sia l'identità. Sia quindi  $k\in\mathbb{N}^+$  con k< n tale che  $F^k=\operatorname{id}_K$ . Allora,  $z^{p^k}=F^k(z)=z$  per ogni  $z\in K$ , cioè K è l'insieme degli zeri di  $x^{p^k}-x$ . Essendo  $\operatorname{deg}^\star(x^{p^k}-x)=p^k$ , tale polinomio ha al più  $p^k$  radici, cioè  $|K|=|Z_K(x^{p^k}-p)|\leq p^k< p^n$ , assurdo. Dunque  $F^k\neq\operatorname{id}_K$ .

Il grado di un'estensione si può chiamare ordine perché è l'ordine di un automorfismo (nel caso dei campi finiti).