Scheda riassuntiva di Teoria dei campi e di Galois

Definizioni e prerequisiti

Si dice **campo** un anello commutativo non banale K che è contemporaneamente anche un corpo. Si dice **omomorfismo di campo** tra due campi K ed L un omomorfismo di anelli. Dal momento che un omomorfismo φ è tale per cui $\operatorname{Ker}\varphi$ è un ideale di K con $1 \notin \operatorname{Ker}\varphi$, deve per forza valere $\operatorname{Ker}\varphi = \{0\}$, e quindi ogni omomorfismo di campi è un'immersione.

Dato l'omomorfismo $\zeta : \mathbb{Z} \to K$ completamente determinato dalla relazione $1 \overset{\zeta}{\mapsto} 1_K$, si definisce **caratteristica di** K, detta $\operatorname{char} K$, il generatore non negativo di $\operatorname{Ker}\zeta$. In particolare $\operatorname{char} K$ è 0 o un numero primo. Se $\operatorname{char} K$ è zero, ζ è un'immersione, e quindi K è un campo infinito, e in particolare vi si immerge anche $\mathbb{Q}$.

Tuttavia non è detto che $\operatorname{char} K = p$ implichi che K è finito. In particolare $\mathbb{Z}_p(x)$, il campo delle funzioni razionali a coefficienti in $\mathbb{Z}_p$, è un campo infinito a caratteristica p. Se $\operatorname{char} K = p$, per il Primo teorema di isomorfismo per anelli, $\mathbb{Z}/p\mathbb{Z}$ si immerge su K tramite la proiezione di ζ; pertanto K contiene una copia isomorfa di $\mathbb{Z}/p\mathbb{Z}$. Per campi di caratteristica p, vale il Teorema del binomio ingenuo, ossia:

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

estendibile anche a più addendi. In particolare, per un campo K di caratteristica p, la $\mathcal{F} : K \to K$ tale per cui $a \overset{\mathcal{F}}{\longmapsto} a^p$ è un omomorfismo di campi, ed in particolare è un'immersione di K in K. Se K è un campo finito, $\mathcal{F}$ è dunque un isomorfismo.

Per ogni p primo e $n \in \mathbb{N}^+$ esiste un campo finito di ordine p^n. In particolare, tutti i campi finiti di ordine p^n sono isomorfi tra loro, possono essere visti come spazi vettoriali di dimensione n sull'immersione di $\mathbb{Z}/p\mathbb{Z}$ che contengono, e come campi di spezzamento di $x^{p^n} - x$ su tale immersione. Poiché tali campi sono isomorfi, si indicano con $\mathbb{F}_p$ e $\mathbb{F}_{p^n}$ le strutture algebriche di tali campi. In particolare con $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$ si intende che esiste un'immersione di un campo con p^n elementi in uno con p^m elementi, e analogamente si farà con altre relazioni (come l'estensione di campi) tenendo bene in mente di star considerando tutti i campi di tale ordine.

Vale la relazione $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{q^m}$ se e solo se $p = q$ e $n \mid m$. Conseguentemente, l'estensione minimale per inclusione comune a $\mathbb{F}_{p^{n_1}}$, ..., $\mathbb{F}_{p^{n_i}}$ è $\mathbb{F}_{p^m}$ dove $m := \operatorname{mcm}(n_1, \dots, n_i)$. Pertanto se $p \in \mathbb{F}_{p^n}[x]$ si decompone in fattori irriducibili di grado $n_1, \dots, n_i$, il suo campo di spezzamento è $\mathbb{F}_{p^m}$. Inoltre, $x^{p^n} - x$ è in $\mathbb{F}_p$ il prodotto di tutti gli irriducibili di grado divisore di n.

Per il Teorema di Lagrange sui campi, ogni polinomio di $K[x]$ ammette al più tante radici quante il suo grado. Come conseguenza pratica di questo teorema, ogni sottogruppo moltiplicativo finito di K è ciclico. Pertanto $\mathbb{F}^*_{p^n} = \langle \alpha \rangle$ per $\alpha \in \mathbb{F}_{p^n}$, e quindi $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$, ossia $\mathbb{F}_{p^n}$ è sempre un'estensione semplice su $\mathbb{F}_p$. Si dice **campo di spezzamento** di una famiglia $\mathcal{F}$ di polinomi di $K[x]$ un sovracampo minimale per inclusione di K che fa sì che ogni polinomio di $\mathcal{F}$ si decomponga in fattori lineari. I campi di spezzamento di $\mathcal{F}$ sono sempre K-isomorfi tra loro. Per il criterio della derivata, $p \in K[x]$ ammette radici multiple se e solo se $\operatorname{MCD}(p, p')$ non è invertibile, dove p' è la derivata formale di p.

Se p è irriducibile in $K[x]$, (p) è un ideale massimale, e $K[x]/(p)$ è un campo che ne contiene una radice, ossia $[x]$. In particolare K si immerge in $K[x]/(p)$, e quindi tale campo può essere identificato come un'estensione di K che aggiunge una radice di p. Se K è finito, detta α la radice aggiunta all'estensione, $L := K[x]/(p) \cong K(\alpha)$ contiene tutte le radici di p (ed è dunque il suo campo di spezzamento). Infatti detto $[L : \mathbb{F}_p] = n$, $[x]$ annulla $x^{p^n} - x$ per il Teorema di Lagrange sui gruppi, e quindi p deve dividere $x^{p^n} - x$; in tal modo p deve spezzarsi in fattori lineari, e quindi ogni radice deve già appartenere ad L. In particolare, ogni estensione finita e semplice di un campo finito è normale, e quindi di Galois.

Si dice che L è un'estensione di K, e si indica con L/K, se L è un sovracampo di K, ossia se $K \subseteq L$. Si indica con $[L : K] = \dim_K L$ la dimensione di L come K-spazio vettoriale. Si dice che L è un'estensione finita di K se $[L : K]$ è finito, e infinita altrimenti. Un'estensione finita di un campo finito è ancora un campo finito. Un'estensione è finita se e solo se è finitamente generata da elementi algebrici. Una K-immersione è un omomorfismo di campi iniettivo da un'estensione di K in un altro campo che agisce come l'identità su K. Un K-isomorfismo è una K-immersione che è isomorfismo.

Dato α, si definisce $K(\alpha)$ il più piccolo sovracampo di K che contiene α. Si definisce l'**omomorfismo di valutazione** $\varphi_{\alpha,K} : K[x] \to K[\alpha]$, detto φ_α se K è noto, l'omomorfismo completamente determinato dalla relazione $p \overset{\varphi_\alpha}{\longmapsto} p(\alpha)$. Si verifica che φ_α è surgettivo. Se φ_α è iniettivo, si dice che α è **trascendentale** su K e $K[x] \cong K[\alpha]$, da cui $[K[\alpha] : K] = [K[x] : K] = \infty$. Se invece φ_α non è iniettivo, si dice che α è **algebrico** su K. Si definisce μ_α, detto il **polinomio minimo** di α su K, il generatore monico di $\operatorname{Ker}\varphi_\alpha$. Si definisce $\deg_K \alpha := \deg \mu_\alpha$. Se α è algebrico su K, $K[x]/(\mu_\alpha) \cong K[\alpha]$, e quindi $K[\alpha]$ è un campo. Dacché $K[\alpha] \subseteq K(\alpha)$, vale allora $K[\alpha] = K(\alpha)$. Inoltre, poiché $\dim_K K[x]/(\mu_\alpha) = \deg_K \alpha$, vale anche che $[K(\alpha) : K] = \deg_K \alpha$. Infine, si verifica che α è algebrico se e solo se $[K(\alpha) : K]$ è finito.

Si dice che L è un'**estensione semplice** di K se $\exists\, \alpha \in L$ tale per cui $L = K(\alpha)$. In tal caso si dice che α è un **elemento primitivo** di K. Si dice che L è un'**estensione algebrica** di K se ogni suo elemento è algebrico su K. Ogni estensione finita è algebrica. Non tutte le estensioni algebriche sono finite (e.g. $\overline{\mathbb{Q}}$ su $\mathbb{Q}$).

Ad opera di Gabriel Antonio Videtta,
https://poisson.phc.dm.unipi.it/~videtta/.
Reperibile su https://notes.hearot.it, nella sezione *Secondo anno → Algebra 1 → 3. Teoria delle estensioni di campo e di Galois → Scheda riassuntiva di Teoria dei campi e di Galois.*