Scheda riassuntiva di Teoria dei campi e di Galois

Campi e omomorfismi

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.

Caratteristica di un campo

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.

Proprietà dei campi 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 mappa $\mathcal{F} : K \to K$ tale per cui $a \overset{\mathcal{F}}{\mapsto} a^p$ è un omomorfismo di campi, ed in particolare è un'immersione di K in K, detta **endomorfismo di Frobenius**. Se K è un campo finito, $\mathcal{F}$ è anche un isomorfismo. Si osserva che per gli elementi della copia $K \supseteq \mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ vale $\mathcal{F}|_{\mathbb{F}_p} = \mathrm{Id}_{\mathbb{F}_p}$, e quindi $\mathcal{F}$ è un elemento di $\mathrm{Gal}(K/\mathbb{F}_p)$.

Campi finiti

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. Tali campi hanno obbligatoriamente caratteristica p, dove $|K| = p^n$. Esiste sempre un isomorfismo tra due campi finiti che manda la copia isomorfa di $\mathbb{Z}/p\mathbb{Z}$ di uno nell'altra.

Poiché i campi finiti di medesima cardinalità 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 $m := \mathrm{mcm}(n_1, \ldots, n_i)$. Pertanto se $p \in \mathbb{F}_{p^n}[x]$ si decompone in fattori irriducibili di grado $n_1, \ldots, n_i$, 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.

Proprietà dei polinomi di $K[x]$

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 $\mathrm{MCD}(p, p')$ 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.

Estensioni di campo

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'altra estensione di K che agisce come l'identità su K. Un K-isomorfismo è una K-immersione che è isomorfismo.

Date estensioni L e M su K, si definisce $LM = L(M) = M(L)$ come il **composto** di L ed M, ossia come la più piccola estensione di K che contiene sia L che M. In particolare, LM può essere visto come L-spazio vettoriale con vettori in M, o analogamente come M-spazio con vettori in L.

Omomorfismo di valutazioni, elementi algebrici e trascendenti e polinomio minimo

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 $\operatorname{Ker}\varphi_\alpha$. IDal momento che K è in particolare un dominio di integrità, μ_α è sempre irriducibile.

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.

Estensioni semplici, algebriche

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 $\mathbb{Q}$).

L'insieme degli elementi algebrici di un'estensione di K su K è un estensione algebrica di K. Pertanto se α e β sono algebrici, $\alpha \pm \beta$, $\alpha\beta$, $\alpha\beta^{-1}$ e $\alpha^{-1}\beta$ (a patto che o $\alpha \neq 0$ o $\beta \neq 0$) sono algebrici.

Campi perfetti, estensioni separabili e coniugati

Si dice che un'estensione algebrica L è un'**estensione separabile** di K se per ogni elemento $\alpha \in L$, μ_α ammette radici distinte. Si dice che K è un **campo perfetto** se ogni polinomio irriducibile ammette radici distinte. In un campo perfetto, ogni estensione algebrica è separabile. Si definiscono i coniugati di α algebrico su K come le radici di μ_α. Se $K(\alpha)$ è separabile su K, α ha esattamente $\deg_K \alpha$ coniugati, altrimenti esistono al più $\deg_K \alpha$ coniugati.

Un campo è perfetto se e solo se ha caratteristica 0 o altrimenti se l'endomorfismo di Frobenius è un automorfismo. Equivalentemente, un campo è perfetto se le derivate dei polinomi irriducibili sono sempre non nulle. Esempi di campi

perfetti sono allora tutti i campi di caratteristica 0 e tutti i campi finiti.

Campi algebricamente chiusi e chiusura algebrica di K

Un campo K si dice **algebricamente chiuso** se ogni $p \in K[x]$ ammette una radice in K. Equivalentemente K è algebricamente chiuso se ogni $p \in K[x]$ ammette tutte le sue radici in K. Si dice **chiusura algebrica** di K una sua estensione algebrica e algebricamente chiusa. Le chiusure algebriche di K sono K-isomorfe tra loro, e quindi si identifica con $\overline{K}$ la struttura algebrica della chiusura algebrica di K.

Se L è una sottoestensione di K algebricamente chiuso, allora $\overline{L}$ è il campo degli elementi algebrici di K su L. Infatti se $p \in L[x]$, p ammette una radice α in K, essendo algebricamente chiuso. Allora α è un elemento di K algebrico su L, e quindi $\alpha \in \overline{L}$. Per il Teorema fondamentale dell'algebra, $\overline{\mathbb{R}} = \mathbb{C}$.

Estensioni normali e K-immersioni di un'estensione finita di K

Sia α un elemento algebrico su K. Allora $[K(\alpha) : K] = \deg_K \alpha$. Le K-immersioni da $K(\alpha)$ in $\overline{K}$ sono esattamente tante quanti sono i coniugati di α e sono tali da mappare α ad un suo coniugato. Se K è perfetto, esistono esattamente $\deg_K \alpha$ K-immersioni da $K(\alpha)$ in $\overline{K}$.

Se L/K è un'estensione finita su K, allora esistono esattamente $[L : K]$ K-immersioni da L in $\overline{K}$. Per quanto detto prima, tali immersioni mappano gli elementi L nei loro coniugati.

Se L è un'estensione separabile finita, allora per ogni $\varphi : K \to \overline{K}$ esistono esattamente $[L : K]$ estensioni $\varphi_i : L \to \overline{K}$ di φ, ossia omomorfismi tali per cui $\varphi_i|_K = \varphi$.

Si dice che un'estensione algebrica L/K è un'**estensione normale** se per ogni K-immersione φ da L in $\overline{K}$ vale che $\varphi(L) = L$. Equivalentemente un'estensione è normale se è il campo di spezzamento di una famiglia di polinomi (in particolare è il campo di spezzamento di tutti i polinomi irriducibili che hanno una radice in L). Ancora, un'estensione L è normale se e solo se per ogni $\alpha \in L$, i coniugati di L appartengono ancora ad L. Per un'estensione normale, per ogni K-immersione $\varphi : L \to \overline{K}$ si può restringere il codominio ad un campo isomorfo a $L \subseteq \overline{K}$, e quindi considerare φ come un automorfismo di L che fissa K.

Si indica con $\mathrm{Aut}_K(L) = \mathrm{Aut}(L/K)$ l'insieme degli automorfismi di L che fissano K. Se L è normale e separabile, si dice **estensione di Galois**, e si definisce $\mathrm{Gal}(L/K) := (\mathrm{Aut}_K\, L, \circ)$, ossia come il gruppo $\mathrm{Aut}_K\, L$ con l'operazione di composizione.

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.*