Appunti di Advanced Coding Theory

7 maggio 2015

Indice

Capitolo 1

Premesse Algebriche

E/F estensione di campi, $\alpha \in E$.

Teorema 1.1. *$F[\alpha]$ è il più piccolo (e unico) sottoanello di E che contiene α, ossia l'intersezione di tutti i sottoanelli contenenti F, α.*

Dimostrazione. Voglio mostrare che $A \subset E \implies \exists K \subset E \,.\, A \subset K \ \wedge\ \forall K' \,.\, A \subset K' \subset K \implies K \subset K'$.

Unicità. $K_1, K_2 \subset K \,.\, A \subset K_1, K_2 \implies K_1 \cap K_2$ è ancora un sottocampo di E contenente A. Quindi mi basta prendere l'instersezione di tutti i sottocampi di E contenenti A, e se ve ne fossero due distinti, si avrebbe immediatamente un assurdo perché la loro intersezione sarebbe ancora più piccola.

Esistenza. E è un sottocampo di E contenente A, quindi l'intersezione è nonvuota.

□

Consideriamo l'applicazione $\varphi_\alpha : F[x] \to F[\alpha] : f \mapsto f(\alpha)$ morfismo applicazione. Si ha che:

- $\ker \varphi_\alpha = \{0\}$, allora α viene detto *trascendente*;
- $\ker \varphi_\alpha \neq \{0\}$, allora α viene detto *algebrico* e il più piccolo elemento non-nullo f è detto *polinomio minimo* di α su F.

$F(\alpha)$ è il più piccolo sottocampo di $E/F \ni \alpha$:

$$F(\alpha) = Q(F[\alpha]) = \left\{ \frac{f(\alpha)}{g(\alpha)} \in E : f(\alpha) \neq 0 \right\}.$$

Nota che $F[\alpha] = F(\alpha) \impliedby F[x]/(f)$ campo $\impliedby f$ polinomio minimo di $\alpha \impliedby \alpha$ algebrico.

Teorema 1.2. *$\forall f \in F[x]$ esiste un campo di spezzamento per f. Tale campo è unico a meno di isomorfismo.*

Dimostrazione.

Esistenza. Per induzione sul grado di f:

- ▶ $\deg f = 1 \implies f = x - \alpha \implies$ il campo di spezzamento è F stesso;
- ▶ $\deg f = n \implies f = gh$ con g irriducibile (g esiste sempre) $\implies \exists \alpha \in F[\alpha] = F(\alpha)$ tale che $g(\alpha) = 0$ per quanto visto prima $\implies f = (x - \alpha)p \in F(\alpha)$ con p di grado $n - 1$. Quindi per induzione il campo di spezzamento esiste.

Nota: corollario banale di questo è che $F(\alpha_1, \ldots, \alpha_n) = F(\alpha_1)(\alpha_2, \ldots, \alpha_n)$.

Unicità. $\hat{*}$ è un isomorfismo $F \to \hat{F} : a \mapsto \hat{a}$. Sia $\alpha_1 \in K_1/F$ radice di f irriducibile, e $\alpha_2 \in K_2/\hat{F}$ radice di $\hat{f}$ irriducibile. Allora esiste un unico isomorfismo $\psi : F[\alpha_1] \to \hat{F}[\alpha_2]$ tale che $a \mapsto \hat{a}$ e $\psi(\alpha_1) = \alpha_2$.
Dimostrare che è unico è banale, poiché presa una qualunque mappa con le stesse caratteristiche φ allora:

$$\begin{aligned} \varphi(a_0 + a_1\alpha_1 + \cdots + a_n\alpha_1^n) = \\ \varphi(a_0) + \varphi(a_1)\varphi(\alpha_1) + \cdots + \varphi(a_n)\varphi(\alpha_n) = \\ \hat{a}_0 + \hat{a}_1\alpha_2 + \cdots + \hat{a}_n\alpha_2^n = \\ \psi(a_0 + a_1\alpha_1 + \cdots + a_n\alpha_1^n). \end{aligned}$$

Per dire che esiste, la si costruisce:

$$\eta : F[x]/(f) \to \hat{F}[x]/(\hat{f}) : g \pmod f \mapsto \hat{g} \pmod{f'}$$

che è ben definita poiché $g_1 \equiv g_2 \mod f \iff f \mid g_1 - g_2 \iff \hat{f} \mid \hat{g}_1 - \hat{g}_2 \iff \hat{g}_1 \equiv \hat{g}_2 \mod \hat{f}$. Allora definisco $\psi = \sigma_1 \circ \eta \circ \sigma_2$ dove $\sigma_1 : F[\alpha_1] \to F[x]/(f)$ e $\sigma_2 : \hat{F}[x]/(\hat{f}) \to F[\alpha_2]$ isomorfismi perché f irriducibile (e quindi anche $\hat{f} = \hat{*}(f)$).

Da qui si procede per induzione ancora sul grado, come visto sopra, e si dimostra che due campi di spezzamento dello stesso f sono isomorfi.

□

Riassumendo velocemente, L/K è detta estensione finita di K se $n = [L : K] < \infty$. L è detto algebrico e $\exists\{\alpha_i\}_i^n$ è una base per L su K e ogni elemento di L può esser scritto in modo unico come combinazione lineare di questi.

Definizione 1.3 (Embedding)**.** Siano L_1/K, L_2/K estensioni. σ è detto *embedding* se $\sigma : L_1 \to L_2$ e $\forall a \in K \sigma(a) = a$.

Segue dalla definizione che σ è una mappa iniettiva e vi è un isomorfismo $L_1 \simeq \sigma(L_1)$. Esso è detto K-*isomorfismo.*

Per ogni campo possiamo trovare un'estensione algebrica $\bar{K}$ in cui ogni polinomio di grado positivo spezza; essa è detta anche *chiusura algebrica* ed è unica a meno di K-isomorfismo.

1.1 Chiusura Algebrica

Sia E estensione del campo F e sia $\sigma : F \to L$ un embedding.

Teorema 1.4 (Chiusura Algebrica)**.** *Per ogni campo K esiste un'estensione algebrica $\bar{K}$ su K in cui ogni polinomio di grado maggiore-uguale a 1 ha radici in $\bar{K}$. Data un'estensione L su K esiste unembedding $\sigma : L \to \bar{K}$ e se $[L : K] < \infty$ allora in numero di embedding differenti è al più $[L : K]$.*

Dimostrazione.

Esistenza. Usando il lemma di Zorn (assioma della scelta) posso costruire un sovracampo il cui tutti i polinomi spezzano.

$$K \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n$$

e al termine i-esimo posso trovare tutte le radici nel campo successivo.

Unicità Se prendo due estensioni, $K(\alpha), K(\beta)$ ed un polinomi irriducibile f s.t. $f(\alpha) = f(\beta)$, allora posso travare un isomorfismo

$$\varphi = \begin{cases} a \in K \mapsto a \\ \alpha \mapsto \beta \end{cases} .$$

Se prendo una chiusura algebrica $\bar{K}$, una delle proprietà che ci interessano è

□

1.2 Teoria di Galois

Si riassumono di sotto alcuni dei risultati più interessanti della Teoria di Galois.

Definizione 1.5 (Gruppo di Galois)**.** Il *gruppo di Galois* è l'insieme di tutti gli automorfismi di E/F in sé stesso, ossia di tutti i morfismi $\sigma : E \to E$ tali che $\sigma : a \mapsto a \ \forall a \in F$, equipaggiato con la composizione $\circ$. Tale gruppo viene identificato con $\mathrm{Gal}(E/F)$

Teorema 1.6. *Sia $f \in F[x]$ con E_1 campo di spezzamento, e $\hat{f} \in \hat{F}[x]$ con E_2 rispettivo campo di spezzamento. Allora il numero di isomorfismi $\sigma : E_1 \to E_2$ con $\sigma_{|F} = \hat{*}$ è esattamente il grado $n = [E_1 : F] = [E_2 : F]$.*

Dimostrazione. Per induzione sul grado n:

- $[E_1 : F] = n = 1 \implies$ l'unico isomorfismo che rispetta $\sigma_{|F} = \hat{*}$ è $*$ stesso;

- $[E_1 : F] = n \implies$ esiste un polinomio irriducibile che divide f, e per ogni radice su g possiamo associarne una su $\hat{g}$, ed esse sono tutti e i soli isomorfismi possibili. Per dimostrare che esiste una roba simile mostro che presa una mappa $\sigma : E_1 \to E_2$. $\sigma_{|F} = \hat{*}$ allora ho $g(\alpha) = \hat{g}(\sigma(\alpha)) = 0$.

$$\begin{aligned} 0 = g(\alpha) = & \\ &= \sigma(g(\alpha)) && [\sigma \text{ morfismo}] \\ &= \sigma(a_0 + a_1\alpha + \cdots + a_m\alpha^m) && [g = \textstyle\sum_i a_i x^i] \\ &= \hat{a}_0 + \hat{a}_1\sigma(\alpha) + \hat{a}_m\sigma(\alpha)^m && [\sigma_{|F} = \hat{*},\ \sigma \text{ morfismo}] \\ &= g(\sigma(\alpha)). \end{aligned}$$

  L'unicità è ovvia perché $\sigma(\alpha)$ è un unico elemento di E_2. Chiamo quindi $\Psi_i : F(\alpha) \to F(\beta_i)$ tale che $\Psi_{i|F} + \hat{*}$ e $\Psi(\alpha) = \beta_i$ dove $\{\beta_i\}_i^m$ è una radice di $\hat{g}$. Allora

$$\{\sigma : E_1 \to E_2 \mid \sigma_{|F} = \hat{*}\} = \bigcup_i^m \{\sigma : E_1 \to E_2 \mid \sigma_{|F(\alpha)} = \Psi_i\} = \bigcup_i A_i$$

  e se ci mettiamo a contarli, sfruttando l'ipotesi induttiva:

$$|\{\sigma : E_1 \to E_2 \mid \sigma_{|F} = \hat{*}\}| = \sum_i |A_i| = \sum_i^m |E_1 : F(\alpha)| = |E_1 : F(\alpha)|m = |E_1 : F(\alpha)||F(\alpha) : F| = |E_1 : F|.$$

  Nota: $|A_i| = |E_1 : F(\alpha)|$ per il passo induttivo, e questo è immediato dalla costruzione di A_i; g fattore irriducibile di f di grado m ha m radici, quindi $|F(\alpha) : F| = m$. Si arriva quindi a qualcosa tipo:

$$\begin{array}{ccc} F & \xrightarrow{\hat{*}} & \hat{F} \\ \downarrow{\scriptstyle i_F} & & \downarrow{\scriptstyle i_{\hat{F}}} \\ F(\alpha) & \xrightarrow{\Psi_i} & \hat{F}(\beta_i) \\ \downarrow{\scriptstyle i_{F\alpha}} & & \downarrow{\scriptstyle i_{\hat{F}(\beta_i)}} \\ E_1 & \xrightarrow{\sigma} & E_2 \end{array}$$

□

Corollario 1.7. *Sia E il campo di spezzamento di $f \in F[x]$. Allora $|E : F| = |\operatorname{Gal}(E/K)|$.*

Dato $G = \{\sigma_i\}_i^n$ famiglia di automorfismi (ricordo ancora, sono K-automorfismi dall'estensione in sé stessa), introduciamo la notazione

$$E^G = \{a \in E \mid \forall \sigma_i \ . \ \sigma_i(a) = a\}.$$

Definizione 1.8 (Estensione di Galois)**.** Un'estensione E/F è detta *di Galois* sse $E^{\operatorname{Gal}(E/F)} = F$, i.e. se

$$F = \{a \in E \mid \forall \sigma_i \in \operatorname{Gal}(E/F) \ . \ \sigma_i(a) = a\}.$$

Teorema 1.9 (Teorema di Dedekind)**.** *Siano $\chi_1, \ldots, \chi_n$ caratteri distinti da G a F. Allora sono linearmente indipendenti su F.*

Dimostrazione. Ricordiamo che un *carattere* da G a F è un morfismo di gruppi $G \to F^*$.

Vogliamo mostrare che $\forall x \in G$

$$a_1\chi_1(x) + a_2\chi_2(x) + \cdots + a_n\chi_n(x) = 0 \implies a_1 = a_2 = \cdots = a_n = 0.$$

Procedo per induzione su n:

- $n = 1 \implies a_1\chi_1 = 0 \implies a_1 = 0$ poiché χ_1 non ha 0 nella sua immagine;

▶ supponiamo $a_n = 1$, eventualmente moltiplicando i coefficienti per a_n^{-1}. Poiché tutti i χ_i sono diversi, esiste un y_0 tale che $\chi_1(y_0) \neq \chi_n(y_0)$. Possiamo quindi fare il magheggio $\chi_i(x) = \chi_i(x_0 y_0) = \chi_i(x_0)\chi_i(y_0)$, oppure ogni termine per $\chi_n(x)$, ottenendo:

$$a_1\chi_1(x)\chi_1(y_0) + a_2\chi_2(x)\chi_2(y_0) + \cdots + a_{n-1}\chi_{n-1}(x)\chi_{n-1}(y_0) + a_n\chi_n(x)\chi_n(y_0) = 0$$
$$a_1\chi_1(x)\chi_n(y_0) + a_2\chi_2(x)\chi_n(y_0) + \cdots + a_{n-1}\chi_{n-1}(x)\chi_n(y_0) + a_n\chi_n(x)\chi_n(y_0) = 0$$

e facendo la differenza dei due:

$$a_1(\chi_1(y_0) - \chi_n(y_0))\chi_1(x) + a_2(\chi_2(y_0) - \chi_n(y_0))\chi_2(x) + \cdots + a_{n-1}(\chi_{n_1}(y_0) - \chi_n(y_0))\chi_{n-1}(x) = 0$$

$\implies$ tutti i coefficienti sono nulli per ipotesi induttiva, poiché coinvolge $n-1$ termini, quindi in particolare $a_1 = 0$. Ma allora l'equazione iniziale diventa una combinazione di $n-1$ termini, e per ipotesi induttiva allora $a_1 = a_2 = \cdots = a_{n-1} = a_n = 0$.

□

Teorema 1.10. *Sia $G = \{\sigma_1, \ldots, \sigma_n\}$ un gruppo di automorfismi rispetto alla composizione. Allora $|E : E^G| = |G|$.*

Dimostrazione. La dimostrazione si divide in due parti ($\geq$, $\leq$), in cui la prima non necessita neppure dell'ipotesi che G sia un gruppo.

Vogliamo mostrare che $|E : E^G| \geq n$. Per farlo, consideriamo una base $\{\alpha_i\}_i^r$ per F e il seguente sistema di equazioni in n incognite:

$$\begin{cases} x_1\sigma_1(\alpha_1) + \cdots + x_{n-1}\sigma_1(\alpha_{n-1}) + x_n\sigma_1(\alpha_r) = 0 \\ x_1\sigma_2(\alpha_1) + \cdots + x_{n-1}\sigma_2(\alpha_{n-1}) + x_n\sigma_2(\alpha_n) = 0 \\ \quad \vdots \\ x_1\sigma_n(\alpha_1) + \cdots + x_{n-1}\sigma_n(\alpha_{n-1}) + x_n\sigma_n(\alpha_n) = 0 \end{cases}$$

Se per assurdo vi fosse una soluzione $\bar{x}_1, \ldots, \hat{x}_n$ non banale al sistema, i.e. $r < n$ allora per ogni $a = \sum_i^r a_i\alpha_i$

$$\begin{aligned} \hat{x}_1\sigma_1(a) + \cdots + \hat{x}_{n-1}\sigma_{n-1}(a) + \hat{x}_n\sigma_n(a) &= \sum_j^n \hat{x}_j\sigma_j(a) \\ &= \sum_j^n \hat{x}_j\sigma_j\left(\sum_i^r a_i\alpha_i\right) = \sum_j^n\sum_i^r \hat{x}_j\sigma_j(a_i\alpha_i) \\ &= \sum_j^n\sum_i^r \hat{x}_j\sigma_j(a_i)\sigma_j(\alpha_i) = \sum_j^n\sum_r^r \hat{x}_j a_i\sigma_j(\alpha_i) \\ &= \sum_i^r a_i \underbrace{(\hat{x}_1\sigma_1(\alpha_i) + \cdots + \hat{x}_{n-1}\sigma_{n-1}(\alpha_i) + \hat{x}_n\sigma_n(\alpha_i))}_{=0 \text{ poiché soluzione}}. \end{aligned}$$

Per il Teorema di Dedekind segue che $\hat{x}_1 = \cdots = \hat{x}_n = 0$, che è assurdo poiché abbiamo scelto proprio una soluzione non baale.

Vogliamo mostrare che $|E : E^G| \leq n$, e lo facciamo ancora per assurdo: supponiamo $|E : E^G| > n$ e scegliamo $\omega_0, \ldots, \omega_n \in E$, $n+1$ elementi linearmente indipendenti su E^G. Allora il sistema di n equazioni su $n+1$ incognite:

$$\begin{cases} x_0\sigma_1(\omega_0) + \cdots + x_{n-1}\sigma_1(\omega_{n-1}) + x_n\sigma_1(\omega_n) + = 0 \\ x_0\sigma_2(\omega_0) + \cdots + x_{n-1}\sigma_2(\omega_n - 1) + x_n\sigma_2(\omega_n) = 0 \\ \quad \vdots \\ x_0\sigma_n(\omega_0) + \cdots + x_{n-1}\sigma_n(\omega_n - 1) + x_n\sigma_n(\omega_n) = 0 \end{cases}$$

che ha una soluzione con il massimo numero di zeri $(a_0, \ldots, a_r, 0, \ldots 0)$. Supponiamo $a_r = 1$ eventualmente moltiplicando per a_r^{-1}, allora

$$\forall j \quad a_0\sigma_j(\omega_0) + \cdots + a_{r-1}\sigma_j(\omega_{r-1}) + \sigma_j(\omega_r) = 0.$$

Si nota che deve esistere un $a_i \notin E^G$, poiché altrimenti si avrebbe una contraddizione quando $\sigma_j = \mathbf{1}$ (ricordiamo che gli ω_i sono lin. indip.). Suppongo sia $a_0 \notin E^G \implies \exists \sigma_k \,.\, \sigma_k(a_0) \neq a_0$. Allora applicando σ_k a tutta l'equazione si ottiene:

$$\forall j \quad \sigma_k(a_0)\sigma_j(\omega_0) + \cdots + \sigma_k(a_{r-1})\sigma_j(\omega_{r-1}) + \sigma_j(\omega_r) = 0.$$

poiché $\sigma_k G = G$. Facendo la differenza si nota che sparisce il termine $\sigma_j(\omega_r)$, ottenendo così una soluzione con uno zero in più di $(a_0, \ldots, a_r, 0, \ldots, 0)$ ma questo è un assurdo. □

Da questo segue immediatamente un corollario che caratterizza le estensioni di Galois:

Corollario 1.11. *E/F è un'estensione di Galois sse $|E : F| = |\operatorname{Gal}(E/F)|$.*

Dimostrazione. " $\implies$ ": $|E : F| = |E : E^G||E^G : F| = |\operatorname{Gal}(E/F)| \cdot 1$ per il teorema precendente $\implies |E^G : F| = 1 \implies F = E^G$.
" $\impliedby$ ": $|E^G : F| = 1 \implies |E : F| = |E : E^G||E^G : F| = |\operatorname{Gal}(E/F)|$. □

Definizione 1.12 (Separabile)**.** Un polinomio $f(x) \in K[x]$ è detto *separabile* se il numero di radici distinte nel suo campo di spezzamento è uguale al grado. Un elemento $\alpha \in L/K$ è detto *separabile* se il suo polinomio minimo è separabile. Un'estensione L/K è detta *separabile* se ogni suo elemento è separabile.

Proposizione 1.13. *g irriducibile $\in F[x]$. Allora g non è separabile $\iff g' = 0$.*

Dimostrazione. " $\implies$ ". g irriducibile, quindi ha grado positivo. D'altra parte $g' = 0$, e l'unica possibilità è che $g(x) = h(x^p)$ dove $p = \operatorname{ch}(F)$.
" $\impliedby$ ". Abbiamo $g \in F[x]$ irriducibile e non separabile $\implies g = (x-\alpha)^2 g$ e pertanto $g' = 2(x-\alpha)f + (x-\alpha)^2 f' \implies$ il gcd $d = (g, g') = ag + bg'$ è tale che $d(\alpha) = 0 \implies g \mid d$ poiché irriducibile quindi polinomio minimo per α. Si arriva quindi a dire che $\deg f \geq \deg g$ e $d \mid g' \implies g' = 0 \veebar \deg d \leq \deg g'$ e l'unica possibilità è che $g' = 0$. □

Definizione 1.14 (Normale)**.** Un'estensione è detto normale se ogni polinomio irriducibile in $F[x]$ che ha una radice in E si spezza in E.

Questo ci porta alla definizione seguente:

Definizione 1.15 (Puramente Inseparabile)**.** Sia E/F con $\operatorname{ch}(F) = p > 0$. Un elemento $\gamma \in E$ è detto *puramente inseparabile* se $\gamma^{q^r} \in F$ per qualche $r \geq 0$.
E/F è detta *puramente inseparabile* se tutti i suoi elementi lo sono.

Proposizione 1.16. *Sia $E \supset F \supset K$ una pila di estensioni. E/K è separabile sse E/F e F/K lo sono.*

Teorema 1.17. *Data un'estensione arbitraria L/K esiste un'unico campo intermedio S s.t. $K \subset S \subset L$ tale che S/K è separabile e L/S è non-separabile.*

Definizione 1.18 (Campo Perfetto)**.** Un campo è detto *perfetto* se tutte le sue estensioni sono separabili.

I campi di caratteristica 0 sono sempre separabili, quindi sono sempre perfetti. I campi di caratteristica positiva sono sempre perfetti, perché gli elementi sono radici di $x^q - x \implies \forall \beta \in K \quad \beta = \alpha^p$ per qualche $\alpha \in K$.

Definizione 1.19 (Estensione Semplice)**.** L/K è detto *semplice* se $L = K(\alpha)$ per qualche $\alpha \in L$. Allora, α è detto *primitivo*. ?? ma come?

Tutte le estensioni di campi finiti separabili sono semplici.

Teorema 1.20. *Sia E/F un'estensione finita. Sono equivalenti:*

(i) E/F è un'estensione di Galois;
(ii) E/F è un'estensione normale e separabile;
(iii) E è il campo di spezzamento per qualche polinomio seprabile $f \in F[x]$.

Dimostrazione. (i) $\implies$ (ii). Pongo $G = \mathrm{Gal}(E/F)$. Sia $p \in F[x]$ irriducibile con $\alpha \in E$ sua radice, quindi polinomio minimo di α. Considero l'insieme $\{\sigma_i(\alpha) \mid \sigma_i \in G\} = \alpha_1, \ldots, \alpha_r$ e il polinomio $q = \prod_i^r (x - \alpha_i)$. Allora, preso un $\sigma \in G$ e ridefinito per funzionare come morfismo sui polinomi senza dar fastidio alle variabili $\tilde{\sigma} : E[x] \to E[x] : a_0 \cdots + a_{n-1}x^{n-1} + a_n x^n \mapsto \sigma(a_0) + \cdots + \sigma(a_{n-1})x^{n-1} + \sigma(a_n)x^n \implies$

$$\begin{aligned} \tilde{\sigma}(q) &= \prod_i^r (x - \sigma(\alpha_i)) && [\sigma \text{ manda } G \text{ in } G] \\ &= \prod_i^r (x - \alpha_i) \\ &= q \end{aligned}$$

$\implies \sigma(a_i) = a_i \implies q \in F[x]$. D'altra parte $\mathbf{1}(\alpha)$ è radice di q quindi $p \mid q$, quindi p ha un sottoinsieme delle radici di q, ed esse stanno tutte in E e sono tutte distinte. Quindi E/F è normale e separabile.

(ii) $\implies$ (iii). $E = F(\alpha_1, \ldots, \alpha_s)$ poiché estensione finita per definizione. Allora $f = p_1 \cdots p_s$, dove $p_i \in F[x]$ è il polinomio minimo di α_i, spezza in E poiché una radice sta in E, quindi ci stanno tutte per la normalità di E/F.

(iii) $\implies$ (i) è immediato per il Corollario 1.7. □

Si può dimostrare, ma non lo riporteremo qui, che i primi due fatti sono equivalenti anche per estensioni infinite.

Gruppo di Galois come permutazione. Data un'estensione di campi E/K di grado n, possiamo costruire una mappa iniettiva $G \to S_n$ con $G = \mathrm{Gal}(E/F)$ e S_n gruppo di permutazioni di n elementi:

$$\Psi : G \to S_n : \sigma \mapsto \pi \quad \text{dove } \sigma(\alpha_i) = \alpha_j \implies \pi(i) = j$$

che, riformulato, vuol dire $\sigma(\alpha_i) = \alpha_{\Psi(\sigma)(i)}$. È banale notare che che poiché σ è bigettiva, anche π lo è, quindi è una permutazione. Poiché Ψ è anche un morfismo, possiamo notare che:

$$\ker \Psi = \{\sigma \in G \mid \Psi(\sigma) = \mathbf{1}\} = \{\mathbf{1}_G\}$$

quindi Ψ è iniettiva.

Teorema 1.21 (Corrispondenza di Galois)**.** *Sia E/F un'estensione di Galois con $|E : F| < \infty \implies$ esiste una corrispondenza tra isottogruppi di* $\mathrm{Gal}(E/F)$ *e i campi intermedi di E/F.*

Dimostrazione. Sia E/F estensione di campi, con $G = \mathrm{Gal}(E/F)$. Definisco le funzioni α, β:

$$H \subset G \;.\; \alpha : H \mapsto E^H \qquad F \subset K \subset E \;.\; \beta : K \mapsto \mathrm{Gal}(E/K)$$

Voglio mostrare che sono una l'inversa dell'altra, i.e. che $\alpha \circ \beta = \mathbf{1}$ e $\beta \circ \alpha = \mathbf{1}$. Si nota anzitutto che:

$$\begin{aligned} H_1 \subset H_2 &\implies \alpha(H_1) \supset \alpha(H_2) && [\text{poiché } \alpha(H_1) \text{ ha meno condizioni}] \\ K_1 \subset K_2 &\implies \beta(K_1) \supset \beta(K_2) && [\text{poiché } \beta(K_1) \text{ è un'estensione più grande}] \end{aligned}$$

da cui si possono ricavare alcune proprietà necessarie per la dimostrazione:

1. $\beta \circ \alpha(H) \supset H$
   poiché $\forall \sigma \in H \implies \sigma(a) = a \; \forall a \in \alpha(H) \implies \sigma \in \beta \circ \alpha(H)$;
2. $\alpha \circ \beta(K) \supset K$
   poiché $\forall a \in K \implies \sigma(a) = a \; \forall \sigma \in \beta(K) = \mathrm{Gal}(E/K) \implies a \in \alpha \circ \beta(K)$;
3. $\alpha \circ \beta \circ \alpha(H) = \alpha(H)$
   poiché da un lato $\alpha(H) = \alpha(H) \implies \alpha\beta(\alpha(H)) \supset \alpha(H)$ e dall'altro $\beta \circ \alpha(H) \supset H \implies \alpha \circ \beta \circ \alpha(H) \subset \alpha(H)$;
4. $\beta \circ \alpha \circ \beta(K) \supset K$
   poiché da un lato $\beta(K) = \beta(K) \implies \beta\alpha(\beta(K)) \supset \beta K$ e dall'altro $\alpha \circ \beta(K) \supset K \implies \beta \circ \alpha \circ \beta(K) \subset \beta(K)$;
5. $H_1 \subsetneq H_2 \subset G \implies \alpha(H_1) \neq \alpha(H_2)$
   poiché per il Teorema 1.10 $|E : E^{H_1}| = |H_1| < |H_2| = |E : E^{H_2}| \implies E^{H_1} \neq E^{H_2}$;
6. $K_1 \subsetneq K_2 \subset E \implies \beta(K_1) \neq \beta(K_2)$
   poiché $E/K_1, E/K_2$ sono di Galois ($\exists f \in F[x] \;.\; E$ è il suo campo di spezzamento, quindi $f \in K_1[x], f \in K_2[x]$) e $|E : K_1| \neq |E : K_2| \implies \mathrm{Gal}(E/K_1) \neq \mathrm{Gal}(E/K_2)$ poiché hanno cardinalità diversa;
7. $\beta \circ \alpha(H) = H$
   poiché $\beta \circ \alpha(H) \supset H$ per 1. e se per assurdo $\beta \circ \alpha(H) neq H$ per 5. sarebbe $\alpha \circ \beta \circ \alpha(H) \neq \alpha(H)$ ma per 3. questa è una contraddizione;

8. $\alpha \circ \beta(K) = K$
   poiché $\alpha \circ \beta(K) \supset K$ per 2. e se per assurdo $\alpha \circ beta(K) \neq K$ per 6. sarebbe $\beta \circ \alpha \circ \beta(K) \neq \beta(K)$ ma per 4. questa è una contraddizione.

□

A questo punto lo Stichtenoth mostra altre caratterizzazioni dei gruppi di Galois, che non credo sia fondamentale studiare. Ad esempio, una dice che se ho E/F estensione con N_1, N_2 campi intermedi, allora il gruppo di Galois id $N = N_1N_2$ è $\mathrm{Gal}(E/N_1) \cap \mathrm{Gal}(E/N_2)$. La dimostrazione di questo è immediata per la definizione di gruppo di Galois:

$$\begin{aligned}\mathrm{Gal}(L/N) &= \{\sigma \text{ morfismo } L \to L \mid \ \sigma(a_1a_1) = a_1a_2 \ \forall a_1, a_2 \in N_1 \times N_2\} \\ &= \{\sigma \text{ morfismo } L \to L \mid \sigma(a_1) = a_1, \ \sigma(a_2) = a_2 \ \forall a_1, a_2 \in N_1 \times N_2\} \qquad [\text{fisso } a_1 = 1, \text{ poi } a_2 = 1] \\ &= \mathrm{Gal}(L/N_1) \cap \mathrm{Gal}(L/N_2).\end{aligned}$$

L'ultima sezione parla di traccia e norme, che comunque sono già trattate nel corso di Finite Fields, quello che però importa ricordare è che data un'estensione $L/K \ni \alpha$ noi definiamo una mappa $\mu_\alpha : L \to L : z \in L \mapsto \alpha \cdot z$. Il norma e traccia sono rispettivamente determinante e traccia di quella matrice, nonché rispettivamente il coefficiente primo (termine noto) e penultimo del polinomio minimo di α.

Nel caso in cui si abbia un'estensione $\mathbb{F}_{q^m}/\mathbb{F}_q$ si può notare che il gruppo degli automorfismi $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ è ciclico in quanto generato dal morfismo di Frobenius $\alpha \mapsto \alpha^q$ e pertanto traccia e norma diventano rispettivamente somma e prodotto dei coniugati.

Riporto giusto per completezza questo teorema, facilissimo da dimostrare una volta prestata attenzione alle dimostrazioni di sopra.

Teorema 1.22 (Hilbert's Theorem 90)**.**

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = 0 \iff \alpha = \beta^q - \beta \text{ per qualche } \beta \in \mathbb{F}_{q^m}.$$

1.3 Complessità

Diremo che $f(n) = O(g(n))$ se $\exists C_1$ costante tale che $f \leq C_1 g \ \ \forall n \in \mathbf{N}$. In particolare, diremo che $f = o(g)$ se $\lim_{n\to\infty} f/g = 0$, ossia quando g è particolarmente sovrastimato rispetto a f. Diremo invece che $f \asymp g$ se $\lim_{n\to\infty} f/g = 1$, ossia quando f e g sono asintoticamente equivalenti.

Ci sarebbero anche altre notazioni, tipo

$$f = \Omega(g) \iff g = O(f) \qquad \text{e} \qquad f = \theta(g) \iff \exists C_1, C_2 \ . \ C_1 g \leq f \leq C_2 g$$

ma non credo siano rilevanti, né che i matematici qui ne siano al corrente.

Teorema 1.23 (Prime Number Theorem)**.** *Sia $\pi(n)$ il numero di interi primi minori di n, allora:*

$$\pi(n) \asymp \frac{n}{\ln(n)}.$$

Si allega ancora un volta un po' a casaccio una classificazione veloce dei problemi decisionali:

- un problema decisionale è detto di classe P se $\exists p(n)$ polinomio tale per cui il problema viene eseguito in tempo $\leq O(p(n))$;
- un problema decisionale è detto di classe NP se data una potenza di calcolo illimitata è possibile risolvero e verificare la correttezza della risposta affermativa in tempo polinomiale (questa cosa è detta *polynomial time certificate*.
- un problema decisionale è detto NP- completo se ogni altro problema Q può esser risolto da P in tempo polinomiale. Quindi un problema è detto NP se un qualunque altro problema NP può esser ridotto ad esso.

1.4 Fondamenti di Geometria Algebrica

Teorema 1.24 (Hilbert Basis Theorem)**.** *Tutti un anello di polinomi su un noetheriano è noetheriano.*

Dimostrazione. Sia I un ideale di $R[x]$, e $\forall n \geq 0$ $J_n := \{0\} \cap \{\mathrm{LC}(f) : f \in I\}$. Chiaramente $J_n \subset J_{n+1}$ poiché $\mathrm{LC}(f) \in J_n \implies \mathrm{LC}(xf) = \mathrm{LC}(f) \in J_{n+1}$. Si può verificare velocemente che l'unione catena infinita di ideali

$$J_0 \subset J_1 \subset \cdots \subset J_n \subset \ldots$$

$J = \bigcup_i J_i$ è ancora un ideale di R, quindi è finitamente generato $\implies$ $J = \langle r_i \rangle_i$ con $r_i \in J_n$ per qualche $J_n \implies \exists N \in \mathbf{N}$. $J_N \supset \{r_i\}_i$ e $J = J_N$.

Lo stesso possiamo dire per ogni $J_n = \langle r_{n,1}, \ldots, r_{n,l_n} \rangle$, per cui J è generato da $\bigcup_{n,i} r_{n,i}$. Preso $f_{n,i}$ un polinomio il cui *leading coefficient* sia $r_{n,i}$ affermo che $J = \langle f_{n,i} \rangle_{n,i}$ per induzione:

- $\deg f = 0 \implies f \in R$ e non c'è nulla da dimostrare;
- $\deg f = n \implies$ (se $n > N$ allora pongo $n = N$ esiste una combinazione lineare $\sum_i a_i \cdot r_{n,i} = \mathrm{LC}(f)$ $\implies f - \sum_i a_i f_{n,i} \in J$ per ipotesi induttiva quindi $f \in J$.

□

Corollario 1.25. *Sia R un anello noetheriano, allora $R[x_1, \ldots, x_m]$ è noetheriano.*

Dimostrazione. Per induzione sulle m variabili. □

Teorema 1.26 (Hilbert *Weak* Nullstellensatz)**.** *Sia I ideale proprio di $\mathbb{F}[X] = \mathbb{F}[x_1, \ldots, x_m]$ con $\mathbb{F}$ algebricamente chiuso. Allora $\exists (a_1, \ldots, a_m) \in \mathbb{F}$ in cui tutti i polinomi di I si annullano.*

Dimostrazione. Sia M un ideale massimale contenente M, allora considero $\mathbb{F}/M$, che identifica $x_i \mapsto t_i$ tramite la proiezione naturale. $\mathbb{F}/M$ è un campo, poiché $t_1, \ldots, t_m$ algebrici $\implies$ $F[t_1, \ldots, t_m]$ è campo. Inoltre $t_1, \ldots, t_m$ alebrici su $\mathbb{F} \implies t_i \in \mathbb{F}$ poiché $\mathbb{F}$ è algebricamente chiuso.

Allora fisso $(t_1, \ldots, t_m) = (a_1, \ldots, a_m)$ e affermo che questa è proprio la soluzione cercata. Infatti $x_i - a_i \in M$ $\forall i < m$ e poiché $\langle x_i - a_i \rangle_i$ è massimale $\implies$ $\langle x_i - a_i \rangle_i = M$ quindi tutti i polinomi di I svaniscono in $(a_1, \ldots, a_m)$. □

Teorema 1.27 (Hilbert *Strong* Nullstellensatz)**.** *Sia I ideale di $\mathbb{F}[X] = \mathbb{F}[x_1, \ldots, x_m]$ con $\mathbb{F}$ algebricamente chiuso. Se $\exists f$ che sia unnulla in $(a_1, \ldots, a_m)$ in cui anche tutti i polinoi di I si annullano $\implies$ $f \in \sqrt{I}$, i.e. $\exists n > 0$. $f^n \in I$.*

1.5 Varietà

Questa parte comprende (con eventuali piccoli approfondimenti) un riassunto dello *Stichtenoth*, Appendice B.

Varietà Affini

Assumiamo K algebricamente chiuso. $\mathbb{A}^n = \mathbb{A}^n(K)$ è l'insieme delle n-uple di K - è uno spazio affine costruito su K.

$V \subset \mathbb{A}^n$ è detto *algebrico* se $\exists M \subset K[x_1, \ldots, x_n]$. $V = \{P \in \mathbb{A}^n \mid F(P) = 0 \ \forall F \in M\}$. L'ideale generato da V è definito come $I(V) := \{F \in K[x_1, \ldots, x_n] \mid F(P) = 0 \ \forall P \in V\}$. Poiché esso è un ideale di $K[x_1, \ldots, x_n]$ noetheriano, allora per il teorema delle basi di Hilbert esso è finitamente generato dai polinomi $F_1, \ldots, F_r$. Questo implica tra le altre cose che $V = \{P \in \mathbb{A}^n \mid F_1(P) = \cdots = F_r(P) = 0\}$. Alle volte useremo la notazione $V(S)$ con $S \in K[x_1, \ldots, x_n]$ per indicare l'insieme algebrico.

$V \subset \mathbb{A}^n$ è detto *irriducibile* se $\nexists V_1, V_2$ propriamente algebrici . $V = V_1 \cap V_2$. Si può osservare che V è irriducibile $\iff$ $I(V)$ è un ideale primo [1] (?? dimostrare).

$V \subset \mathbb{A}^n$ è detto *varietà affine* se è un insieme algebrico irriducibile.

Tra i possibili insiemi algebrici, vale la pena menzionare quelli più grandi e quelli più piccoli. I primi sono le ipersuperfici, ossia gli zeri di un unico polinomio. I secondi sono il luogo deli zeri di esattamente n polinomi.

Proposizione 1.28. *L'unione e l'intersezione di varietà sono ancora varietà.*

Dimostrazione. Per l'unione vale:

$$\begin{aligned} V(I) \cup V(J) &= \{p \in K \mid f(p) = 0 \ \wedge \ g(p) = 0 f, g \in V(I) \times V(J)\} \\ &= \{p \in K \mid f(p)g(p) = 0\} && [K[x_1, \ldots, x_n] \text{ è un dominio di integrità}] \\ &= V(IJ). \end{aligned}$$

[1] $I \subset R$ è un ideale primo primo sse $\forall ab \in I \implies a \in I \ \vee \ b \in I$

Per l'intersezione si nota da un lato che $V(I) \cap V(J) = \{ p \in K \mid f(p) = 0 \ \wedge \ g(p) = 0 \}$ che è un sovrainsieme di $V(I+J) = \{ p \in K \mid f(p) + g(p) = 0 \}$. D'altro canto

$$V(I+J) = \{ p \in K \mid \lambda_1 f(p) + \lambda_2 g(p) \ \forall f, g \in V(I) \times V(J), \ \lambda_i \in K \}.$$

Se fisso $\lambda_1 = 0$ ottengo $V(I) \subset V(I+J)$. Se fisso $\lambda_2 = 0$ ottengo $V(J) \subset V(I+J)$, quindi $V(I) \cap V(J) \subset V(I+J)$. Segue per assioma di estensione la tesi. □

Corollario 1.29. *Ogni sottoinsieme finito di $\mathbb{A}^n$ è algebrico.*

Possiamo munire quindi l'insieme della *topologia di Zarinski*, dove ogni chiuso è un isieme algebrico. Infatti, l'unione finita è ancora algebrica (abbiamo sempre i generatori), e l'intersezione di un numero finito di insiemi algebrici è ancora algebrica.

Il *coordinate ring* $\Gamma(V) = \frac{K[x_1,\dots,x_m]}{I(V)}$ è la classe dei resti di $I(V)$. Si nota che se $I(V)$ è composto dai polinomi $f = F + I(V)$ e ognuno di essi induce una mappa (l'applicazione) $f : V \to K : P \mapsto F(P) \quad \forall P \in V$. Inoltre, se $I(V)$ è primo, allora $\Gamma(V)$ è un dominio d'integrità.

Il campo $K(V) = \mathrm{Quot}(\Gamma(V))$ è il campo delle funzioni razionali. Si può facilmente notare che si ha $K(V) \supset K$ e $\frac{K(V)}{K}$ è il grado di trascendenza.

Fissato $P \in V$, si definisce l'*anello locale*

$$\mathcal{O}_p = \{ f \in K(V) \mid f = g/h \text{ con } h(P) \neq 0 \}$$

esso ha campo quoziente $K(V)$ e un solo ideale massimale

$$\mathcal{M}_p = \{ f \in K(V) \mid f = g/h \text{ con } h(P) \neq 0 \ \wedge \ g(P) = 0 \}.$$

Varietà Proiettive

Definiamo lo spazio proiettivo

$$\mathbf{P}^n = \mathbf{P}^n(K) = \frac{\mathbb{A}^{n+1} - \{0\}}{K} = \{ (a_0 : \cdots : a_n) : a_i \in K, \text{non tutti gli } a_i \text{ sono nulli} \}.$$

$P = (a_0 : \cdots : a_n)$ è detto punto e gli $a_0, \dots, a_n$ sono le *coordinate omogenee*. Un *monomio* è un elemento $G \in K[x_0, \dots, x_n]$. $G = a \prod_i^n x_i^{e_i}$ tale che $a \in K$ non nullo e $\sum_i e_i = d$. Un *polinomio omogeneo* è una somma di monomi dello stesso grado. Un ideale generato da polinomi omogenei è detto *ideale omogeneo*.

Un sottoinsieme $V \subset \mathbf{P}^n$ è detto *algebrico* se è il luogo degli zeri di un insieme di polinomi $M \subset K[x_1, \dots, x_n]$

$$V = \{ P \in \mathbf{P}^n \mid F(P) = 0 \ \forall F \in M \}.$$

Notache che tale luogo degli zeri è ben definito poiché $F(P) = 0 \iff F(\lambda P) = \lambda^d F(P) = 0$. Da qui possiamo fare le stesse costruzioni di prima

Denotiamo con $I(V) \subset K[x_0, \dots, x_n]$ ideale dei polinomi di $K[x_0, \dots, x_n]$ che hanno V tra le radici. Una *varietà proiettiva* è un insieme algebrico è irriducibile. In tal caso,

$$\Gamma_h(V) = K[x_0, \dots, x_n]/I(V)$$

è un dominio di integrità.

Il campo $K(V)$ è lo spazio delle frazioni su $\Gamma_h(V)$ dove il denominatore è non nullo. Una funzione razionale $f = g/h$ con $g = G + I(V)$ e $h = H + I(V)$ dello stesso grado d, è tale che $f(P) = \frac{g(P)}{h(P)} = \frac{\lambda^d g(P)}{\lambda^d h(P)} = \frac{g(\lambda P)}{h(\lambda P)}$ ha un *valore* unico e ben definito. Giusto per non sentirmi in colpa definisco l'anello locale $\mathcal{O}_p(V) := \{ f \in K(V) \mid f \text{ è definito in } P \}$, ma sono tutte costruzioni che si ricavano facilmente dal caso affine.

Varietà proiettive e spazi affini. Considero la mappa

$$\varphi_i : \mathbb{A}^n \to \mathbf{P}^n : (a_0 : \cdots : a_{n-1}) \mapsto (a_0 : \cdots : a_{i-1} : 1 : a_{i+1} : \cdots : a_n)$$

che in particolare è una bigezione su $U_i = \{ (a_0 : a_1 : \cdots : a_n) \in \mathbf{P}^n \mid a_i \neq 0 \}$. Gli U_i costituiscono un ricoprimento di $\mathbf{P}^n$. Per ogni U_i chiamo quello che resta *iperpiano all'infinito*, i.e. $H_i = \mathbf{P}^n - U_i = \{ a_i = 0 \}$ e i suoi elementi sono detti *punti all'infinito*. Se abbiamo una varietà proiettiva, posso definire $V_i = \varphi^{-1}(V \cap U_i) \subset \mathbb{A}^n$ che è una

varietà affine se $U_i \cap V$ è non-nullo; naturalmente $V = \bigcup_i (V \cap U_i)$ poiché $\{ U_i \}_i$ è un ricoprimento di $\mathbf{P}^n$. Si può notare che l'ideale genarato da V_i può esser scritto come

$$I(V_i) = \{ F(x_0 : \cdots : 1 : \ldots x_{n-1}) \mid F \in I(V) \}.$$

Possiamo trovare dei K-isomorfismi $K(V) \to K(V_i)$ che mandano $f = g/h \in K(V)$ - quindi con $g, h \in \Gamma(V)$ - in $g^*/h^* \in K(V_i)$ e tali sono costruiti prendendo dei rappresentanti di g, h, diciamo $G, H \in K[x_0, \ldots, x_{n-1}]$ e costruendo $G^* = G(x_0, \ldots, 1, \ldots, x_{n-1})$, $H^* = H(x_0, \ldots, 1, \ldots, x_{n-1})$ da cui poi mi prendo le classi di resto su $\Gamma(V_i)$ g^*, h^* rispettivamente.

Viceversa, possiamo trovare la *chiusura proiettiva* di una varietà V mediante la trasformazione

$$* : I(V) \to K[x_0, \ldots, x_n] : F(x_0, \ldots, x_{n-1}) \mapsto F^* = x_n^d F(x_0/x_n, \ldots, x_{n-1}/x_n)$$

e la chiusura viene denotata

$$\bar{V} = \{ P \in \mathbf{P}^n \mid F^*(P) = 0 \ \forall F \in I(V) \}.$$

Si può mostrare che $V \simeq \bar{V}$.

Mappe e Morfismi Si considerino le varietà proiettive $V \subset \mathbf{P}^m$ e $W \subset \mathbf{P}^n$. Siano $F_0, \ldots, F_n \in K[x_0, \ldots, x_m]$ polinomi omogenei tali che:

(a) $F_0, \ldots, F_n$ hanno lo stesso grado;
(b) non tutti gli F_i stanno in $I(V)$;
(c) $\forall H \in I(W) \ . \ H(F_0, \ldots, F_n) \in I(V)$.

Ad esempio $Q \in V \implies \exists i \ . \ F_i(Q) \neq 0 \implies (F_0(Q) : \cdots : F_n(Q)) \in W \subset \mathbf{P}^n$.
Diremo che

$$(F_0, F_1, \ldots, F_n) \sim (G_0, G_1, \ldots, G_n) \iff F_i G_j \equiv F_j G_i \pmod{I(V)}$$

e la classe di equivalenza è detta *mappa razionale* e viene identificata con ϕ. Una mappa razionale è detta *regolare* o *definita* in P se $\exists G_0, \ldots, G_n \in K[x_0, \ldots, x_m]$ tali che

$$\phi = (G_0 : G_1 : \cdots : G_n) \quad \text{e} \quad \exists i \ . \ G_i(P) \neq 0$$

da cui segue che $\phi(P) = (G_0(P) : \cdots : G_n(P)) \in W$ (ed è ben definita).

Due varietà V_1, V_2 sono dette *birazionalmente equivalenti* se esistono mappe razionali tra i due spazi $\phi_1 : V_1 \to V_2$ e $\phi_2 : V_2 \to V_1$ la cui composizione è l'identità, i.e. $\phi_1 \circ \phi_2 = \mathbf{1}_{V_1} \ \wedge \ \phi_2 \circ \phi_1 = \mathbf{1}_{V_2}$. Si può dimastrare che tale caso si ha sse le due varietà sono K-isomorfe.

Una mappa regolare su tutto V è detta *morfismo*. Due varietà sono dette isomorfe se esisono due morfismi e la loro composizione è l'identità. Naturalmente, isomorfismo implica birazionale equivalenza, tuttavia non è sempre vero il contrario.

Curve Algebriche

Una *curva algebrica* è una varietà di dimensione 1 (?? cos'è la dimensione). $P \in V$ è detto *nonsingolare* o *semplice* se l'anello locale $\mathcal{O}_p$ è un *discrete valuation ring* (i.e. un PID con un solo ideale massimale $\neq \{ 0 \}$). I punti singolari su una curva sono finiti; in particolare la curva è detta *liscia* o *nonsingolare* se non ha singolarità.

Nel caso affine, abbiamo che una curva affine $V \subset \mathbb{A}^2$ è data dal luogo degli zeri di un polinomio irriducibile $G \in K[x_0, x_1]$. Tale curva è detta *liscia* se soddisfa il criterio di Jacobi:

$$G = \frac{\partial G}{\partial x_0}(p) = \frac{\partial G}{\partial x_0}(p) = 0$$

non ha soluzioni.

Nel caso proiettivo, abbiamo che una curva piana proiettiva $V \subset \mathbf{P}^2$ è data dal luogo degli zeri di un polinomio irriducibile omogeneo $H \in K[x_0, x_1, x_2]$. Similmente al caso affine, un punto p è detto nonsingolare se

$$H = \frac{\partial H}{\partial x_0}(p) = \frac{\partial H}{\partial x_1}(p) = \frac{\partial H}{\partial x_2} = 0$$

non ha soluzioni.

Mappe tra Curve. Sia $\phi : V \to W$ una mppa razionale tra le varietà proiettive V, W. Si può dimostrare che:

- ϕ è definita su tutti i punti nonsingolari $P \in V$; inoltre, se V è liscia allora ϕ è un morfismo.
- se ϕ è noncostante su V liscia, allora ϕ è surgettiva.

Esiste una 1-1 corrispondenza $P \mapsto \mathcal{M}_P(V)$ che rende possibile estendere definizioni da campi di funzioni algebriche a curve algebriche, e viceversa. Ad esempio, il genere di una curva V è il genere del campo di funzioni $K(V)$.

Divisori. Un divisore D su V è una somma formale $D = \sum_{p \in V} n_P \cdot P$ dove $n_P \in \mathbf{Z}$ ed $n_P \neq 0$ su un insieme discreto di V. Il gruppo dei divisori forma un gruppo additivo $\mathrm{Div}(X)$. Il divisore principale di una funzione razionale f, denotato (f) è definito

$$(f) = \sum_{p \in V} \nu_p(f) \cdot p$$

dove ν_p è la valutazione discreta in P su $K(V)$, ed è talvolta detto *ordine della funzione*. L'insieme dei divisori principali $\mathrm{PDiv}(V)$ forma un sottogruppo dei divisori.

Il gruppo quoziente

$$\mathrm{Jac}(V) = \frac{\mathrm{Div}^0(V)}{\mathrm{PDiv}(V)},$$

dove $\mathrm{Div}^0(V)$ sono i divisori di grado 0, è detto *Jacobiano di* V.

Capitolo 2

Introduzione alle Curve Ellittiche

Una curva ellittica $\mathcal{E}$ su un campo K è una curva in incognite x, y tale che

$$\mathcal{E}(x,y) : y^2 + bxy + cy = x^3 + \alpha x^2 + \beta x + \gamma \qquad \text{(Equazione di Wierstrass generale)}$$

Voglio rendere più compatta tale espressione. Se la caratteristica del campo è diversa da $2, 3$ mediante manipolazioni algebriche, possiamo ammazzare i coefficienti b, c. Pongo $y \leftarrow y - \frac{bx}{2} - \frac{c}{2}$ e similmente mi comporto per x.

Proposizione 2.1. *Dato un polinomio $t^n + bt^{n-1} + \cdots = 0$, posso ammazzare il termine di grado $n-1$ mediante la sostituzione $\tilde{t} = t - \frac{b}{n}$.*

Allora l'equazione diventa:

$$\mathcal{E} : y^2 = x^3 + Ax + B \qquad \text{(Equazione di Wierstrass)}$$

Definisco la curva $\mathcal{E}(L)$ con $L \supset K$ come l'insieme delle soluzioni sull'estensione L. Di modo da poter conferire a questo insieme struttura di gruppo, sono necessarie due altre assunzioni:

- non vi siano radici multiple, i.e. $(r_1 - r_2)(r_1 - r_3)(r_2 - r_3) \neq 0$; equivalentemente, si assume che il determinante
$$4A^3 + 27B^2 \neq 0;$$
- alla curva viene aggiunto un punto formale $\infty = 0$, elemento neutro. In genere, è comodo pensare a questo termine come punto che sta in cima all'asse y.

Riepilogando,

$$\mathcal{E}(L) = \{\infty\} \cup \{(x,y) \in L^2 : y^2 = x^3 + Ax + B\}. \tag{2.1}$$

Le curve ellittiche possono assuere forme diverse su campi diversi. Nel caso di campi finiti, abbiamo un gruppo abeliano finito, la cui importanza si riscontra soprattutto in crittografia; su $\mathbb{R}$ abbiamo che la curva ellittica è isomorfa a S^1 o $\mathbf{Z}_2 \times S^1$ (abbiamo un cerchio possibile sulla sinitra, più l'altro pezzo sulla destra che sta insieme col punto all'infinito); su $\mathbb{C}$ abbiamo che $\mathcal{E}(\mathbb{C})$ è un toro.

2.1 Legge di Gruppo

Mediante entrambe queste assunzioni possiamo munire l'insieme di un'operazione di somma $+$.

L'opposto di un punto $P = (x_0, y_0)$ è $-P = (x_0, -y_0)$. La somma $P + \infty = P \quad \forall P \in \mathcal{E}$, per definizione di elemento neutro. La somma di due punti $P_1 \neq P_2$ viene fatta considerando l'intersezione della retta passante per i due punti con $\mathcal{E}$, e prendendo l'opposto del terzo punto di intersezione $P = (x_3, y_3)$, diverso dai due precedenti per costruzione. Se $x_1 = x_2$ allora $P + Q = \infty$, altrimenti si considera la pendenza

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

da cui segue immediatamente che $y_3 = m(x_3 - x_1) + y_1$; x_3, invece, può esser trovata interpolando la retta con l'equazione di $\mathcal{E}$. Possiamo fare di meglio: notiamo che

$$y^2 = (m(x - x_1) - y_1)^2 = x^3 + Ax + B$$

può osser riordinata come $x^3 + m^2x^2 + \cdots = 0$. D'altra parte quella stessa cubica ha come radici i tre punti:

$$(x - x_1)(x - x_2)(x - x_3) = x^3 - (x_1 + x_2 + x_3)x^2 + \dots$$

per cui $x_3 = m^2 - x_1 - x_2$. Terminiamo prendendone l'opposto, quindi segue che:

$$x_3 = m^2 - x_2 - x_1, \qquad y_3 = m(x_1 - x_3) - y_1. \tag{2.2}$$

Quando $P = Q$, considero la retta tangente. Quando $y_1 = y_2 = 0$ allora $P_1 + P_2 = \infty$, altrimenti:

$$\frac{\partial[y^2]}{\partial x} = \frac{\partial[x^3 + Ax + C]}{\partial x} \implies 2y\frac{\partial y}{\partial x} = 3x^2 + A \implies m = \frac{\partial y}{\partial x} = \frac{3x_1^2 + A}{2y_1}$$

che implica, come visto sopra:

$$x_3 = m^2 - 2x_1, \qquad y_3 = m(x_1 - x_3) - y_1. \tag{2.3}$$

È immediato verificare che l'opposto $-P \in \mathcal{E} \wedge P - P = \infty$. Riepilogando, la somma definita sul gruppo mantiene le proprietà di:

Chiusura. L'equazione della curva $\mathcal{E}$ ha sempre tre soluzioni per costruzione, quindi la somma di due punti appartiene sempre alla curva.
Inverso. $P = (x, y) \in \mathcal{E} \implies -P = (x, -y) \in \mathcal{E}$.
Associativa. Si può dimostrare, ma è incredibilmente incasinato e non credo l'abbiamo dimostrato a lezione.
Commutativa. La linea per P, Q è la stessa per Q, P;

2.2 Proiettivizzazione

L'idea di proiettivizzare la curva ellittica $\mathcal{E} = \{ f = 0 \}$ ci permette di giustificare l'introduzione del punto formale ∞. Consideriamo l'iniezione $\mathbb{A}^2_K \hookrightarrow \mathbf{P}^2_K : (x, y) \mapsto (x : y : 1)$ e la mappa $F : \mathbf{P}^2 \to K : z^3 f(xz^{-1}, yz^{-1})$. Si ha che $F(\lambda x, \lambda y, \lambda z) = \lambda^3 F(x, y, z)$ ed $F = 0 \iff f = 0$. Nel caso di due rette parallele:

$$y = mx + b_1 z \qquad y = mx + b_2 z \qquad (b_1 \neq b_2)$$

oppure

$$x = c_1 z \qquad x = c_2 z \qquad (c_1 \neq c_2)$$

Si può facilmente notare che la loro intersezione si ha per $z = 0$, rispettivamente nei punti proiettivi $(1 : m : 0)$ (quando sostituiamo $z = 0$ nella prima equazione ottenendo $y = mx$) o $(0 : 1 : 0)$ (sostituendo nella seconda). Di questi due, però, l'unico che appartiene alla curva F è $(0 : 1 : 0)$, poiché $z = 0 \implies x^3 = 0 \implies (x : y : z) = (0 : 1 : 0)$. Tale punto è unico, non vi è differenza tra il sopra e il sotto (poiché $(0 : 1 : 0) = (0 : -1 : 0)$), e ogni suo multiplo sta nella stessa classe.

Vale la pena notare che cerchiamo sempre una curva con tre soluzioni distinte, e senza punti singolari. La prima richiesta è necessaria per poter fare la somma. La seconda va approfondita invece:

Definizione 2.2 (Singolarità)**.** Un punto è detto *singolare* se tutte le sue derivate parziali sono nulle. Per contrasto, una curva è detta *nonsingolare* se non vi sono punti di singolarità.

Studiamo la curva ellittica proiettivizzata $F : y^2z - x^3 - Axz^2 - Bz^3 = 0$
Notiamo che $z \neq 0$ poiché altrimenti $x^3 = 0 \implies y^2 = 0 \implies (0 : 0 : 0) \in \mathcal{E}$, ma questo è impossibile. Possiamo quindi assumere senza perdita di generaltà che $z = 1$.
Le derivate direzionali sono:

$$F_x = -3x^2 - Az^2 \qquad F_y = 2yz \qquad F_z = y^2 - 2Axz - 2Bz^2$$

È immadiato notare che se la curva fosse singolare, si avrebbe che $F_y = 0 \implies y = 0$, quindi $\mathcal{E} : x^3 + Ax + B = 0$ è un polinomio in x. Inoltre $F_x = 0$, quindi c'è una radice doppia, ma questo è stato escluso.

Osservazione 2.3. Una curva ellittica è una curva *liscia* in $\bar{K}$.

2.3 Altri Sistemi di coordinate

`TODO: questa parte fa cagare, non è stata fatta a lezione e il Washington la spiega di merda.`

Allo scopo di render più efficienti gli algoritmi per la computazione della somma nel gruppo delle curve ellittiche, torna comodo trovare altri sistemi di coordinate in cui rappresentare le curve. Precisamente, usando la somma vista sopra, è stato misurato un costo computazionale tra le 9 e le 40 volte quello della moltiplicazione. È quindi conveniente studiare un sistema di coordinate in cui queste possano essere evitate.

Coordinate Proiettive: è la trasformazione più naturale da fare. Omogeneizziamo l'equazione della cuva e su di essa definiamo la somma di due punti. Tale somma verrà fuori non necessitare di alcuna inversione.

Coordinate Jacobiane: usiamo le coordinate proiettive $(x : y : z)$ per indicare le coordinate affini $(x/z^2, y/z^3)$. Questo crea un cambiamento nella forma di Wierstrass che diventa:

$$y^2 = x^3 + Axz^4 + Bz^6$$

Nota: qui le formule di addizione diventano più semplici se $A = -3$. Si suppone che sia questa la ragione per cui tutte quelle del NIST sono così.

Coordinate di Edwards: sono state studiate da Bernstein e Lange. Si creano una curva isomorfa ad una curva ellittica:

$$C : x^2 + y^2 = 1 + c^2(1 + dx^2y^2)$$

con $c,\ d \in K^\times$ e d non un quadrato. Le formule additive così risultano particolarmente semplici. Nota bene però che non sempre possiamo fare questa trasformazione restando in K, spesso è necessario muoversi nella sua chiusura.

2.4 j-invariant

Sia $\mathcal{E} : y^2 = x^3 + Ax + B$ curva ellittica con $A, B \in K$ campo di caratteristica diversa da 3 o 2. La sostituzione

$$x \leftarrow \mu^2 x \qquad\qquad y \leftarrow \mu^3 y$$

con $\mu \in \bar{K}^*$ porta a una nuova curva $\mathcal{E}' : y^2 = x^3 + A'x + B'$, dove $A' = \mu^4 A$ e $B' = \mu^6 B$. Possiamo mostrare che $\mathcal{E}$ ed $\mathcal{E}'$ condividono lo stesso invariante, detto *j-invariant*:

$$j(\mathcal{E}) = 1728\frac{4A^3}{4A^3 + 27B^2}$$

Teorema 2.4. *Siano $\mathcal{E}_1,\ \mathcal{E}_2$ due curve ellittiche tali che $j(\mathcal{E}_1) = j(\mathcal{E}_2)$. Allora esiste una trasformazione $x_2 = \mu^2 x_1 \quad y_2 = \mu^3 y_1$ simile a quella di sopra, che trasforma un'equazione nell'altra.*

Dimostrazione. Assumiamo anzitutto il caso $A_1 \neq 0$, tratteremo dopo il caso nullo. $A_1 \neq 0 \implies j \neq 0 \implies A_2 \neq 0$. Esiste quindi un $\mu\ .\ A_2 = \mu^4 A_1$. Allora

$$\frac{4A_2^3}{4A_2^3 + 27B_2^2} = \frac{4A_1^3}{4A_1^3 + 27B_1^2} = \frac{4\mu^{-12}A_2^3}{4\mu^{-12}A_2^3 + 27B_1^2} = \frac{4A_2^3}{4A_2^3 + 27\mu^{12}B_1^2}$$

che implica $B_2^2 = (\mu^6 B_1)^2 \implies B_2 = \pm\mu^6 B_1$. Se $B_2 =' \mu^6 B_1$ abbiamo finito, altrimenti pongo $\mu \leftarrow i\mu$ (dove $i^2 = -1$) per cui si avrà ancora $A_2 = \mu^4 A_1$ e inoltre $B_2 = \mu^6 B_1$.

Se $A_1 = 0 \implies j = 0 \implies A_2 = 0$. Inoltre, il determinante $4A_i^3 + 27B_i^2 \neq 0$ implica $B_1, B_2 \neq 0$, quindi $\exists\mu\ .\ B_2 = \mu^6 B_1$. □

Ci sono due particolari valori di j-invariant che compaiono spesso:

- $j = 0$. In questo caso, la cuva è della forma $\mathcal{E} : y^2 = x^3 + B$;
- $j = 1728$. In questo caso, la curva è della forma $\mathcal{E} : y^2 = x^3 + Ax$.

Inoltre, per questi due casi di j-invarianti vi sono importanti automorfismi (omeomorfismi bigettivi dal gruppo in sé stesso), oltre al classico $(x, y) \mapsto (x, -y)$

Esercizio 2.5. Dimostrare:

(i) la mappa $(x, y) \mapsto (x, -y)$ è un automorfismo su $\mathcal{E} : y^2 = x^3 + Ax + B$;
(ii) la mappa $(x, y) \mapsto (\zeta x, -y)$, dove ζ è una 3-radice dell'unità, è un automorfismo su $\mathcal{E} : y^2 = x^3 + B$;
(iii) la mappa $(x, y) \mapsto (-x, iy)$, dove $i^2 = 1$, è un automorfismo su $\mathcal{E} : y^2 = x^3 + Ax$.

Dimostrazione. Siano $P = (x_1, y_1)$, $Q = (x_2, y_2)$ punti, e la loro somma $P + Q = (x_3, y_3)$, dove:

$$\begin{cases} x_3 = m^2 - x_2 - x_1 \\ y_3 = m(x_1 - x_3) + y_1 \end{cases} \qquad m = \frac{y_2 - y_1}{x_2 - x_1}$$

(i). La mappa $\varphi : P \mapsto -P$ è una mappa razionale e chiusa in $\mathcal{E} : y^2 = x^3 + Ax + B$. Abbiamo che $\varphi(P + Q) = (x_3, -y_3)$, dove

$$\begin{cases} x_3 = (-m)^2 - x_2 - x_1 \\ -y_3 = (-m)(x_1 - x_3) + (-y_1) \end{cases} \qquad -m = \frac{(-y_2) - (-y_1)}{x_2 - x_1}$$

ma questa è proprio la somma $\varphi(P) + \varphi(Q) = (x_1, -y_1) + (x_2, -y_2)$.

(ii). La mappa $\varphi : (x, y) \mapsto (\alpha x, -y)$ definita sulla curva $\mathcal{E} : y^2 = x^3 + B$ su K è chiusa, e razionale. Inoltre, α è definita come una 3-radice dell'unità; segue che $K^{(3)}$ possiede un elemento α di inverso $\alpha^2 = -(\alpha + 1)$ (inverso poiché $\alpha^3 = 1$, e l'uguagliaza si mostra facilmente dall'equazione $x^2 + x + 1 = (x - \alpha)(x - \alpha^2)$). Abbiamo che $\varphi(P + Q) = (\alpha x_3, -y_3)$, dove

$$\begin{cases} \alpha x_3 = [-\alpha^2 m]^2 = (\alpha x_1) - (\alpha x_2) \\ -y_3 = (-m)(x_1 - x_2) - (-y_1) = [-\alpha^2 m][(\alpha x_1) - (\alpha x_2)] - (-y_1) \end{cases}$$

Nota: per cercare le soluzioni posso risolvere in β l'equazione $(-m)(x_1 - x_2) = \beta m(\alpha x_1 - \alpha x_2)$.

(iii). La mappa $\varphi : (x, y) \mapsto (-x, iy)$ dove $i^2 = -1$ è una mappa razionale chiusa su $\mathcal{E} : y^2 = x^3 + Ax$ (si verifica immediatamente prendendo un punto nella curva e verificando che la sua immagine vi appartiene ancora). Abbiamo che $\varphi(P + Q) = (-x_3, iy_3)$, dove:

$$\begin{cases} -x_3 = [(-i)m]^2 - (-x_1) - (-x_2) \\ iy_3 = [-im][(-x_1) - (-x_3)] + (iy_1) \end{cases} \qquad -im = \frac{iy_2 - i_1}{(-x_2) - (-x_1)}$$

Ci sarebbe ancora da dimostrare nel caso in cui $P = Q$, ma meh. □

Avere la stessa j-invariante quindi implica che le due curve ellittiche sono isomorfe *sulla chiusura di* K. Nota bene che se lavoriamo solo in K, potrebbero esserci due curve aventi stesso j-invariant ma non esistere un automorfiso che manda una curva nell'altra mediante una mappa razionale.

Definizione 2.6 (Twist)**.** Due curve definite su K aventi lo stesso j-invariant sono dette *twist* l'una dell'altra.

Data una curva ellittica $\mathcal{E} : y^2 = x^3 + Ax + B$ definita su K, dato un $d \in K^\times$, diremo che la curva $\mathcal{E}^{(d)} : y^2 = x^3 + Ad^2 + Bd^3$ è il d-twist della curva $\mathcal{E}$.

`TODO: proseguire con esercizio 2.23`

2.5 Morfismi

Definizione 2.7. Un endomorfismo è un omeomorfismo dato da funzioni razionali sulla curva. Più precisamente, una mappa $\varphi : \mathcal{E}(\overline{K}) \to \mathcal{E}(\overline{K})$ è detta *endomorfismo* o *omeomorfismo* se:

$$\begin{aligned} &\varphi(P + Q) = \varphi(P) + \varphi(Q) \\ &\varphi((x, y)) = (R_1(x, y), R_2(x, y)) \quad \text{dove } R_1, R_2 \text{ sono funzioni razionali} \end{aligned}$$

Segue immediatamente da questo che $\varphi(\infty) = \infty$ e $\varphi(-P) = -\varphi(P)$.

Possiamo esprimere meglio gli endomorfismi: sappiamo che R_1, R_2 sono funzioni razionali, dove posso sostituire ogni potenza pari di y con un polinomio in x e razionalizzare il denominatore. Quindi posso riscrivere i polinomi razionali R_1, R_2 come:

$$R_i(x, y) = \frac{p_1^{(i)}(x) + p_2^{(i)}(x)y}{p_3^{(i)}(x)}$$

. Inoltre, notando che $-\varphi((x, y)) = \varphi(-(x, y)) = \varphi((x, -y))$ segue che $R_1(x, -y) = R_1(x, y) \implies p_2^{(1)} = 0$ e $R_2(x, -y) = -R_2(x, y) \implies p_1^{(2)}(x) = 0$. Segue:

$$\varphi(x, y) = (r_1(x), r_2(x)y)$$

dove r_1, r_2 sono polinomi razionali in x.

Diremo che $\varphi((x, y)) = \infty$ quando $r_1(x) = p(x)/q(x)$ è tale che $q(x) = 0$.

Definizione 2.8 (Grado)**.** Il grado di un endomorfismo $\varphi : (x, y) \mapsto (p/q(x), r(x)y)$ è il massimo dei gradi tra p, q.
Se $\varphi = 0$ è l'endomorfismo banale, diremo che $\deg \varphi = 0$.

Definizione 2.9 (Separabilità)**.** Un endomorfismo $\varphi : (x, y) \mapsto (r_1(x), r_2(x)y)$ non identicamente nullo è detto separabile se $r_1' \neq 0$, o equivalentemente $p' = 0 \ \wedge \ q' = 0$.

Proposizione 2.10. *Siano $p(x)$ e $q(x)$ due polinomi senza radici comuni.*

$$\frac{d}{dx}\left[\frac{p(x)}{q(x)}\right] = 0 \iff p' = 0 \ \wedge \ q' = 0$$

Dimostrazione. " $\Longleftarrow$ " è banale:

$$\frac{d}{dx}\left[\frac{p(x)}{q(x)}\right] = \frac{p'q + q'p}{q^2} = 0.$$

" $\Longrightarrow$ " Se $r_1' = 0$ allora o r_1 è costante, oppure stiamo in un campo di caratteristica prima ch $K = P$. Quindi

$$r_1(x) = r_0(x^P) = \frac{p_0(x^P)}{q_0(x^P)} \implies \begin{cases} p'(x) = p_0'(x^P) = 0 \\ q'(x) = q_0'(x^P) = 0 \end{cases}$$

□

Teorema 2.11 (Mappa di Frobenius)**.** *La mappa di Frobenius $\phi_q : \mathcal{E}(\bar{\mathbb{F}}_q) \to \mathcal{E}(\bar{\mathbb{F}}_q)(x, y) \mapsto (x^q, y^q)$ è un endomorfismo non separabile.*

Dimostrazione.

"*Endomorfismo.***"** Siano $P = (x_1, y_1)$ e $Q = (x_2, y_2) \in \mathcal{E}(\mathbb{F}_q)$.
Se $x_1 = x_2$ allora $\infty = \varphi(P + Q) = \varphi(P) + \varphi(Q)$. Se $P \neq Q$ allora $\varphi(P + Q) = (x_3, y_3)$ con:

$$x_3 = m^2 - x_1^q - x_2^q, \quad y_3 = m(x_1^q - x_3^q) - y_1^q, \quad \text{dove } m = \frac{y_2^q - y_1^q}{x_2^q - x_1^q}$$

che è proprio la somma $\varphi(P) + \varphi(Q)$. Se $P = Q$ similmente abbiamo $\varphi(2Q) = (x_3, y_3)$ con:

$$x_3 = m^2 - 2x_1^q \quad y_3^q = m(x_1^q - x_3^q) - y_1^q \quad \text{dove } m = \frac{3^q(x_1^q)^2 + A^q}{2^q y)1^q}$$

e poiché $2, 3, A \in \mathbb{F}_q$ per Eulero-Fermat sono invarianti rispetto a Frobenius.
"*Non Separabile.***"** Immediato da $q = 0$ in $\mathbb{F}_q \implies (x^q)' = 0$.

□

Proposizione 2.12. *Sia φ un endomorfismo non separabile su una curva ellittica $\mathcal{E}$. Allora:*

$$\deg \varphi = |\ker \varphi|$$

Dimostrazione. ?? [non l'ho capita, perché (a,b) sono il kernel?] □

Teorema 2.13. *Gli endomorfismi su curve ellittiche sono tutti surgettivi.*

Dimostrazione. ?? □

2.6 Curve Ellittiche (mod n)

Definizione 2.14 (Tupla Primitiva)**.** Sia R un anello. Una tupla $x_1, x_2, \ldots, x_n$ è detta primitiva sse:

$$\exists r_1, r_2, \ldots, r_n \ . \ r_1x_1 + r_2x_2 + \cdots + r_nx_n = 1.$$

Se $R = \mathbf{Z}_n$, tale condizione è equivalente a cheidere che $\gcd(n, x_1, x_2, \ldots, x_n) = 1$. Se R è un campo, tale condiziona implica che almeno uno degli x_i sia nonzero.

In generale, $x_1, x_2, \ldots, x_n$ è primitiva se l'ideale da essa generato è R.

Diremo che due triple primitive (x, y, z) e (x', y', z') sono equivalenti se esiste un elemento invertibile $u \in R^\times$ tale che $(x', y', z') = (ux, uy, uz)$.

Chiamando il rappresentante della classe di equivalenza di (x, y, z) come $(x : y : z)$ possiamo definire lo spazio proiettivo

$$\mathbf{P}^2(R) = \{(x : y : z) \in R^3 : x, y, z \text{ primitiva}\}$$

Si nota anzitutto che se R è un campo questo è proprio il genere di proiettivizzazione che era stata fatta nella Sezione 2.2.

Proposizione 2.15. *Sia R un anello tale che $\mathbf{Z} \subset R \subset \mathbf{Q}$. Allora $\mathbf{P}^2(R) = \mathbf{P}^2(\mathbf{Z})$.*

Dimostrazione. È sufficiente notare che dato un elemento $(x : y : z)$ di $\mathbf{P}^2(\mathbf{Q})$, è possibile trovare un altro rappresentante della sua classe di equivalenza che abbia elementi solo interi, di massimo comun divisore 1. Segue che $\mathbf{P}^2(\mathbf{Q}) = \mathbf{P}^2(\mathbf{Z})$. A questo punto la tesi è immediata. □

Per poter lavorare con le curve ellittiche $\pmod n$ servono due condizioni:

- $2 \in R^*$;
- ogni matrice $(a_{ij}) \in \mathcal{M}^{m\times n}(R)$ tale che i suoi termini sono primitivi - i.e., $(a_1 1, \ldots, a_m n) = 1$ - e ogni sottomatrice 2×2 è singolare allora esiste una combinazione R-lineare che forma una tupla primitiva.

La prima condizione è necessaria per poter lavorare con l'equazione di Wiertrass. A rigor di logica dovremmo anche specificare che stiamo lavorando su $\mathbf{Z}_{(2)} = \{\, x/2^k \mid k \geq 0 \,\}$, ma questa è una finezza tecnica visto che comunque $\mathbf{P}^2(\mathbf{Z}_{(2)}) = \mathbf{P}^2(\mathbf{Z})$.

2.7 Caratteristica due

Per questo specifico caso, non possiamo usare l'equazione di Wierstrass generale. Infatti, se siamo in caratteristica 2, allora la curva affine $f(x, y) = y^2 - x^3 - Ax - B$ ha derivate parziali $(df/dy) = 2y = 0$ e $(df/dx) = -3x^2 - A$. Un qualunque punto che soddisfa $df/dx = 0$ è quindi singolare.

Torniamo quindi all'equazione generale di Wierstrass:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

ed esaminiamo i due casi:

- $a_1 \neq 0$. Allora possiamo fare un cambio di variabili e arrivare alla forma

$$y^2 + xy = x^3 + a_2x^2 + a_6.$$

- $a_1 = 0$. Allora possiamo fare un semplice cambio di variabili $x \leftarrow x - a_2$ e ottenere

$$y^2 + a_3y = x^3 + a_4x + a_6.$$

In entrambi i casi non incorriamo in alcun problema quando proiettivizziamo - il punto all'infinito rimane $(0 : 1 : 0)$ e quanto si vede facilmente omogeneizzando, impostando $z = 0$ e ottenendo $x = 0$.

Quel che cambia è l'opposto, dove è necessario usare la formula generale:

$$-(x, y) = (x, -a_1x - a_3 - y)$$

Esercizio 2.16. Sia $P = (x_0, y_0) \neq \infty$ sulla curva ellittica

$$\mathcal{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Sisa $-P$ l'altro punto di intersezione con la retta $\overline{\infty P}$ su $\mathcal{E}$. Mostrare che $-P = (x, -a_1x - a_3 - y)$.

Dimostrazione. Notiamo che in un'equazione quadratica, il termine lineare è la somma delle soluzioni: $(y-\alpha_1)(y-\alpha_2) = y^2 - (\alpha_1 + \alpha_2)y + \alpha_1\alpha_2$. Mettiamo a sistema $\mathcal{E}$ con la retta $x = x_0$, e otteniamo qualcosa tipo $y^2 + a_1x_0y + a_3y + \cdots$. Segue che:

$$y_0 + y = -(a_1x_{0a3}) \implies y = -a_1x_0 - a_3 - y_0.$$ □

Per qualche ragione a questo punto il Washington riporta a questo punto le formule di duplicazione per entrambi i casi. Visto che non sono troppo difficili, studio di sotto come, dato $P = (x_0, y_0)$, sia possibile calcolare $2P$.

Esaminiamo il primo caso. Abbiamo $\mathcal{E} : y^2 + xy + x^3 + a_2x^2 + a_6 = 0$. Usiamo l'implicit differentiation e otteniamo

$$2y\frac{dy}{dx} + \frac{d[xy]}{dx} + 3x^2 + 2a_2x = \frac{d[xy]}{dx} + x^2 = y + x\frac{dy}{dx} + x^2 = 0.$$

Stiamo cerando la retta tangente a P $y = m(x - x_0) + y_0 = mx + b$, dove $m = (dy/dx) = (x^2 + y)/x$ e $b = mx_0 + y_0$. Sostituendo nell'equazione iniziale otteniamo che

$$\begin{aligned} 0 &= (mx + b)^2 + x(mx + b) + x^3 + a_2x^2 + \cdots = (m^2 + m + a_2)x^2 + \cdots \\ \implies & x_0 + x_0 + x_1 = x_1 = m^2 + m + a_2. \end{aligned}$$

Nel secondo caso abbiamo equazione della curva:

$$\mathcal{E} : y^2 + a_3y + x^3 + a_4x + a_6 = 0.$$

Anche qui, procedo allo stesso modo usando implicit differentiation, e ottengo che $m = (dy/dx) = (x^2 + a_4)/a_3$. Come prima, sostituisco $y = mx + b$ e ottengo che $x_0 + x_0 + x_1 = x_1 = m^2$.

2.8 Curve Singolari

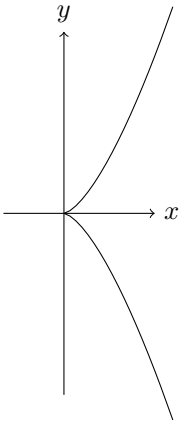
Si distinguono i casi in cui vi sono due radici multiple, e tre radici multiple. Indicheremo con $\mathcal{E}^*$ la curva ellittica a cui sono stati rimossi i punti di singolarità.

Radice tripla

A meno di traslazioni, ci troviamo davanti ad un'equazione della forma

$$x^3 = y^2$$

che ha unica singolarità nel punto $(0, 0)$, e tutte le linee passanti per questo punto hanno al più un altro punto di intersezione con $\mathcal{E}$. Pertanto, volendo costruire un gruppo, decidiamo di escludere questo punto, e definire una somma su tutti gli altri punti.



Teorema 2.17. *La mappa*

$$\varphi : \mathcal{E}^* \to K : \begin{cases} \infty & \mapsto 0 \\ (x, y) & \mapsto x/y \end{cases}$$

è un isomorfismo di gruppi additivi, quindi $K \simeq \mathcal{E}^* = \mathcal{E} - \{(0, 0)\}$.

Dimostrazione. Consideriamo $t = x/y$, allora posso esprimere x, y in funzione di t:

$$x = \left(\frac{y}{x}\right)^2 = \left(\frac{1}{t}\right)^2 \qquad\qquad y = \frac{x}{t} = \left(\frac{y}{x}\right)^2\frac{1}{t} = \left(\frac{1}{t}\right)^3$$

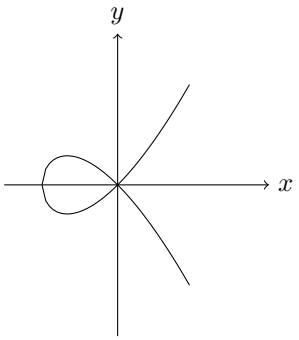
quindi la funzione è bigettiva. Rimane mostrare che è un morfismo di gruppi, e lo si fa per sostituzione, sono un macello di conti. □

Radice doppia

Il caso in cui $y^2 = p(x) = (x - A)^2(x - B)$ possiamo traslare la x ottenendo un'equazione della forma

$$y^2 = x^2(x + a) \qquad [a \neq 0]$$

con unico punto singolare $(0, 0)$, di ordine due.



Tale funzione interseca il fascio di rette passanti per l'origine $y = mx$ sse:

$$\begin{cases} y = mx \\ y^2 = x^3 + ax^2 \end{cases} \implies x^2(m^2 - x - a) = 0 \implies x = 0 \quad \vee \quad x = m^2 - a$$

$x = 0$ ha ordine 3 sse $m = \pm\sqrt{a} = \pm\alpha \in \overline{K}$??.

Teorema 2.18. *Se $\alpha \in K$ allora $\mathcal{E}^*(K) \simeq K^*$; se $\alpha \notin K$ allora $\mathcal{E}^*(K) \simeq \{u + \alpha v : u^2 - av^2 = 1\}$. Il membro di destra è inteso come gruppo moltiplicativo.*

Capitolo 3

Punti di Torsione

Sia G gruppo abeliano finito. Sia K campo su cui vive $\mathcal{E}$, e $\overline{K}$ la sua chiusura algebrica.

Teorema 3.1. $(n,m)=1 \implies \mathcal{E}(\mathbf{Z}/nm\mathbf{Z}) \simeq \mathcal{E}(\mathbf{Z}/n\mathbf{Z}) \times \mathcal{E}(\mathbf{Z}/m\mathbf{Z})$.

Dimostrazione. $\mathcal{E} : y^2z = x^3 + Axz^2 + Bz^3 \quad (A, B \in \mathbf{Z}/nm\mathbf{Z})$ con $\Delta = 3A^3 - 27B^2 \neq 0$. Allora, per il teorema cinese del resto $\Delta \not\equiv 0 \pmod{n}, \Delta \not\equiv 0 \pmod{m}$ e la curva ellittica è ben definita anche sei due gruppi additivi; sempre per il teorema cinese dei resti si ha che:

$$(x:y:z) \in \mathcal{E} \iff y^2z \equiv x^3 + Axz^2 + Bz^3 \pmod{mn} \iff \begin{cases} y^2z \equiv x^3 + Axz^2 + Bz^3 \pmod{n} \\ y^2z \equiv z^2 + Axz^2 + Bz^3 \pmod{m} \end{cases}$$

Abbiamo così mostrato che i due spazi sono in bigezione. Possiamo ridurre anche le formule dell'addizione modulo n, m per dimostrare che la mappa $\varphi : \mathcal{E}(\mathbf{Z}/nm\mathbf{Z}) \to \mathcal{E}(\mathbf{Z}/n\mathbf{Z}) \times \mathcal{E}(\mathbf{Z}/m\mathbf{Z})$ è un morfismo, i.e. $\varphi(P+Q) = \varphi(P) + \varphi(Q)$. □

Teorema 3.2. *G è prodotto finito di gruppi ciclici, cioè isomorfi a $\mathbf{Z}/n\mathbf{Z}$ in modo essenzialmente unico.*

Dimostrazione. La prima parte è immediata, dato che G è unione dei suoi gruppi ciclici, e per il teorema cinese del resto $(n,m)=1 \implies \mathbf{Z}/nm\mathbf{Z} \simeq \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$. Si ha quindi che $G = G_1 \times \cdots \times G_k \simeq \mathbf{Z}/h_1\mathbf{Z} \times \cdots \times \mathbf{Z}/h_k\mathbf{Z}$ con $(a,b) \in G_i \times G_j \ \wedge \ k \equiv kb \equiv 0 \implies k(a,b) \equiv 0$. Per farlo mi basta prendere un scegliere il primo $p_i^{e_i}$ con esponente massimo, e considerare il gruppo ridotto. Tale rappresentazione è unica. □

Definizione 3.3 (Punti di Torsione)**.** $\mathcal{E}[n] = \{P \in \mathcal{E}(\overline{K}) : nP = \infty\}$ è detto insieme dei punti di torsione.

Esempio 3.4. Punti di torsione su un toro. $T^1[n] \simeq (S_1 \times S_1)[n] \simeq S_1[n] \times S_1[n]$ che ha come soluzioni tutti i multipli di $2\pi/n$.

Pertanto $T^1 \simeq \mathbf{Z}/n\mathbf{Z}^2$.

Esempio 3.5 (Caso $\mathcal{E}[2]$). Sia $\mathrm{ch}(K) \neq 2$. Allora $\mathcal{E}[2] = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Possiamo scrivere l'equazione per $\mathcal{E}$ come $y^2 = (x-e_1)(x-e_2)(x-e_3)$ da cui segue che $2P = \infty \iff$ la retta tangente è verticale, i.e. $y = 0$. Pertanto

$$\mathcal{E}[2] = \{\infty, (e_1,0), (e_2,0), (e_3,0)\} \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$$

.

Se invece $\mathrm{ch}(K) = 2$, si hanno le due equazioni possibili. Anche qui $2P = 0 \implies$ la tangente sul punto è verticale $\implies y = 0$.

- $f : y^2 + a_3y + x^3 + a_4x + a_6 = 0 \implies \frac{\partial f}{\partial y} = 2y - a_3 = 0$ con $a_3 \neq 0$ per ipotesi $\implies \mathcal{E}[n] = \{\infty\}$.
- $f : y^2 + xy + x^3 + a_2x^2 + a_6 = 0 \implies \mathcal{E}[2] = \{\infty, (0, \sqrt{a_6})\} \simeq \mathbf{Z}/2\mathbf{Z}$.

Esempio 3.6 (Caso $\mathcal{E}[3]$). Se $\mathrm{ch}(K) \neq 3 \implies 2P = -P \implies 2P_x = P_x$. usando le formule per la tangente viene fuori

$$m^2 - 2x = x \text{ dove } m = \frac{3x^2 + A}{2y}$$

da cui salta fuori un'equazione di quarto grado con discriminante non nullo, da cui segue che vi sono $4 \cdot 2 = 8$ soluzioni, a cui si aggiunge ∞. Visto come gruppo astratto, $G \simeq \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$. Se il campo ha caratteristica 3 si avrà invece $G \simeq \mathbf{Z}/3\mathbf{Z}$ oppure $\{\infty\}$.

Vale la pena notare che nel piano proiettivo, il polinomio omogeneo F ha soluzione in $(0:0:0)$, e che per il teorema di Eulero tutti i punti di singolarità posson esser trovati mediante

$$\sum_i x_i \frac{\partial F}{\partial x_i} = dF \implies x\frac{\partial F}{\partial x}(0) + y\frac{\partial F}{\partial y}(0) + z\frac{\partial F}{\partial z}(0) = dF = 0 \tag{3.1}$$

Teorema 3.7. *Sia $\mathcal{E}$ curva ellittica, n intero positivo. Allora, $\mathcal{E}[n] \simeq \mathbf{Z}/n\mathbf{Z}^2$ se $\mathrm{ch}(K) \nmid n$. Altrimenti $n = p^e m \quad (con\ (p,m) = 1)$ e $\mathcal{E}[n] = \mathcal{E}[m] \times \mathcal{E}[p^e]$.*

Se $\mathcal{E}[p^e] \simeq \{\infty\}$ allora la curva ??