ALGEBRA 2 – LEZIONI DAL 16 DICEMBRE 2003 AL 21 GENNAIO 2004

Sommario delle lezioni:

- 16 Dic: **Lezione 27**. Estensioni di campi. Grado di un'estensione. Estensioni finite. Elementi algebrici e trascendenti. Polinomio minimo di un elemento algebrico. Il polinomio minimo è irriducibile. α è algebrico su $F \Leftrightarrow F(\alpha)$ è un estensione finita di $F \Leftrightarrow F[\alpha] = F(\alpha)$. $[L : F] = [L : K][K : F]$. Se α e β sono algebrici su F, $F(\alpha, \beta)$ è un'estensione finita di F. Gli elementi di L che sono algebrici su F formano un campo. $F(\alpha)$ è isomorfo a $F[x]/(q(x))$, dove q è il polinomio minimo di α. *(due ore)*
- 17 Dic: **Lezione 28**. Costruzione di un'estensione di F in cui un polinomio irriducibile $p(x) \in F[x]$ abbia una radice. Campi con quattro elementi. Due campi con nove elementi. Isomorfismo esplicito tra $\mathbb{F}_3[x]/(x^2 + 1)$ e $\mathbb{F}_3[x]/(x^2 + x - 1)$. Esistenza di campi di spezzamento. *(un'ora)*
- 12 Gen: **Lezione 29**. Campi di spezzamento. Un isomorfismo di campi si estende ad un isomorfismo di campi di spezzamento. Il campo di spezzamento di un polinomio è unico a meno di isomorfismo. Classificazione dei campi finiti. Un campo finito con p^n elementi è campo di spezzamento del polinomio $x^{p^n} - x$. Due campi finiti con lo stesso numero di elementi sono isomorfi. Esistenza del campo con p^n elementi. Automorfismo di Frobenius. Teorema dell'elemento primitivo per campi finiti. *(due ore)*
- 13 Gen: **Lezione 30**. La corrispondenza di Galois. Teorema dell'elemento primitivo per campi di caratteristica 0. Estensioni di Galois. Gruppo di Galois di un'estensione, campo fisso di un gruppo di automorfismi. Esempi: $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{2}, \omega)$, $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Corrispondenza tra sottogruppi del gruppo di Galois ed estensioni intermedie. Gli automorfismi di un'estensione permutano le radici di un polinomio irriducibile. Se G è un gruppo finito di automorfismi di K, allora l'estensione $K^G \subset K$ è un'estensione algebrica. *(due ore)*
- 14 Gen: **Lezione 31**. Se G è un gruppo di automorfismi di K, allora $[K : K^G] = |G|$. L'ordine del gruppo di Galois divide il grado dell'estensione. Se $F \subset K$ è un'estensione di Galois, un polinomio irriducibile in $F[x]$ che ammetta una radice in K si spezza in K. Un'estensione di Galois è un campo di spezzamento. Se $F \subset K$ è di Galois, il campo fisso per il gruppo di Galois è esattamente F. Un campo di spezzamento è un'estensione di Galois. Corrispondenza di Galois. *(un'ora)*
- 19 Gen: **Lezione 32**. Fine della dimostrazione del teorema fondamentale della teoria di Galois. Costruzioni con riga e compasso. Impossibilità della duplicazione del cubo, della quadratura del cerchio, della costruzione dell'ettagono regolare. *(due ore)*
- 20 Gen: **Lezione 33**. Estensioni ciclotomiche di $\mathbb{Q}$. Costruibilità con riga e compasso dell'n-agono regolare quando n è un primo di Fermat. Un esercizio sugli anelli. *(due ore)*
- 21 Gen: **Lezione 34**. Risoluzione di un'equazione algebrica per radicali. *(un'ora)*

1. Fattorizzazione di polinomi ed irriducibilità

In queste note raccolgo alcuni risultati che non sono riuscito, per motivi di tempo, a trattare durante il corso. Dal momento che non sono complicati, e che aiutano la comprensione di alcuni fenomeni di teoria di campi, preferisco trattarli al di fuori del corso piuttosto che saltarli del tutto.

Le cose che vado a raccontare sono: il lemma di Gauss e la fattorialità dell'anello dei polinomi a coefficienti in un dominio a fattorizzazione unica, il teorema fondamentale dell'algebra, alcuni criteri di irriducibilità dei polinomi a coefficienti negli interi.

1.1. Il lemma di Gauss e la fattorizzazione unica negli anelli di polinomi.

In quello che segue, D sarà sempre un dominio a fattorizzazione unica, e $\mathfrak{p}$ un ideale primo. Ricordiamo che i domini a fattorizzazione unica non sono necessariamente ad ideali principali, sebbene questi siano praticamente gli unici esempi che abbiamo incontrato finora.

Date: 27 gennaio 2004.

In un dominio a fattorizzazione unica ogni elemento ammette una fattorizzazione come prodotto (finito) di elementi irriducibili, e ogni elemento irriducibile è primo, cioè genera un ideale primo. Il succo del lemma di Gauss è la seguente affermazione:

Lemma 1.1. *Sia A un anello, e $\mathfrak{p}$ un suo ideale primo. Allora la famiglia $\mathfrak{p}[x]$ dei polinomi a coefficienti in $\mathfrak{p}$ è un ideale primo dell'anello $A[x]$.*

Dimostrazione. Il quoziente $A/\mathfrak{p}$ è un dominio di integrità, e quindi tale è anche l'anello dei polinomi $(A/\mathfrak{p})[x]$. Sia $\pi : A[x] \to (A/\mathfrak{p})[x]$ l'applicazione di riduzione modulo $\mathfrak{p}$ dei coefficienti di un polinomio. L'applicazione π è un omomorfismo di anelli, ed il suo nucleo è costituito dai polinomi i cui coefficienti giacciono in $\mathfrak{p}$: in altre parole $\ker \pi = \mathfrak{p}[x]$. Ma allora $(A/\mathfrak{p})[x] \simeq A[x]/\mathfrak{p}[x]$: poiché $(A/\mathfrak{p})[x]$ è un dominio di integrità, $\mathfrak{p}[x]$ deve essere un ideale primo di $A[x]$. □

Se ora D è un dominio a fattorizzazione unica, dato un polinomio $p(x) \in D[x]$ possiamo definire il suo "*contenuto*" come il massimo comun divisore dei suoi coefficienti: il contenuto di $f(x)$ si indica con $c(f(x))$. Un polinomio è primitivo se ha contenuto 1. In altre parole, il contenuto di un polinomio è il "più grande" fattore in D che possiamo raccogliere a fattor comune da $p(x)$.

Lemma 1.2 (Gauss)**.** *Il prodotto di polinomi primitivi è ancora un polinomio primitivo.*

Dimostrazione. Siano $f(x), g(x) \in D[x]$ polinomi a coefficienti in D. Se il loro prodotto $f(x)g(x)$ non è primitivo, allora il $c(fg)$ è diverso da 1, e possiamo quindi trovare un elemento primo π che lo divide. Se $\mathfrak{p} = (\pi)$ è l'ideale primo generato da π, allora $f(x)g(x) \in \mathfrak{p}[x]$. Ma $\mathfrak{p}[x]$ è un ideale primo di $D[x]$, e quindi almeno un fattore appartiene a $\mathfrak{p}[x]$. Quindi se il prodotto di $f(x)$ e $g(x)$ non è primitivo, allora almeno uno tra $f(x)$ e $g(x)$ non è primitivo. In altre parole, se $f(x)$ e $g(x)$ sono entrambi primitivi, anche il loro prodotto deve esserlo. □

Corollario 1.3. *Il contenuto del prodotto di due polinomi in $D[x]$ è pari al prodotto dei contenuti dei polinomi.*

Dimostrazione. Se $f(x) = c(f)\overline{f(x)}$ e $g(x) = c(g)\overline{g(x)}$, allora i polinomi $\overline{f(x)}$ e $\overline{g(x)}$ sono primitivi. Il prodotto $f(x)g(x)$ è pari a $c(f)c(g)\overline{f(x)}\,\overline{g(x)}$, ed è quindi il prodotto di $c(f)c(g)$ e di un polinomio primitivo. Il suo contenuto è quindi $c(f)c(g)$. □

Siamo pronti a mostrare il risultato fondamentale di questo paragrafo. Sia D un dominio a fattorizzazione unica, e $D[x]$ il suo anello dei polinomi. Sappiamo che D si immerge nel suo campo delle frazioni F, e alla stessa maniera $D[x]$ si immerge nell'anello $F[x]$, che è un dominio a ideali principali, ed è quindi a fattorizzazione unica. Possiamo quindi pensare di utilizzare la fattorizzazione di polinomi in $F[x]$ per fattorizzare un polinomio in $D[x]$. Questa strategia è vincente! Il punto essenziale per mostrarlo è il seguente:

Proposizione 1.4. *Sia $p(x)$ un elemento di $D[x]$. Allora $p(x)$ è irriducibile in $D[x]$ se e solo se è irriducibile in $F[x]$. In altre parole, ogni polinomio in $D[x]$ che si esprime come prodotto di polinomi a coefficienti in F si esprime anche come prodotto di polinomi a coefficienti in D.*

Dimostrazione. Dobbiamo innanzitutto comprendere che cosa rappresenti una fattorizzazione di $p(x) \in D[x]$ nell'anello $F[x]$. Gli elementi di F sono frazioni del tipo a/b, dove a, b sono elementi di D. Dato un polinomio $f(x) \in F[x]$ è sempre possibile imporre un denominatore comune ai coefficienti di $f(x)$ ed esprimerlo come rapporto tra un polinomio in $D[x]$ ed un unico denominatore in D. Pertanto una fattorizzazione

$$p(x) = f_1(x)f_2(x)$$

si riduce a

$$p(x) = \frac{F_1(x)}{d_1} \cdot \frac{F_2(x)}{d_2} = \frac{F_1(x)F_2(x)}{d_1 d_2},$$

dove $F_1, F_2 \in D[x]$ e $d_1, d_2 \in D$. Pertanto una fattorizzazione di $p(x)$ in $F[x]$ fornisce una fattorizzazione di $dp(x) = d_1 d_2 p(x) = F_1(x)F_2(x)$ in $D[x]$. Siamo ora pronti a mostrare che se un polinomio $p(x) \in D[x]$ si fattorizza in $F[x]$, si fattorizza allora anche in $D[x]$.

Se $p(x)$ si fattorizza in $F[x]$, allora esiste un elemento $d \neq 0$ in D tale che il multiplo $dp(x)$ si fattorizza in $D[x]$:

$$dp(x) = a(x)b(x).$$

Questo può succedere per diversi valori di $d \in D$: il nostro scopo è dimostrare che accade anche per $d = 1$.

Scegliamo, tra tutti i $d \in D$ tali che $dp(x)$ si fattorizzi in $D[x]$, uno per cui il numero dei fattori di una sua fattorizzazione in elementi primi di D sia minimo[1]. Se d non è invertibile, allora possiamo trovare un primo π che divide d: scriviamo $d = \pi d'$ ed indichiamo con $\mathfrak{p}$ l'ideale primo (π) generato da π.

Sappiamo quindi che $dp(x) \in \mathfrak{p}[x]$. Dal momento che $dp(x) = a(x)b(x)$, e che $\mathfrak{p}$ è un ideale primo, otteniamo che almeno uno tra $a(x)$ e $b(x)$ – diciamo $a(x)$ – appartiene a $\mathfrak{p}$. Ma allora tutti i suoi coefficienti sono multipli di π, e possiamo scrivere $a(x) = \pi A(x)$, dove $A(x) \in D[x]$. Otteniamo quindi

$$\pi d' p(x) = dp(x) = a(x)b(x) = \pi A(x)b(x),$$

da cui $d'p(x) = A(x)b(x)$. Pertanto anche $d'p(x)$ si fattorizza come prodotto di polinomi a coefficienti in D, e il numero di fattori in una fattorizzazione in primi di d' è uno in meno che per d, un assurdo. L'unica possibilità è che il d minimale sia invertibile. Ma allora anche $p(x)$ si fattorizza in $D[x]$, da cui la tesi. □

Teorema 1.5. *Sia D un dominio a fattorizzazione unica. Allora l'anello $D[x]$ è un dominio a fattorizzazione unica.*

Dimostrazione. L'esistenza della fattorizzazione si dimostra per induzione sul grado del polinomio $p(x)$ da fattorizzare mentre la sua unicità segue dall'unicità della fattorizzazione nell'anello $F[x]$, e dal fatto che gli elementi irriducibili sono gli stessi in $D[x]$ e in $F[x]$. □

Corollario 1.6. *Gli anelli $\mathbb{Z}[x_1, ..., x_n]$ e $F[x_1, ..., x_n]$, dove F è un campo, sono domini a fattorizzazione unica.*

Gli anelli $\mathbb{Z}[x_1, ..., x_n]$ e $F[x_1, ..., x_n]$ costituiscono esempi di domini a fattorizzazione unica in cui non ogni ideale è principale.

1.2. **Il criterio di Eisenstein.** Può capitare, come vedremo in teoria dei campi, che un problema di algebra si riduca alla fattorizzazione di un polinomio in polinomi irriducibili. Può essere utile avere qualche metodo utile a portata di mano.

Proposizione 1.7 (Criterio di Eisenstein)**.** *Sia $a(x) = x^m + a_{m-1}x^{m-1} + ... + a_1x + a_0$ un polinomio a coefficienti in $\mathbb{Z}$. Se un primo p divide tutti gli a_i ma p^2 non divide a_0, allora $a(x)$ è irriducibile.*

Dimostrazione. Sia $a(x) = f(x)g(x)$ una fattorizzazione di $a(x)$, dove $f(x) = \sum_i f_i x^i$, $g(x) = \sum_i g_i x^i$. Allora $a_0 = f_0 g_0$. Poiché a_0 è divisibile per p, ma non per p^2, solo uno tra f_0 e g_0 è multiplo di p. A meno di scambiare il ruolo di f e g possiamo supporre che sia f_0 ad essere divisibile per p. Pertanto $p|f_0$ e $p \not| g_0$.

Mostriamo adesso per induzione che p divide tutti i coefficienti di $f(x)$ fino a quello di grado $m-2$. Supponiamo di sapere che p divide i coefficienti $f_0, f_1, ..., f_n$. Il coefficiente $a_{n+1} = f_{n+1}g_0 + f_n g_1 + ... + f_1 g_n + f_0 g_{n+1}$ è divisibile per p, come tutti gli addendi dopo il primo nel secondo membro. Quindi anche $f_{n+1}g_0$ è divisibile per p, da cui $p|f_{n+1}$.

Ora, se il grado di $g(x)$ è superiore ad 1, allora tutti i coefficienti di $f(x)$ sono divisibili per p, mentre $a(x)$ ha il primo coefficiente uguale ad 1, ed è quindi primitivo.

Se invece $g(x) = x + g_0$ ha grado 1, allora $a(x) = 0$ ammette una soluzione intera $x_0 = -g_0$. Ma questo è impossibile: infatti se p divide x_0, allora p^2 divide $x_0^m + a_{m-1}x_0^{m-1} + ... + a_1 x_0$, mentre per ipotesi non divide a_0. La somma di questi due termini non può quindi annullarsi. Se al contrario p non divide x_0, allora divide tutti i termini di grado minore di m, ma non divide x^m, e si conclude alla stessa maniera. □

Esempi:

- I polinomi $x^4 + 2$, $x^4 + 3$ sono irriducibili. Infatti il criterio di Eisenstein si applica al primo polinomi con il primo $p = 2$ ed al secondo con il primo $p = 3$.
- Il polinomio x^4+4 è riducibile su $\mathbb{Z}$. Infatti $x^4+4 = x^4+4x^2+4-4x^2 = (x^2+2)^2-(2x)^2 = (x^2 + 2x + 2)(x^2 - 2x + 2)$.

[1] Ad esempio, in $\mathbb{Z}$ sarebbe preferibile 35 a 12, perché $35 = 5 \cdot 7$ è prodotto di due primi, mentre $12 = 2 \cdot 2 \cdot 3$ è prodotto di tre fattori primi

- Il polinomio $x^4 + 9$ è irriducibile sugli interi. Si vede facilmente come non possieda soluzioni razionali – in realtà non ne possiede neanche di reali! – e quindi non ammette fattori lineari che lo dividano. Bisogna tuttavia scartare anche l'eventualità che $x^4 + 9$ si fattorizzi come prodotto di due polinomi di secondo grado. Se questo accade allora

$$x^4 + 9 = (x^2 + ax + b)(x^2 + cx + d),$$

dove a, b, c, d sono numeri interi, e i fattori a secondo membro sono monici in quanto il prodotto dei primi coefficienti deve essere 1: a meno di cambiare segno ad entrambi possiamo supporre che siano entrambi uguali ad 1. Sviluppando il prodotto si ottengono le equazioni $a + c = 0$, $b + d + ac = 0$, $ad + bc = 0$, $bd = 9$, che dobbiamo risolvere sugli interi. Dalla prima otteniamo $c = -a$, da cui $ad + bc = a(d - b) = 0$. Quindi $a = 0$ oppure $d = b$.

Ma se $a = c = 0$, allora $b + d + ac = b + d = 0$, che è incompatibile con $-b^2 = bd = 9$. Invece, se $b = d$, allora da $bd = 9$ segue $b = d = \pm 3$ e quindi $0 = ac + b + d = -a^2 + 2b$ da cui $a^2 = \pm 6$. Ma ± 6 non sono quadrati di interi, e quindi anche questa possibilità è da scartare. Il polinomio $x^4 + 9$ non ammette fattori né di primo né di secondo grado, ed è quindi irriducibile. Si noti che il criterio di Eisenstein non si applica a tale polinomio, pur essendo irriducibile.
- Sia p un numero primo. Il polinomio ciclotomico $\Phi_p(x) = x^{p-1} + x^{p-2} + ... + x + 1$ è irriducibile. Possiamo infatti facilmente calcolare $\Phi_p(x+1)$: dal momento che $\Phi_p(x) = (x^p - 1)/(x - 1)$ avremo $\Phi_p(x + 1) = ((x + 1)^p - 1)/x$ e quindi

$$\Phi_p(x + 1) = x^p - 1 + \binom{p}{1} x^{p-2} + \binom{p}{2} x^{p-3} + ... + \binom{p}{p-2} x + \binom{p}{p-1}.$$

E' facile vedere come tutti i coefficienti successivi al primo di tale polinomio siano divisibili per p, e come il termine noto non sia divisibile per p^2. Pertanto $\Phi_p(x + 1)$ è irriducibile, e quindi anche $\Phi_p(x)$ lo è. Infatti una fattorizzazione di $\Phi_p(x)$ fornirebbe una fattorizzazione di $\Phi_p(x + 1)$.

1.3. **Radici razionali di polinomi a coefficienti interi.**

Lemma 1.8. *Sia $f(x) = f_n x^n + ... + f_1 x + f_0$ un polinomio a coefficienti interi, e sia a/b una sua soluzione razionale, con $(a, b) = 1$. Allora se un primo p divide a, p deve dividere anche f_0, mentre se divide b, deve dividere anche f_n.*

In altre parole le soluzioni razionali di un polinomio a coefficienti interi si ottengono tutte come rapporto tra un divisore del termine noto ed uno del primo coefficiente.

Dimostrazione. Sia $f(a/b) = 0$. Semplificando i denominatori si ottiene:

$$f_n a^n + f_{n-1} a^{n-1} b + ... + f_1 a b^{n-1} + f_0 b^n = 0.$$

Se p divide a, allora p divide tutti gli addendi tranne al più l'ultimo, e ne divide anche la somma. Pertanto p divide anche $f_0 b^n$. Essendo primo con b, in quanto $(a, b) = 1$, allora dividerà necessariamente f_0. La seconda parte dell'enunciato si dimostra in maniera analoga. □

Esempi:

- Il polinomio $x^3 + 15x + 4$ è irriducibile sugli interi. Se fosse riducibile, infatti, avrebbe almeno un fattore lineare, e quindi una radice (intera) razionale. Ma le possibili radici razionali sono soltanto $\pm 1, \pm 2, \pm 4$, e si controlla facilmente (sostituendo) che nessuno di questi valori soddisfa il polinomio dato.
- Il polinomio $4x^3 - 15x - 2$ è riducibile sugli interi. Per cercarne soluzioni razionali, scriviamo tutti i possibili rapporti tra divisori del termine noto e divisori del primo coefficiente: essi sono $\pm 2, \pm 1, \pm 1/2, \pm 1/4$. Sostituendo nel polinomio, scopriamo che 2 è l'unico di tali valori ad annullare il polinomio, e ne è quindi l'unica radice razionale. Dividendo per $x - 2$ otteniamo $4x^3 - 15x - 2 = (x - 2)(4x^2 + 8x + 1)$. Dal momento che $x = 2$ non è soluzione del polinomio $4x^2 + 8x + 1$, esso è allora sicuramente irriducibile, non essendoci altre radici razionali di $4x^3 - 15x - 2$.

1.4. **Riduzione modulo n.** Verificare la riducibilità o l'irriducibilità di un polinomio a coefficienti negli interi modulo n è talvolta molto semplice. Ad esempio il polinomio $x^2 + x + 1 \in \mathbb{F}_2[x]$ è sicuramente irriducibile. Infatti si spezza in fattori lineari solo se ammette soluzioni in $\mathbb{F}_2$: per controllare se questo succeda dobbiamo sostituire in $x^2 + x + 1$ ogni elemento di $\mathbb{F}_2$. Ma ve ne sono soltanto due: 0 e 1. Sostituendo vediamo che questi due valori non sono soluzioni, e che quindi $x^2 + x + 1$ è un polinomio irriducibile. E' in effetti l'unico polinomio irriducibile di secondo grado. Gli altri sono

$$x^2 = x \cdot x, \qquad x^2 + 1 = (x + 1)(x + 1), \qquad x^2 + x = x(x + 1).$$

Allo stesso modo, troviamo i polinomi irriducibili di grado 3: essi sono

$$x^3 + x + 1, \qquad x^3 + x^2 + 1.$$

Ora, l'applicazione che associa ad un polinomio in $\mathbb{Z}[x]$ il polinomio ottenuto prendendo i suoi coefficienti modulo 2 è un omomorfismo di anelli. Pertanto ad una fattorizzazione di un polinomio in $\mathbb{Z}[x]$ corrisponde una fattorizzazione del polinomio corrispondente in $\mathbb{F}_2$. Se il polinomio corrispondente è irriducibile, deve essere irriducibile anche il polinomio dal quale siamo partiti.
Esempi:

- Il polinomio $x^3 + 15x + 25$ è irriducibile sugli interi. In effetti la sua riduzione modulo 2 è il polinomio $x^3 + x + 1$ che è irriducibile su $\mathbb{F}_2$.
- Il polinomio $4x^2 - 7x - 16$ è irriducibile sugli interi dal momento che la sua riduzione modulo 3 è irriducibile su $\mathbb{F}_3$. Infatti sostituendo i valori $x = 0, 1, 2$ in $x^2 + 2x + 2$ otteniamo $2, 2, 1$ e quindi $x^2 + 2x + 2$ non può spezzarsi in fattori lineari.
- Il polinomio $4x^2 + 8x + 1$ è irriducibile su $\mathbb{Z}$ in quanto la sua riduzione modulo 5 è irriducibile modulo 5. Essa è $-x^2 + 3x + 1$, ed i suoi valori su $0, 1, 2, 3, 4$ sono $1, 3, 3, 1, 2$.
- Attenzione! Il polinomio $x^4 + 1$ è irriducibile su $\mathbb{Z}$, eppure la sua riduzione modulo p è riducibile per ogni primo p. (Mostratelo!)

1.5. **Il teorema fondamentale dell'algebra.** Se analizzare l'irriducibilità di polinomi su $\mathbb{Z}$ e su $\mathbb{Q}$ può presentare qualche difficoltà, il panorama è completamente diverso quando analizziamo lo stesso problema sui campi $\mathbb{R}$ e $\mathbb{C}$. Il campo dei numeri complessi è infatti un esempio di *campo algebricamente chiuso*, il che vuol dire che ogni polinomio a coefficienti complessi si spezza nel prodotto di fattori lineari. Questo ha conseguenze anche per il campo dei numeri reali, nel quale i polinomi irriducibili possono avere soltanto grado uno o due.

Il teorema fondamentale dell'algebra ha varie dimostrazioni, tutte di natura più o meno topologica. Ve ne do una sperando abbiate già seguito un corso di topologia, e conosciate il concetto di omotopia e gruppo fondamentale.

Teorema 1.9. *Sia $p(x) = p_n x^n + ... + p_1 x + p_0$ un polinomio non costante a coefficienti in $\mathbb{C}$. Allora esiste un complesso $z_0 \in \mathbb{C}$ tale che $p(z_0) = 0$.*

Dimostrazione. Per semplicità supporremo che $p(x)$ sia monico, cioè che $p_n = 1$. Costruiamo delle applicazioni $f_r : S^1 \to S^1$, $r \in \mathbb{R}_+$, come segue:

$$f_r(\theta) = \frac{p(re^{i\theta})}{|p(re^{i\theta})|}.$$

Questa definizione è ben posta solamente se il denominatore non si annulla, cioè se $p(x)$ non radici di norma pari ad r.

Prima di affrontare la dimostrazione del teorema, facciamo un po' di chiacchiere: è facile descrivere l'applicazione f_r quando r è molto piccolo o molto grande. L'applicazione f_0 è un'applicazione costante. $f_0(\theta)$ calcola $p(0e^{i\theta}) = p(0) = p_0$ e lo rinormalizza: fornisce quindi sempre lo stesso valore. Quando r è molto piccolo, i termini non costanti di $p(x)$ non influiscono granché sul valore di f_r, e quindi $f_r(\theta)$ è una piccola perturbazione di $p_0/|p_0|$.

Per grandi valori di r il quadro è completamente diverso. Infatti il termine che *comanda* è x^n, che per r sufficientemente grande è molto maggiore di tutti gli altri. Pertanto nel calcolare $f_r(\theta)$ possiamo tenere conto soltanto di questo termine. Se $p(x) = x^n$, l'applicazione di f_r si riduce a $f_r(\theta) = n\theta$, e quindi f_r è l'applicazione che gira n volte attorno ad S^1. I comportamenti di f_r per piccoli e grandi valori di r non sono allora compatibili, e questo ci fornirà una dimostrazione del teorema.

Lemma 1.10. *Per grandi valori di r, l'applicazione $f_r : S^1 \to S^1$ è ben definita ed è omotopa a $\theta \mapsto n\theta$.*

Dimostrazione. Sia $R = 2(|p_0| + |p_1| + ... + |p_{n-1}| + 1)$. Se $|x| > R$, abbiamo che $|x^n| > R^n > 2(|p_0| + |p_1 x| + ... + |p_{n-1}x^{n-1}|) \geq 2|p_0 + p_1 x + ... + p_{n-1}x^{n-1}|$. Definiamo $p^t(x) = x^n + t(p_{n-1}x^{n-1} + ...p_1 x + p_0)$. Chiaramente, $p^0(x) = x^n$ mentre $p^1(x) = p(x)$. Inoltre, $p^t(x) = 0$ non ha soluzioni se $|x| > R$.

Allora $f_r^t(\theta) = p^t(re^{i\theta})/|p^t(re^{i\theta})|$ definisce un'omotopia tra $f_r^0(\theta) = n\theta$ e $f_r^1(\theta) = f_r(\theta)$. □

Lemma 1.11. *Supponiamo che il polinomio $p(x)$ non ammetta radici complesse di norma minore o uguale a T Allora l'applicazione $f_r : [O, T] \times S^1 \to S^1$ è un omotopia tra f_0 e f_T.*

Dimostrazione. f_r è ben definita, in quanto il suo denominatore non si annulla. □

Possiamo adesso terminare la dimostrazione. Se $p(x)$ non ammette radici complesse, le applicazioni f_0 e f_r sono omotope per qualsiasi $r \in \mathbb{R}_+$. Ma f_0 è omotopa ad una costante, mentre f_r per r sufficientemente grande ha grado n. Da questo un assurdo. □

Corollario 1.12. *Gli unici polinomi irriducibili in $\mathbb{C}[x]$ sono quelli di grado 1.*

Corollario 1.13. *I polinomi irriducibili in $\mathbb{R}[x]$ sono tutti quelli di grado 1, e quelli della forma $ax^2 + bx + c$, con $b^2 - 4ac < 0$.*

Dimostrazione. Ogni polinomio di grado 1 è necessariamente irriducibile. Quelli di grado 2 sono irriducibili se non hanno radici reali.

Per mostrare che non vi sono altri polinomi irriducibili, utilizziamo il teorema fondamentale dell'algebra. Sia $p(x)$ un polinomio a coefficienti reali di grado maggiore di 2. Per il teorema fondamentale dell'algebra, l'equazione $p(x) = 0$ ammette almeno una soluzione x_0 in $\mathbb{C}$. Se questa soluzione è reale, allora $p(x)$ è divisibile per $x - x_0$, e quindi $p(x)$ è riducibile.

Se invece x_0 non è reale, scriviamo $x_0 = \alpha + \beta i$. Dal momento che i coefficienti di $p(x)$ sono tutti reali, anche il complesso coniugato di x_0 è radice di $p(x)$. Questo mostra che $p(x)$ è divisibile per $(x - \alpha - \beta i)(x - \alpha + \beta i) = x^2 - 2\alpha x + (\alpha^2 + \beta^2)$, un polinomio a coefficienti reali. Anche in questo caso $p(x)$ non può essere irriducibile. □

2. ESTENSIONI DI CAMPI

Siano F, L due campi contenuti uno nell'altro: $F \subset L$. Questa è chiamata una *estensione di campi* e sarà l'oggetto principale del nostro interesse nel resto del corso. Facciamo subito alcune ovvie osservazioni preliminari.

Lemma 2.1. *Sia $F \subset L$ un'estensione di campi. Allora L è uno spazio vettoriale su F. Se $[L : F]$ è la dimensione di L come F-spazio vettoriale, allora $[L : F] = [L : K][K : F]$ per ogni estensione intermedia $F \subset K \subset L$.*

Dimostrazione. Se $\alpha_1, ..., \alpha_m$ è una base di L su K e $\beta_1, ..., \beta_n$ è una base di K su F, si dimostra facilmente che gli mn prodotti $\alpha_i\beta_j$ formano una base di L su F. La dimostrazione data a lezione ricalca quella sull'Herstein. Questo mostra che se $[L : K] = m$ e $[K : F] = n$, allora $[L : F] = mn$. □

Corollario 2.2. *Siano $F \subset L$ campi finiti, $[L : F] = n$. Allora se $|F| = q$, si avrà $|L| = q^n$.*

Dimostrazione. L è isomorfo, come spazio vettoriale, a F^n, e il numero di n.uple a coefficienti in F è pari a q^n. □

Se F è un campo, può essere sempre considerato come estensione del sottocampo generato da 1. Questo sottocampo conterrà tutti gli elementi ottenuti sommando 1 a se stesso più volte, nonché tutti i loro inversi, ed è detto *campo primo* di F.

Proposizione 2.3. *Il sottocampo di F generato da 1 è isomorfo a $\mathbb{Q}$ se la caratteristica di F è 0, e ad $\mathbb{F}_p$ se la caratteristica di F è uguale a p.*

Dimostrazione. Se la caratteristica di F è 0, allora gli elementi ottenuti sommando 1 a se stesso più volte, ed i loro inversi additivi, sono tutti distinti, e formano perciò un sottoanello isomorfo a $\mathbb{Z}$. Ma allora il sottocampo generato da 1 contiene tutti i rapporti tra tali elementi, ed è quindi isomorfo a $\mathbb{Q}$.

Se la caratteristica di F è p, gli elementi ottenuti sommando 1 a se stesso sono esattamente p, e le operazioni di somma e prodotto tra di essi sono come nell'anello $\mathbb{Z}/(p)$. Ma tale anello è un campo, e quindi il sottocampo generato da 1 è isomorfo a $\mathbb{F}_p$. □

Corollario 2.4. *Ogni campo di caratteristica* 0 *è infinito. Il numero di elementi in un campo finito è* p^n*, dove* p *è la caratteristica del campo.*

2.1. **Estensioni finite ed elementi algebrici.** Sia ora $F \subset L$ un'estensione finita, cioè una in cui $[L : F] = n < \infty$. Se α è un elemento di L, allora le potenze $1, \alpha, \alpha^2, ..., \alpha^n$ saranno necessariamente linearmente dipendenti su F. Questo vuol dire che, per un'opportuna scelta di $c_i \in F$, avremo

$$c_n\alpha^n + c_{n-1}\alpha^{n-1} + ... + c_2\alpha^2 + c_1\alpha + c_0 = 0,$$

o in altre parole che α soddisfa un polinomio $c(x) = c_n x^n + ...c_1 x + c_0$ a coefficienti in F. Un tale elemento si dice *algebrico su* F. Abbiamo quindi mostrato

Lemma 2.5. *Ogni elemento di un'estensione finita di* F *è algebrico su* F*.*

E' vero anche il viceversa.

Lemma 2.6. *Sia* $F \subset L$ *un'estensione di campi. Se* $\alpha \in L$ *è algebrico su* F*, allora* α *appartiene ad una sottoestensione finita di* F*.*

Dimostrazione. Sia $x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ un polinomio a coefficienti in F che annulli α. Allora

$$\alpha^n = -(a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0). \tag{1}$$

Dimostriamo per induzione che ogni potenza di α si esprime come combinazione lineare degli elementi $1, \alpha, \alpha^2, ..., \alpha^{n-1}$. In effetti $\alpha^{N+1} = \alpha(\alpha^N)$. Per ipotesi induttiva sappiamo che $\alpha^N = c_0 1 + c_1\alpha + ... + c_{n-1}\alpha^{n-1}$ per un'opportuna scelta di elementi $c_i \in F$. Ma allora $\alpha^{N+1} = c_0\alpha + c_1\alpha^2 + ... + c_{n-2}\alpha^{n-1} + c_{n-1}\alpha^n$ e possiamo sostituire in α^n l'espressione (1).

Essendo $1, \alpha, ..., \alpha^{n-1}$, generatori lineari di L su F, la dimensione di L come F-spazio vettoriale è limitata da n. □

Prima di procedere, un po' di notazioni. Sia $F \subset L$ un'estensione di campi, e prendiamo $\alpha \in L$. L'intersezione di tutti i sottoanelli di L che contengono sia F che α si indica con $F[\alpha]$, mentre l'intersezione di tutti i sottocampi di L con la stessa proprietà è indicato con $F(\alpha)$.

Lemma 2.7. *Gli elementi contenuti* $F[\alpha]$ *sono tutte e sole le combinazioni* F*-lineari di potenze di* α*.*

Dimostrazione. Sia R un sottoanello di L che contenga α. Allora contiene $\alpha^2 = \alpha \cdot \alpha$, ed ogni altra potenza di α. Se R contiene anche F, dovrà allora contenere anche i prodotti di elementi di F con potenze di α, nonché tutte le loro somme. In conclusione, un sottoanello R di L che contenga sia F che α deve contenere tutte le combinazioni lineari a coefficienti in F di potenze di α. Questo mostra che l'intersezione $F[\alpha]$ di tutti i sottoanelli di L che contengono F e α contiene tutte le espressioni polinomiali in α a coefficienti in α.

Per mostrare che questi sono i soli elementi di $F[\alpha]$, basta mostrare che formano un sottoanello di F. Ma moltiplicando due polinomi in α a coefficienti in F si ottiene ancora un polinomio in α a coefficienti in F. La dimostrazione è allora conclusa. □

Lemma 2.8. *Gli elementi di* $F(\alpha)$ *sono del tipo* $p(\alpha)/q(\alpha)$*, con* $p(x), q(x) \in F[x]$*, e* $q(\alpha) \neq 0$*.*

Dimostrazione. Come nel lemma precedente, si mostra che un sottocampo di L che contenga F e α deve contenere anche il sottoanello $F[\alpha]$. Essendo tuttavia un campo dovrà contenere anche i rapporti tra gli elementi di $F[\alpha]$.

E' semplice mostrare, a questo punto, che i rapporti di espressioni polinomiali in α a coefficienti in F formano un sottocampo di L. □

Chiaramente $F[\alpha]$ è contenuto in $F(\alpha)$. Vi sono tuttavia casi in cui i due concetti coincidono.

Un elemento α è algebrico su F quando annulla almeno un polinomio $0 \neq p(x) \in F[x]$. E' chiaro che l'insieme dei polinomi $p(x) \in F[x]$ tali che $p(\alpha) = 0$ è un ideale di $F[x]$. Sappiamo che gli ideali di $F[x]$ sono principali, ed esiste quindi un generatore di tale ideale, ovvero un polinomio di grado minimo di cui α sia soluzione. Questo polinomio è detto *polinomio minimo* di α, e può essere scelto monico, a meno di moltiplicarlo per un elemento di F.

Lemma 2.9. *Sia* $F \subset L$ *un'estensione di campi,* $\alpha \in L$ *un elemento algebrico su* F*. Allora il polinomio minimo* $p(x)$ *di* α *su* F *è irriducibile su* F *e* $F(\alpha)$ *è isomorfo al quoziente* $F[x]/(p(x))$*.*

Dimostrazione. Se $p(x) = a(x)b(x)$, allora $a(\alpha)b(\alpha) = p(\alpha) = 0$. Ma allora $a(\alpha) = 0$ oppure $b(\alpha) = 0$. In ogni caso, esistono polinomi che annullano α di grado minore di quello di $p(x)$, e quindi $p(x)$ non è il polinomio minimo.

Costruiamo ora l'applicazione $\phi : F[x] \to L$ tale che $\phi(p(x)) = p(\alpha)$. ϕ è chiaramente un omomorfismo, e la sua immagine coincide con $F[\alpha]$. Il nucleo di ϕ è l'ideale $(p(x))$ generato dal polinomio minimo di α. Sappiamo che $p(x)$ è irriducibile, quindi $(p(x))$ è un ideale massimale, ed il quoziente $F[x]/(p(x))$ è un campo. Per il teorema di omomorfismo, l'immagine $F[\alpha]$ di ϕ è isomorfa al campo $F[x]/(p(x))$ ed è quindi essa stessa un campo. Concludiamo che $F[\alpha] = F(\alpha)$ e che questo sottocampo di L è isomorfo a $F[x]/(p(x))$. □

Teorema 2.10. *Sia $F \subset L$ un'estensione di campi, α un elemento di L. Le seguenti affermazioni sono equivalenti.*

(1) *α è algebrico su F.*
(2) *$F[\alpha] = F(\alpha)$.*
(3) *$F[\alpha]$ è un campo.*
(4) *$F(\alpha)$ è un'estensione finita di F.*

Dimostrazione. (1) ⇒(2). Abbiamo già visto che se α è algebrico, allora $F[\alpha] = F(\alpha)$.

(2) ⇒(3). Se $F[\alpha] = F(\alpha)$ allora chiaramente $F[\alpha]$ è un campo.

(3) ⇒(1). Se $F[\alpha]$ è un campo, l'omomorfismo $\phi : F[x] \to F[\alpha]$ definito sopra non può essere iniettivo. Se così fosse, $F[\alpha]$ sarebbe isomorfo a $F[x]$, che non è un campo. Allora α è algebrico su F.

(1) ⇒(4). Se α è algebrico, allora $F(\alpha)$ è isomorfo a $F[x]/(p(x))$ dove $p(x)$ è il polinomio minimo di α. Se $p(x)$ ha grado n, ogni classe di equivalenza in $F[x]/(p(x))$ contiene uno e un solo polinomio di grado minore di n. Perciò $[1], [x], ..., [x^{n-1}]$ costituiscono una base di $F[x]/(p(x))$. Quindi $F(\alpha)$ è un F-spazio vettoriale di dimensione n.

(4) ⇒(1). Abbiamo già mostrato che gli elementi contenuti in un'estensione finita di F sono algebrici. □

Esempi.

- Il campo $\mathbb{Q}(\sqrt{2})$ è un'estensione di $\mathbb{Q}$. L'elemento $\sqrt{2}$ soddisfa il polinomio $x^2 - 2$, ma non soddisfa nessun polinomio di grado 1 a coefficienti in $\mathbb{Q}$, in quanto $\sqrt{2}$ non è razionale. Quindi $x^2 - 2$ è il suo polinomio minimo.

  Avremmo potuto mostrare questo fatto direttamente verificando che $x^2 - 2$ è irriducibili, il che segue dal criterio di Eisenstein. Il grado $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$ è uguale al grado del polinomio minimo dell'algebrico che aggiungiamo, ed è quindi 2.
- π non è un numero algebrico – ma è un risultato troppo complesso per mostrarlo qui. In ogni caso, $\mathbb{Q}(\pi)$ non può essere un'estensione finita di $\mathbb{Q}$, perché in quel caso ogni suo elemento sarebbe algebrico. In altre parole $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$.

Esercizi.

(a) Calcolare il grado dell'estensione $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2} + \sqrt{5})$.
(b) Calcolare il grado dell'estensione $\mathbb{R} \subset \mathbb{C}$.
(c) Qual è il polinomio minimo di $\sqrt{3} + i$? E di $\sqrt{3 + i}$?

2.2. **Campi di spezzamento.** Il quoziente $F[x]/(p(x))$ fornisce anche una costruzione utile per creare artificialmente un'estensione di F contenente radici di $p(x)$.

Proposizione 2.11. *Sia F un campo, $p(x) \in F[x]$ un polinomio irriducibile. Allora $L = F[x]/(p(x))$ è una estensione di F in cui $p(x)$ ammette almeno una radice.*

Dimostrazione. Indichiamo con $\alpha \in L$ la classe di congruenza del polinomio x. In altre parole $\alpha = [x]$. Allora $\alpha^2 = [x][x] = [x^2]$. Alla stessa maniera otteniamo che $\alpha^n = [x^n]$. Segue abbastanza facilmente che $f(\alpha) = f([x]) = [f(x)]$, qualunque sia il polinomio $f(x)$. Ma allora $p(\alpha) = [p(x)] = [0]$. Questo mostra che l'elemento $\alpha \in L$ è radice di $p(x)$. □

Corollario 2.12. *Sia F un campo, $0 \neq f(x) \in F[x]$. Allora esiste una estensione finita L di F in cui $f(x)$ si fattorizza nel prodotto di polinomi lineari.*

Dimostrazione. Possiamo esprimere $f(x)$ come prodotto di polinomi irriducibili in $F[x]$. Se tali polinomi sono tutti di primo grado, allora $f(x)$ si fattorizza in F come prodotto di polinomi lineari.

Supponiamo che così non sia, e scegliamo un fattore irriducibile non lineare $q(x)$ nella fattorizzazione di $f(x)$. Allora $F' = F[x]/(q(x))$ è un campo in cui $q(x)$ ammette una radice, e quindi la fattorizzazione di $f(x)$ in $F'[x]$ è un raffinamento di quella in $F[x]$. Reiterando questo procedimento, otteniamo dopo un numero finito di passi un'estensione L in cui $f(x)$ si spezza completamente. □

Un'estensione finita L di F si dice campo di spezzamento di $f(x) \in F[x]$ se $f(x)$ si spezza in fattori lineari su L, ma su nessun suo sottocampo proprio. E' chiaro che se $f(x)$ si spezza su L come $f(x) = (x - \alpha_1)...(x - \alpha_n)$, allora $F(\alpha_1, ..., \alpha_n) \subset L$ è un campo di spezzamento di $f(x)$.

Corollario 2.13. *Ogni polinomio $0 \neq f(x) \in F[x]$ ammette un campo di spezzamento.*

Se $\phi : F \to \overline{F}$ è un omomorfismo, possiamo definire un'applicazione $F[x] \to \overline{F}$ semplicemente calcolando ϕ sui coefficienti dei polinomi. In questa modo si ottiene un omomorfismo di anelli, che indicheremo ancora con ϕ per non appesantire la notazione. Essenziale per i nostri interessi è il seguente fatto:

Proposizione 2.14. *Siano $F, \overline{F}$ campi, e $\phi : F \to \overline{F}$ un isomorfismo. Se $f(x) \in F[x]$ e $\overline{f}(x) \in \overline{F}[x]$ sono tali che $\phi(f(x)) = \overline{f}(x)$, e $L, \overline{L}$ sono campi di spezzamento di $f(x)$ e $\overline{f}(x)$ rispettivamente, allora esiste un isomorfismo $\Phi : L \to \overline{L}$ tale che $\Phi|F \equiv \phi$.*

Dimostrazione. Per induzione su $[L : F]$. Se $[L : F] = 1$, allora $L = F$, e quindi $f(x)$ si spezza completamente in F. Applicando ϕ alla fattorizzazione di $f(x)$ in fattori lineari, otteniamo una simile fattorizzazione per $\overline{f}(x)$. Questo mostra che $\overline{L} = \overline{F}$. Ma allora l'estensione cercata è ϕ stessa.

Sia ora $[L : F] = n > 1$, e supponiamo che l'enunciato sia vero per tutte le estensioni di grado inferiore. Scegliamo una radice α di un fattore irriducibile non lineare $q(x)$ di $f(x)$ e una radice β del fattore irriducibile $\overline{q}(x) = \phi(q(x))$ di $\overline{f}(x)$. Abbiamo gli isomorfismi $F(\alpha) \simeq F[x]/(q(x))$ e $\overline{F}(\beta) \simeq \overline{F}[x]/(\overline{q}(x))$.

Consideriamo ora la composizione

$$F[x] \xrightarrow{\phi} \overline{F}[x] \xrightarrow{\pi} \overline{F}[x]/(\overline{q}(x)),$$

dove π è la proiezione al quoziente. Il nucleo di questa composizione è l'ideale $(q(x))$, mentre la composizione è suriettiva, e per il teorema di omomorfismo abbiamo un isomorfismo $F[x]/(q(x)) \simeq \overline{F}[x]/(\overline{q}(x))$.

Allora la composizione di isomorfismi

$$F(\alpha) \simeq F[x]/(q(x)) \simeq \overline{F}[x]/(\overline{q}(x)) \simeq \overline{F}(\beta)$$

estende l'isomorfismo $\phi : F \to \overline{F}$. Dal momento che $[L : F(\alpha)] < [L : F]$, per ipotesi induttiva questo isomorfismo si estende ad un isomorfismo di L con $\overline{L}$. □

Corollario 2.15. *Due campi di spezzamento $L, \overline{L}$ di uno stesso polinomio sono isomorfi.*

Dimostrazione. Applichiamo la proposizione precedente a $\mathrm{id} : F \to F$. □

3. CAMPI FINITI

Diamo ora un'applicazione dei risultati appena dimostrati a proposito dei campi di spezzamento. Prima di procedere, dimostro due risultati tecnici che mi serviranno in seguito.

3.1. **Massimo comun divisore di polinomi e radici multiple.**

Lemma 3.1. *Sia $F \subset L$ campi, $p(x), q(x) \in F[x]$. Allora il massimo comun divisore di $p(x)$ e $q(x)$ in $F[x]$ è uguale a quello in $L[x]$.*

Dimostrazione. Il massimo comun divisore $d(x)$ tra $p(x)$ e $q(x)$ in $F[x]$ può essere espresso come $d(x) = a(x)p(x) + b(x)q(x)$, per opportuni polinomi $a(x), b(x) \in F[x]$.

Consideriamo ora gli ideali di $L[x]$: $I = (d(x))$, $J = (a(x), b(x))$. Sappiamo che $d(x)$ divide sia $a(x)$ che $b(x)$ in $F[x]$, quindi la stessa cosa è vera in $L[x]$. Allora $a(x), b(x) \in I \Rightarrow J \subset I$. Ma $d(x) = a(x)p(x) + b(x)q(x)$, quindi $d(x) \in J \Rightarrow I \subset J$. Perciò $I = J$.

Possiamo concludere che gli ideali $(d(x))$ e $(a(x), b(x))$ dell'anello $L[x]$ coincidono, e quindi che il massimo comun divisore in $L[x]$ tra $a(x)$ e $b(x)$ è ancora $d(x)$. □

Il prossimo lemma parla di radici multiple. α è una radice multipla di $p(x)$ se $(x - \alpha)^2$ divide $p(x)$. La derivata di un polinomio $p(x) = p_n x^n + ... + p_1 x + p_0$ è come sempre $np_n x^{n-1} + ... + 2p_2 x + p_1$.

Lemma 3.2. *Sia F un campo, $p(x) \in F[x]$. Se $(p(x), p'(x)) = 1$, allora $p(x)$ non ha radici multiple in F.*

Dimostrazione. Se $\alpha \in F$ è una radice multipla di $p(x)$, allora $p(x) = (x-\alpha)^2 h(x)$. Ma allora $p'(x) = 2(x-\alpha)h(x) + (x-\alpha)^2 h'(x) = (x-\alpha)(2h(x) + (x-\alpha)h'(x))$. Questo mostra che $x-\alpha$ divide sia $p(x)$ che la sua derivata $p'(x)$. Di conseguenza questi due polinomi non possono essere primi tra loro. □

Corollario 3.3. *Sia F un campo, $p(x) \in F[x]$, e supponiamo che $p(x)$ si spezzi in F nel prodotto di fattori lineari. Le radici di $p(x)$ sono semplici (cioè non multiple) se e solo se $(p(x), p'(x)) = 1$.*

Dimostrazione. Sappiamo già che se $p(x)$ è primo con la sua derivata, le radici di $p(x)$ sono semplici. Supponiamo ora che $p(x)$ non sia primo con la sua derivata. Se $x-\alpha$ divide sia $p(x)$ che $p'(x)$, scriviamo $p(x) = (x-\alpha)h(x)$. Allora $p'(x) = (x-\alpha)h'(x) + h(x)$. Poiché $x-\alpha$ divide sia $p'(x)$ che $(x-\alpha)h'(x)$, deve dividere anche la loro differenza $h(x)$, e quindi $p(x) = (x-\alpha)h(x)$ è divisibile per $(x-\alpha)^2$. □

Corollario 3.4. *Sia $q(x)$ un polinomio irriducibile a coefficienti nel campo F di caratteristica nulla. Allora $(q(x), q'(x)) = 1$.*

Dimostrazione. Supponiamo che la caratteristica di F sia 0. Allora $q'(x)$ è un polinomio non nullo. Il massimo comun divisore $(q(x), q'(x))$ divide $q'(x)$, che ha grado inferiore a quello di $q(x)$. Essendo un divisore del polinomio irriducibile $q(x)$ dovrà essere uguale a 1. □

Osservazione. Un controesempio nel caso di caratteristica finita è istruttivo. Sia $F = \mathbb{F}_p(t)$ il campo delle frazioni dell'anello $\mathbb{F}_p[t]$. Il polinomio $q(x) = x^p - t \in F[x]$ ha derivata 0, e quindi $(q(x), q'(x)) = q(x)$. Nel campo $L = \mathbb{F}_p(t^{1/p})$, il polinomio $q(x)$ si spezza in fattori lineari, però $q(x) = (x - t^{1/p})^p$ e quindi l'unica radice $t^{1/p}$ è multipla.

Questo non succede nel caso in cui F sia un campo finito : se $q(x) \in F[x]$ ha derivata nulla, allora $q(x) = a_n x^{np} + a_{n-1}x^{(n-1)p} + \ldots + a_1 x^p + a_0$ in quanto gli unici monomi di derivata nulla hanno grado multiplo di p. Vedremo in seguito che in un campo finito ogni elemento è una potenza p-esima. Ma allora se $a_i = (b_i)^p$ si ha $q(x) = (b_n x^n + \ldots + b_1 x + b_0)^p$ e quindi $q(x)$ non può essere irriducibile. I campi in cui i polinomi irriducibili non hanno radici multiple si dicono *perfetti*. Un'estensione algebrica $F(\alpha)$ per cui il polinomio minimo di α non ammette radici multiple è detta *separabile*. Evidentemente le estensioni algebriche di campi perfetti sono tutte separabili! Gli unici campi di caratteristica non nulla che considereremo sono quelli finiti, e quindi tutte le nostre estensioni algebriche saranno separabili.

3.2. **Classificazione dei campi finiti.** Sia L un campo finito. Allora la caratteristica di L è un numero primo p, e l'ordine di L è p^n dove $n = [L : \mathbb{F}_p]$. Mostreremo che per ogni scelta di p e di $n \geq 1$ esiste un solo campo di ordine p^n a meno di isomorfismo. Per fare ciò mostreremo che ogni campo di un fissato ordine è campo di spezzamento dello stesso polinomio.

Lemma 3.5. *Sia L un campo con p^n elementi. Allora $x^{p^n} = x$ per ogni $x \in L$.*

Dimostrazione. Il gruppo moltiplicativo L^* possiede $p^n - 1$ elementi. Pertanto $x^{p^n - 1} = 1$ per ogni $x \in L^*$, da cui $x^{p^n} = x$. Ma questa equazione è soddisfatta anche per $x = 0$, ed è quindi valida per ogni elemento di L. □

Lemma 3.6. *Sia L un campo con p^n elementi. Allora L è campo di spezzamento del polinomio $x^{p^n} - x \in \mathbb{F}_p[x]$.*

Dimostrazione. Il polinomio $x^{p^n} - x$ possiede p^n radici in L, e quindi necessariamente si spezza nel prodotto di fattori lineari. Questo non accade in nessun sottocampo di L, in quanto i sottocampi di L hanno meno di p^n elementi, e non possono quindi contenere tutte le radici di $x^{p^n} - x$. □

Corollario 3.7. *Due campi finiti con lo stesso numero di elementi sono isomorfi.*

Dimostrazione. Sono entrambi campi di spezzamento del polinomio $x^{p^n} - x \in \mathbb{F}_p[x]$. Ma campi di spezzamento dello stesso polinomio sono isomorfi. □

L'unico tassello mancante alla completa descrizione dei campi finiti è un risultato che ci garantisca l'esistenza di almeno un campo di ordine p^n. Prima di fare questo, abbiamo bisogno di fare conoscenza con l'automorfismo di Frobenius.

Lemma 3.8. *Sia L un campo finito di caratteristica p, $F : L \to L$ l'applicazione definita da $F(x) = x^p$. Allora F è un automorfismo di L.*

Dimostrazione. Se a, b sono elementi di un dominio di caratteristica p, allora $(a+b)^p = a^p + b^p$. Infatti tutti i coefficienti binomiali $\binom{p}{i}, i \neq 0, p$ sono divisibili per p, e quindi tutti i termini intermedi si annullano. Allora abbiamo $F(x+y) = (x+y)^p = x^p + y^p = F(x) + F(y)$ e chiaramente $F(xy) = (xy)^p = x^p y^p = F(x)F(y)$. Iniettività e suriettività sono facili. Notate che, per la suriettività di F, ogni elemento di L è una p-esima potenza, come promesso nell'osservazione della pagina precedente. □

Corollario 3.9. *Ogni potenza di F è un automorfismo di L. $F^i = \mathrm{id}$ solo se i è un multiplo di $n = [L : \mathbb{F}_p]$.*

Dimostrazione. La composizione di automorfismi è un automorfismo, quindi F^i è un automorfismo. Supponiamo che $F^i = \mathrm{id}$ con $i < n$. Allora ogni elemento di L soddisfa $x^{p^i} - x = 0$, ma questo è impossibile, in quanto L possiede $p^n > p^i$ elementi, mentre un polinomio di grado p^i a coefficienti in un campo può avere al più p^i radici. Questo mostra che F ha ordine n nel gruppo degli automorfismi di L. □

Lemma 3.10. *Sia L il campo di spezzamento di $q(x) = x^{p^n} - x \in \mathbb{F}_p[x]$. Allora L possiede esattamente p^n elementi.*

Dimostrazione. Consideriamo in L il sottoinsieme $F = \{\alpha \in L | \alpha \text{ è radice di } q(x)\}$. Gli elementi di F sono quelli fissati dall'automorfismo F^n, ed è facile mostrare che formano un sottocampo di L. Inoltre la derivata di $q(x)$ è $p^n x^{p^n - 1} - 1 = -1$, quindi $(q(x), q'(x)) = 1$. Ma allora le radici di $q(x)$ in L sono tutte semplici, e $q(x)$ ammette p^n radici. Questo mostra che F è un campo con p^n elementi, e quindi che $q(x)$ si spezza su F, da cui $L = F$. □

3.3. **Automorfismi di un campo finito.**

Lemma 3.11. *Sia L un campo finito di caratteristica p. Allora $x^p = x$ se e solo se $x \in \mathbb{F}_p$.*

Dimostrazione. Abbiamo già visto, all'inizio del corso, che $a^p \equiv a \mod p$, quindi $x^p = x$ per ogni $x \in \mathbb{F}_p$. Tuttavia $x^p = x$ ha al più p soluzioni in L, e quindi non ci sono altre soluzioni. □

Lemma 3.12. *Sia $p(x) \in \mathbb{F}_p[x]$ un polinomio irriducibile di grado d, e sia L un'estensione di F_p in cui $p(x)$ possieda una radice α. Allora $p(x)$ si spezza in L, e le sue radici sono $\alpha, \alpha^p, ..., \alpha^{p^{d-1}}$.*

Dimostrazione. Sappiamo che $0 = p(\alpha) = a_d \alpha^d + ... + a_1 \alpha + a_0$. Applicando ad entrambi i membri l'automorfismo di Frobenius, otteniamo $a_d F(\alpha)^d + ... + a_1 F(\alpha) + a_0 = 0$, quindi anche $F(\alpha)$ è una radice di $p(x)$. Ripetendo il procedimento, si mostra che $F^i(\alpha)$ è soluzione di $p(x) = 0$ per ogni i. Chiaramente $F^d = \mathrm{id}$ nel campo $\mathbb{F}_p(\alpha)$, in quanto $\mathbb{F}_p(\alpha)$ possiede p^d elementi.

Consideriamo ora il polinomio di grado d

$$q(x) = (x - \alpha)(x - F(\alpha))...(x - F^{d-1}(\alpha)). \tag{2}$$

Per calcolare il polinomio $F(q(x))$ i cui coefficienti si ottengono da quelli di $q(x)$ applicando F, possiamo calcolare direttamente F sulla fattorizzazione (2) e poi moltiplicare. Ma si vede che l'applicazione di F a tale prodotto permuta semplicemente i fattori, quindi $F(q(x)) = q(x)$. Abbiamo trovato un polinomio i cui coefficienti non cambiano dopo l'applicazione di F. Per il lemma precedente, i coefficienti appartengono a $\mathbb{F}_p$. I polinomi $p(x)$ e $q(x)$ hanno lo stesso grado, ed hanno entrambi α come radice. Dal momento che $p(x)$ è il polinomio minimo di α, concludiamo che $p(x) = q(x)$. Abbiamo osservato in precedenza che un polinomio irriducibile a coefficienti in un campo finito non può avere radici multiple in un'estensione. Ne deduciamo in particolare che gli elementi $\alpha, F(\alpha), ..., F^{d-1}(\alpha)$ sono tutti distinti. □

Mostriamo ora, nel caso dei campi finiti, un risultato importante che dimostreremo in seguito per campi di caratteristica zero.

Teorema 3.13. *Sia L un campo finito di caratteristica p. E' sempre possibile trovare $\gamma \in L$ in modo che $L = \mathbb{F}_p(\gamma)$.*

Dimostrazione. L^* è un gruppo ciclico. Se γ ne è un generatore, ogni elemento di L^* è potenza di γ, e quindi appartiene a $\mathbb{F}_p(\gamma)$. Ma allora $\mathbb{F}_p(\gamma)$ contiene tutti gli elementi di L, in quanto ogni campo contiene 0. □

Teorema 3.14. *Gli unici automorfismi di un campo finito L sono le potenze dell'automorfismo di Frobenius.*

Dimostrazione. Scegliamo $\gamma \in L$ in modo che $L = \mathbb{F}_p(\gamma)$. Se $[L : \mathbb{F}_p] = n$, il polinomio minimo di γ deve avere grado n, e quindi $1, \gamma, ..., \gamma^{n-1}$ formano una $\mathbb{F}_p$-base di L.

Sia ϕ un automorfismo di L. $\phi(\gamma)$ deve essere una radice del polinomio minimo di γ. Dal momento che ogni polinomio minimo è irriducibile, per quanto detto precedentemente avremo $\phi(\gamma) = F^i(\gamma)$ per qualche i. Ma allora $\phi(\gamma^m) = \phi(\gamma)^m = F(\gamma)^m = F(\gamma^m)$. Ogni elemento si scrive come combinazione lineare delle potenze di γ a coefficienti in $\mathbb{F}_p$. Ma allora $\phi(c_0 + c_1\gamma + ... + c_{n-1}\gamma^{n-1}) = c_0 + c_1\phi(\gamma) + ...+c_{n-1}\phi(\gamma^{n-1}) = c_0+c_1F^i(\gamma)+...+c_{n-1}F^i(\gamma^{n-1}) = F^i(c_0+...c_{n-1}\gamma^{n-1})$. Quindi $\phi \equiv F^i$. □

4. La corrispondenza di Galois

4.1. **Il teorema dell'elemento primitivo.** Abbiamo visto, alla fine del paragrafo precedente, che ogni campo finito si può ottenere come estensione algebrica $\mathbb{F}_p(\gamma)$ di un singolo elemento. Questo risultato è in qualche maniera inaspettato. Sapevamo già della possibilità di costruire un'estensione aggiungendo elementi algebrici, ma non vi è alcun motivo apparente per cui un'estensione ottenuta aggiungendo più di un elemento debba poter essere ottenuta aggiungendone uno singolo. Tuttavia questo risultato vale anche per campi infiniti di caratteristica 0. Le dimostrazioni di quest'ultima parte del corso sono un riordinamento di quelle del libro di Artin (e siccome Artin è un didatta migliore di me, le sue dimostrazioni sono scritte meglio...).

Teorema 4.1. *Sia F un campo di caratteristica 0, L una sua estensione finita. Allora L contiene un elemento γ tale che $L = F(\gamma)$.*

Dimostrazione. Senza perdita di generalità, possiamo supporre che $L = F(\alpha, \beta)$. Siano allora $f(x), g(x) \in F[x]$ i polinomi minimi di α e β su F. Voglio mostrare che per un'opportuna scelta di $c \in F$ l'elemento $\gamma = \beta + c\alpha$ genera tutto L.

Sia $K = F(\gamma)$. L'elemento α è soluzione sia di $f(x)$ che di $h(x) = g(\gamma - cx) \in K[x]$: infatti $h(\alpha) = g(\gamma - c\alpha) = g(\beta) = 0$. Voglio ora calcolare il massimo comun divisore in $K[x]$ tra $f(x)$ e $g(\gamma - cx)$. Per un risultato precedente, è sufficiente calcolarlo in $M[x]$, dove M è un'estensione di K: il risultato sarà lo stesso.

Scegliamo allora come M il campo di spezzamento del polinomio $f(x)g(x)$. M contiene quindi tutte le radici di $f(x)$ e di $g(x)$. Allora in $M[x]$, abbiamo le fattorizzazioni

$$f(x) = (x - \alpha)(x - \alpha_1)(x - \alpha_2)...(x - \alpha_m), \qquad g(x) = (x - \beta)(x - \beta_1)(x - \beta_2)...(x - \beta_n).$$

Per calcolare il MCD tra $f(x)$ e $h(x)$ mi basta vedere quali dei fattori di $f(x)$ dividano $h(x)$. Ora, $(x - \alpha_i)$ divide $h(x)$ se e solo se $h(\alpha_i) = 0$. Ma $h(\alpha_i) = g(\gamma - c\alpha_i)$. Sappiamo già che $\gamma = \beta - c\alpha$, quindi $h(\alpha_i) = 0$ solo quando $\gamma - c\alpha_i$ è uno dei β_j.

Ma allora $\gamma - c\alpha_i = \beta_j \Rightarrow \beta + c(\alpha - \alpha_i) = \beta_j$ e questo capita solo se $c = (\beta_j - \beta)/(\alpha - \alpha_i)$. Se c evita questi valori, al variare di i, j, allora l'unico fattore a dividere $h(x)$ sarà $(x - \alpha)$.

Scegliamo quindi c distinto da tali valori. Il MCD di $f(x)$ e $h(x)$ è $x - \alpha$. Ma $f(x), h(x) \in K[x]$, e quindi il loro MCD giace anch'esso in $K[x]$. Pertanto tutti i coefficienti di $x - \alpha$ appartengono a K. Questo mostra che $\alpha \in K$. Ma poiché $\gamma = \beta + c\alpha \in K$ allora anche $\beta \in K$. Questo dimostra che $F(\alpha, \beta) \subset K$, e quindi che $L = K$. □

4.2. **Estensioni di Galois.** In questa sezione ci occuperemo di descrivere la corrispondenza di Galois tramite alcuni esempi. Questa corrispondenza mette in relazione le sottoestensioni di una estensione di campi con i sottogruppi del gruppo di Galois dell'estensione. Prima di passare agli esempi, ci servono alcune definizioni.

Definizioni.

- Il *gruppo di Galois* dell'estensione $F \subset L$ è l'insieme degli automorfismi del campo L che fissano il sottocampo F elemento per elemento, ovvero gli elementi di

  $$\mathrm{Gal}(L/F) = \{\phi : L \to L | \phi \text{ è un isomorfismo, } \phi(f) = f \text{ per ogni } f \in F\}.$$

  E' immediato verificare che $\mathrm{Gal}(L/F)$ è chiuso rispetto alla composizione di automorfismi, e contiene almeno l'automorfismo identico. Inoltre l'inverso di un automorfismo di L che fissa F è ancora un elemento di $\mathrm{Gal}(L/F)$. Quindi $\mathrm{Gal}(L/F)$ è un gruppo rispetto alla composizione – da cui il nome di gruppo di Galois.
- Sia G un gruppo di automorfismi del campo L. Allora il sottoinsieme di L

  $$L^G = \{\alpha \in L | g(\alpha) = \alpha \text{ per ogni } g \in G\}$$

  è un sottocampo di L (mostratelo!) detto *campo fisso* di L rispetto a G, o più semplicemente il campo fisso di G.

Esempi.

- $F = \mathbb{Q}, L = \mathbb{Q}(\sqrt{2})$. Il campo L si ottiene da F estendendolo con l'algebrico $\sqrt{2}$. Sappiamo quindi che $L = \mathbb{Q}(\sqrt{2})$ è un'estensione finita di $\mathbb{Q}$. Per calcolarne il grado, determiniamo il polinomio minimo di $\sqrt{2}$. Si vede facilmente che $\sqrt{2}$ verifica il polinomio $x^2 - 2 \in \mathbb{Q}[x]$. Sappiamo – è un risultato classico che si vede anche prima dell'università – che $\sqrt{2}$ non è un numero razionale. Questo vuol dire che non può esservi alcun polinomio di grado 1 a coefficienti in $\mathbb{Q}$ di cui $\sqrt{2}$ sia radice. Allora $x^2 - 2$ è il polinomio di grado minimo di cui $\sqrt{2}$ sia radice: in altre parole ne è il polinomio minimo.

  La teoria ci dice che se $q(x) \in F[x]$ è il polinomio minimo di α su F, allora $q(x)$ è irriducibie, $F(\alpha)$ è isomorfo al quoziente $F[x]/(q(x))$ e il grado $[F(\alpha) : F]$ dell'estensione è pari al grado di $q(x)$. Nel nostro caso, $q(x) = x^2 - 2$ ha grado 2, e quindi $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

  E' possibile trovare estensioni intermedie di $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$, cioè campi K tali che $\mathbb{Q} \subset K \subset \mathbb{Q}(\sqrt{2})$? Come osservazione preliminare ricordiamo che se $F \subset K \subset L$, allora $[L : F] = [L : K][K : F]$. Le uniche maniere di fattorizzare 2 sono $2 \cdot 1$ e $1 \cdot 2$, quindi abbiamo due casi: se $[K : F] = 1$, allora $K = F$; se invece $[L : K] = 1$, allora $L = K$. In conclusione, non è possibile trovare un campo strettamente compreso tra $\mathbb{Q}$ e $\mathbb{Q}(\sqrt{2})$.

  Passiamo ora alla determinazione del gruppo di Galois. $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ è l'insieme di tutti gli automorfismi di $\mathbb{Q}(\sqrt{2})$ che si restringono all'identità su $\mathbb{Q}$. La teoria ci dice che le potenze di $\sqrt{2}$ fino alla $n-1$.esima, dove n è il grado del polinomio minimo, sono una base di $\mathbb{Q}(\sqrt{2})$ visto come spazio vettoriale su $\mathbb{Q}$. In altre parole, ogni elemento di $\mathbb{Q}(\sqrt{2})$ si scrive in modo unico nella forma $a + b\sqrt{2}$, dove $a, b \in \mathbb{Q}$. Un automorfismo ϕ che lascia gli elementi di $\mathbb{Q}$ invariati è completamente determinato dal valore di $\phi(\sqrt{2})$.

  Facciamo nuovamente ricorso alla teoria: se $\alpha \in L$ è un algebrico su F il cui polinomio minimo su F è $q(x)$, per ogni radice $\beta \in L$ di $q(x)$ possiamo costruire un automorfismo ϕ di L tale che $\phi(\alpha) = \beta$.

  Nel nostro caso particolare, dobbiamo soltanto determinare tutte le soluzioni in $\mathbb{Q}(\sqrt{2})$ dell'equazione $x^2 + 2 = 0$. E' facile vedere che le due soluzioni $\pm\sqrt{2}$ sono entrambe elementi del nostro campo L, e quindi abbiamo due automorfismi: il primo manda $\sqrt{2}$ in se stesso, ed è quindi l'identità. Il secondo manda $\sqrt{2}$ in $-\sqrt{2}$, e quindi $\phi(a+b\sqrt{2}) = a-b\sqrt{2}$ per ogni scelta di $a, b \in \mathbb{Q}$. Il gruppo di Galois contiene due automorfismi, ed è perciò isomorfo al gruppo C_2.
- $F = \mathbb{Q}, L = \mathbb{Q}(\sqrt[3]{2})$. Come sopra, il campo L è isomorfo a $\mathbb{Q}[x]/(x^3 - 2)$. In effetti $x^3 - 2$ ammette $\beta = \sqrt[3]{2}$ come radice. Inoltre $x^3 - 2$ è un polinomio irriducibile su $\mathbb{Q}$: questo si può vedere con il criterio di Eisenstein, o più semplicemente verificando che $x^3 - 2$ non ammette radici razionali (a lezione abbiamo fatto così). Possiamo concludere che $[L : F] = 3$, dal momento che $L = F(\beta)$, ed il grado del polinomio minimo di β è 3.

  Per quanto riguarda le estensioni intermedie, è chiaro che se K è un'estensione intermedia tra F e L, allora il suo grado deve essere un divisore di 3. Ma allora le uniche possibilità sono $[K : F] = 1 \Rightarrow K = F$ e $[K : F] = 3 \Rightarrow K = L$. Concludiamo per l'impossibilità di estensioni intermedie.

  Terminiamo con la determinazione del gruppo di Galois. Gli automorfismi di L che fissano F sono determinati dall'immagine di β, che sappiamo essere un coniugato di β. Ora, i coniugati di β sono le radici del suo polinomio minimo su $\mathbb{Q}$, e cioè le soluzioni dell'equazione $x^3 - 2 = 0$. Ma è evidente che $L \subset \mathbb{R}$, e l'unica soluzione reale di questa equazione è β. Pertanto ogni automorfismo di L che fissi $\mathbb{Q}$ deve mandare β in se stesso, e coincide quindi con l'automorfismo identico.

  Concludiamo che l'unico elemento di $\mathrm{Gal}(L/F)$ è in questo caso l'identità, e pertanto che il gruppo di Galois dell'estensione è banale. Notiamo anche che il grado dell'estensione è diverso dall'ordine del gruppo di Galois. Con una terminologia che introdurremo in seguito, possiamo dire che $F \subset L$ non è un'estensione di Galois.
- $F = \mathbb{Q}, L = \mathbb{Q}(\sqrt[3]{2}, -\frac{1}{2} + i\frac{\sqrt{3}}{2})$. Indichiamo con β e ω gli elementi $\sqrt[3]{2}$ e $-\frac{1}{2} + i\frac{\sqrt{3}}{2}$, ed indichiamo con K l'estensione intermedia $\mathbb{Q}(\beta)$. Abbiamo visto, nel caso precedentemente considerato, che K è un'estensione di grado 3 di $\mathbb{Q}$. E' evidente come ω non appartenga a K: in effetti gli elementi di K sono tutti reali, mentre ω ha parte immaginaria non nulla. Pertanto $L = K(\omega)$ è un'estensione non banale di K. Il polinomio minimo di ω su $\mathbb{Q}$ è $x^2 + x + 1$. Di conseguenza, il polinomio minimo di ω su K deve essere un divisore di $x^2 + x + 1$; inoltre

non può avere grado 1, altrimenti $\omega \in K$ e l'estensione sarebbe banale. Quindi x^2+x+1 è il polinomio minimo di ω anche sul campo K, e l'estensione $K \subset L$ ha grado 2. Concludendo, $[K:F]=3, [L:K]=2$, da cui $[L:F]=6$.

Passiamo alle estensioni intermedie. Il grado di un'estensione intermedia deve dividere 6; escludendo i casi banali, deve essere quindi 2 oppure 3. E' facile verificare che i campi

$$\mathbb{Q}(\beta), \qquad \mathbb{Q}(\beta\omega), \qquad \mathbb{Q}(\beta\omega^2), \qquad \mathbb{Q}(\omega),$$

sono estensioni intermedie (tutte di grado 3 meno l'ultima, che ha grado 2). Più difficile è invece verificare come queste siano le uniche estensioni intermedie: sarà però evidente alla luce del teorema di corrispondenza di Galois, che dimostreremo in seguito.

Per quanto riguarda il gruppo di Galois dell'estensione $\mathbb{Q} \subset L$, osserviamo che $\beta, \beta\omega, \beta\omega^2$ sono le tre radici di x^3-2, e quindi $G = \mathrm{Gal}(L/F)$ agisce su di esse permutandole. Abbiamo visto a lezione come ogni permutazione induca un automorfismo: questo mostra che G è isomorfo al gruppo delle permutazioni su 3 elementi, e possiede pertanto 6 elementi. $F \subset L$ è quindi un'estensione di Galois. Si noti, incidentalmente, che L è campo di spezzamento del polinomio x^3-2: vedremo in seguito che un'estensione è di Galois se e solo se è il campo di spezzamento di qualche polinomio.

- $F=\mathbb{Q}, L=\mathbb{Q}(\sqrt{2},\sqrt{3})$. L è un'estensione di F di grado 4. Per convincercene, osserviamo che $\mathbb{Q}(\sqrt{2})$ è un'estensione di grado 2 che non contiene $\sqrt{3}$. Infatti, se il quadrato di $a+b\sqrt{2}, a, b \in \mathbb{Q}$ è 3 allora $a^2+2b^2+2ab\sqrt{2}=3 \Rightarrow 2ab=0, a^2+2b^2=3$. Ma da $2ab=0$ segue che $a=0$ oppure $b=0$. Se $b=0$ allora $a \in \mathbb{Q}$ è una radice quadrata di 3, il che è impossibile. Se invece $a=0$ allora $2b^2=3$, il che è di nuovo impossibile per lo stesso motivo.

  Pertanto il polinomio minimo di $\sqrt{3}$ su $\mathbb{Q}(\sqrt{2})$ non è di grado 1. Dovendo dividere x^2-3, sarà proprio questo polinomio. Allora il grado di $\sqrt{3}$ su $\mathbb{Q}(\sqrt{2})$ è 2, e $[L:\mathbb{Q}(\sqrt{2})]=2$, da cui $[L:F]=4$.

  Per quanto riguarda il gruppo di Galois di questa estensione, sappiamo che un automorfismo manda $\sqrt{2}$ in se stesso o in $-\sqrt{2}$ e lo stesso è vero per $\sqrt{3}$. Le quattro possibilità forniscono effettivamente quattro automorfismi, per cui questa estensione è di Galois. Le estensioni intermedie sono $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6})$. Che non ve ne siano altre, segue ancora dal teorema di corrispondenza di Galois. L è il campo di spezzamento del polinomio $(x^2-2)(x^2-3)$.
- $F=\mathbb{R}, L=\mathbb{C}$. In questo caso, $[L:F]=2$, dal momento che $1, i$ costituiscono una base reale di $\mathbb{C}$. Gli automorfismi di $\mathbb{C}$ che fissano $\mathbb{R}$ sono l'identità e la coniugazione complessa. $\mathbb{R} \subset \mathbb{C}$ è quindi un'estensione di Galois. $\mathbb{C}$ è il campo di spezzamento (su $\mathbb{R}$) del polinomio x^2+1, così come di ogni polinomio reale irriducibile di grado 2.

4.3. **Dimostrazione della corrispondenza di Galois.** Darò ora il resoconto più asettico possibile della dimostrazione data a lezione del teorema di corrispondenza della teoria di Galois. In questo paragrafo tutti i campi sono di caratteristica zero.

Lemma 4.2. *Siano $F \subset L$ campi, $\alpha \in L$ un elemento algebrico su F, $q(x) \in F[x]$ il suo polinomio minimo. Allora:*

(a) Se ϕ è un automorfismo di L, l'elemento $\beta=\phi(\alpha)$ ha lo stesso polinomio minimo di α.
(b) Se β ha lo stesso polinomio minimo di α esiste un (unico) automorfismo $\phi : F(\alpha) \to F(\beta)$ tale che $\beta=\phi(\alpha)$.

Dimostrazione. Ogni automorfismo di un campo manda somme in somme e prodotti in prodotti. In particolare, se ϕ è un automorfismo di L, allora $\phi(q(\alpha)) = q(\phi(\alpha))$. Ma allora, dal momento che $q(\alpha)=0$, avremo $q(\beta)=q(\phi(\alpha))=0$. Questo dimostra il primo enunciato.

Per quanto riguarda il secondo, ricordiamo che il campo $F(\alpha)$ è isomorfo al quoziente $F[x]/(q(x))$ tramite un isomorfismo che mette in corrispondenza α con la classe di congruenza $[x] \in F[x]/(q(x))$ ed è l'identità su F. Ma allora la composizione

$$F(\alpha) \xrightarrow{\sim} F[x]/(q(x)) \xrightarrow{\sim} F(\beta)$$

è un isomorfismo tra $F(\alpha)$ e $F(\beta)$ che manda α in β. □

Gli elementi in L che possiedono lo stesso polinomio minimo di un algebrico α sono talvolta detti *coniugati* di α in L.

Corollario 4.3. *Il gruppo di Galois di un'estensione finita è finito.*

Dimostrazione. Se $F \subset L$ è un'estensione finita, il teorema dell'elemento primitivo mostra l'esistenza di $\alpha \in L$ tale che $L = F(\alpha)$, quindi ogni automorfismo ϕ di $\mathrm{Gal}(L/F)$ è univocamente determinato dal valore $\phi(\alpha)$. Ma quest'ultimo va scelto tra i coniugati di α, che sono in numero finito. □

Questa dimostrazione ci insegna qualcosa in più dell'enunciato del corollario: l'ordine del gruppo di Galois di un'estensione finita non può essere più grande del grado dell'estensione. Saremo più precisi a proposito fra non molto.

Lemma 4.4. *Sia L un campo, e G un gruppo finito di automorfismi di L. Allora ogni elemento $\alpha \in L$ è algebrico su L^G, ed il suo grado divide l'ordine di G.*

Dimostrazione. Se $\phi \in G$, possiamo calcolare l'immagine di α attraverso ϕ. L'elemento $\phi(\alpha)$ che otterremo è, per il lemma precedente, un coniugato di α, quindi una radice del polinomio caratteristico di α.

Consideriamo allora l'insieme $\Gamma = \{\phi(\alpha) | \phi \in G\}$ dei coniugati di α che si ottengono in questo modo: X è detto anche *orbita* di α sotto l'azione di G. Possiamo allora formare il prodotto $f(x) = \prod_{\gamma \in \Gamma}(x - \gamma)$. E' facile vedere come $\phi(f(x))$ coincida con $f(x)$ per ogni $\phi \in G$: in effetti l'azione degli elementi di G si limita a permutare tra loro i fattori $x - \gamma$. Questo mostra che tutti i coefficienti del polinomio $f(x)$ sono invarianti per l'azione di G, e quindi che $f(x) \in L^G[x]$. Ma allora α soddisfa un polinomio — e cioè $f(x)$ — a coefficienti in L^G. Questo vuol dire che α è algebrico su L^G.

Per calcolare il grado di α abbiamo bisogno di essere un po' più precisi: innanzitutto mostriamo che $f(x)$ è il polinomio minimo di α su L^G. Questo è evidente, dal momento che tutte le radici di $f(x)$ sono coniugate ad α, e sono quindi radici del polinomio minimo $q(x) \in F[x]$ di α. Ma questo mostra che $f(x)$ divide il polinomio $q(x)$, che è irriducibile, da cui $f(x) = q(x)$.

Il grado di α è per definizione il grado del suo polinomio irriducibile $f(x)$, che è prodotto di tanti fattori di primo grado quanti sono gli elementi di Γ. Il grado di α è quindi pari al numero degli elementi di Γ.

Poniamo allora $H = \{\phi \in G | \phi(\alpha) = \alpha\}$. H è detto *stabilizzatore* di α, ed è chiaramente un sottogruppo di G. E' chiaro che se un automorfismo $\psi \in G$ è tale che $\psi(\alpha) = \gamma$, allora l'insieme degli elementi di G che mandano α in γ coincide con la classe laterale ψH (mostratelo!). Questo mostra che gli elementi di Γ sono in corrispondenza con le classi laterali di H in G, ed il loro numero $[G : H]$ divide l'ordine di G. Pertanto il grado di α divide $|G|$. □

Proposizione 4.5. *Sia L un campo, e G un gruppo finito di automorfismi di L. Allora l'ordine di G coincide con il grado dell'estensione $L^G \subset L$.*

Dimostrazione. La dimostrazione sarebbe semplice se sapessimo che $L^G \subset L$ è un'estensione finita. In tal caso il teorema dell'elemento primitivo ci assicura l'esistenza di $\alpha \in L$ tale che $L = L^G(\alpha)$, pertanto per calcolare il grado dell'estensione è sufficiente determinare il grado dell'elemento α. Per il Lemma 4.4, o meglio per la sua dimostrazione, il grado di α è pari al numero dei suoi coniugati della forma $\phi(\alpha), \phi \in G$. Ma se $\phi(\alpha) = \alpha$, allora ϕ è l'identità su $L^G(\alpha)$. Pertanto, lo stabilizzatore di α in G coincide con il solo automorfismo identico, e quindi gli elementi dell'orbita di α sono tanti quanti gli elementi di G. Allora il grado di α è $|G|$, e quindi $[L : L^G] = |G|$.

Perché questa dimostrazione sia valida, è essenziale però convincersi che $L^G \subset L$ è un'estensione finita, ma a lezione ho clamorosamente dimenticato di farlo vedere. Mostriamolo per assurdo: scegliamo un elemento $\alpha_1 \in L$ non contenuto in $F = L^G$. Per il lemma precedente, α_1 è algebrico su F, quindi $F_1 = F(\alpha_1)$ è un'estensione finita di F, che non può coincidere con L (perché L non è un'estensione finita). Allora possiamo trovare un elemento $\alpha_2 \in L$ non contenuto in F_1, e formare $F_2 = F_1(\alpha_2)$. Anche F_2 è un'estensione finita di F, e possiamo quindi continuare con questo procedimento in modo da formare una catena di estensioni

$$F \subset F_1 \subset F_2 \subset \ldots \subset F_n \subset \ldots$$

tutte contenute in L. Ogni F_i è un'estensione finita di F, quindi per il teorema dell'elemento primitivo esiste $\gamma_i \in F_i$ tale che $F_i = F(\gamma_i)$. Per il Lemma 4.4 il grado di γ_i divide $|G|$ quindi $[F_i : F] < |G|$ per ogni i, ma questo è assurdo, in quanto per costruzione ogni campo F_i è contenuto propriamente nel successivo, e quindi i numeri $[F_i : F]$ sono strettamente crescenti in i. □

Corollario 4.6. *Sia $F \subset L$ un'estensione finita, $G = \mathrm{Gal}(L/F)$ il suo gruppo di Galois. Allora $|G|$ divide $[L : F]$*

Dimostrazione. Sappiamo che G è un gruppo finito di automorfismi di L e quindi, per la proposizione appena dimostrata, $|G| = [L : L^G]$.

Per la definizione di gruppo di Galois, ogni elemento di F è fissato dagli automorfismi contenuti in G, e quindi $F \subset L^G$. Ma allora $[L : F] = [L : L^G][L^G : F]$ e quindi $|G|$ divide $[L : F]$. □

Diremo che un'estensione finita $F \subset L$ è un'*estensione di Galois* o anche *normale* se il grado $[L : F]$ è pari all'ordine del gruppo di Galois $\mathrm{Gal}(L/F)$. Questa definizione è per il momento insoddisfacente: definisce un concetto fondamentale come le estensioni di Galois in termini di una loro proprietà accessoria, piuttosto che tramite una qualche caratteristica fondamentale. Vedremo la proprietà caratterizzante delle estensioni di Galois, in termini di automorfismi, in fondo al paragrafo.

Corollario 4.7. *Sia G un gruppo finito di automorfismi del campo L. Allora L è un'estensione di Galois di L^G, e $G = \mathrm{Gal}(L/L^G)$.*

Dimostrazione. Sappiamo già che $[L : L^G] = |G|$. Ma G è un sottogruppo di $\mathrm{Gal}(L/L^G)$, il cui ordine deve dividere $[L : L^G]$. □

Lemma 4.8. *Se $F \subset L$ è un'estensione di Galois, e $G = \mathrm{Gal}(L/F)$, allora $F = L^G$.*

Dimostrazione. Per la definizione di gruppo di Galois, abbiamo $F \subset L^G$. Ora, $[L : L^G] = |G|$ per la Proposizione 4.5, mentre $[L : F] = |G|$ per la definizione di estensione di Galois. Pertanto $F = L^G$, e $q(x)$ è il polinomio minimo di α su F. □

Proposizione 4.9. *Sia $F \subset L$ un'estensione di Galois, $q(x) \in F[x]$ un polinomio irriducibile. Se esiste $\alpha \in L$ tale che $q(\alpha) = 0$, allora $q(x)$ si spezza in fattori lineari su L.*

Dimostrazione. Sia $G = \mathrm{Gal}(L/F)$. Con la notazione del Lemma 4.4, il polinomio minimo di α su $L^G = F$ si ottiene come

$$q(x) = \prod_{\gamma \in \Gamma} (x - \gamma),$$

e quindi si spezza completamente su L. □

Siamo pronti per una caratterizzazione completa delle estensioni di Galois.

Corollario 4.10. *Se $F \subset L$ è un'estensione di Galois, allora esiste un polinomio irriducibile $q(x) \in F[x]$ di cui L è il campo di spezzamento.*

Dimostrazione. Scriviamo $L = F(\alpha)$ per mezzo del teorema dell'elemento primitivo. Se $q(x)$ è il polinomio minimo di α su F, la proposizione precedente mostra che L è il campo di spezzamento di $q(x)$. □

Questo corollario si inverte.

Lemma 4.11. *Sia $\phi : F \to \overline{F}$ un isomorfismo di campi, $f(x) \in F[x], \overline{f}(x) \in \overline{F}[x]$ polinomi corrispondenti tramite ϕ, ed $L, \overline{L}$ i rispettivi campi di spezzamento. Allora il numero degli isomorfismi $\Phi : L \to \overline{L}$ che estendono ϕ è uguale a $[L : F]$.*

Dimostrazione. Per induzione su $[L : F]$. Sia $q(x) \in F[x]$ un fattore irriducibile di $f(x)$. Allora $\phi(q(x))$ è anch'esso un fattore irriducibile di $\overline{f}(x)$. Chiaramente $q(x)$ si spezza completamente su L, e quindi $\phi(q(x))$ fa altrettanto su $\overline{L}$. Se $\alpha \in L$ è una radice di $q(x)$, $F(\alpha) \simeq F[x]/(q(x))$. Allo stesso modo $\overline{F}(\beta) \simeq \overline{F}[x]/(\phi(q(x)))$ per ogni radice $\beta \in \overline{L}$ di $\phi(q(x))$. Ma allora per ogni tale β è possibile estendere ϕ ad un isomorfismo $F(\alpha) \to \overline{F}(\beta)$ che manda α in β.

Il numero di possibili scelte di β è uguale al grado di $\phi(q(x))$, che è uguale a quello di $q(x)$, e cioè a $[F(\alpha) : F]$. Pertanto ϕ si estende in $[F(\alpha) : F]$ modi diversi ad $F(\alpha)$. Per ipotesi induttiva, ciascuno di questi isomorfismi si estende in $[L : F(\alpha)]$ modi a tutto L. In totale abbiamo $[L : F(\alpha)][F(\alpha) : F] = [L : F]$ estensioni di ϕ ad isomorfismi tra i campi di spezzamento. □

Proposizione 4.12. *Sia L il campo di spezzamento del polinomio $f(x) \in F[x]$. Allora $F \subset L$ è un'estensione di Galois.*

Dimostrazione. Gli elementi del gruppo di Galois sono gli isomorfismi $\Phi : L \to L$ che estendono l'isomorfismo $\mathrm{id} : F \to F$. Per il lemma appena dimostrato, il loro numero è $[L : F]$. □

Corollario 4.13. *Siano $F \subset K \subset L$ campi. Se $F \subset L$ è un'estensione di Galois, allora anche $K \subset L$ è di Galois.*

Dimostrazione. Per il Corollario 4.9, L è il campo di spezzamento di un polinomio a coefficienti in F. Ma dal momento che F è contenuto in K, questo stesso polinomio può essere visto come polinomio a coefficienti in K, ed L ne è ancora il campo di spezzamento. Per la proposizione appena dimostrata, $K \subset L$ è allora un'estensione di Galois. □

Siamo ora pronti per affrontare il teorema di corrispondenza di Galois.

Teorema 4.14. *Sia $F \subset L$ un'estensione di Galois, $G = \mathrm{Gal}(L/F)$ il suo gruppo di Galois. Vi è una corrispondenza biunivoca*

$$\{\textit{Estensioni intermedie } F \subset K \subset L\} \qquad \longleftrightarrow \qquad \{\textit{Sottogruppi } H < G\}$$

che associa all'estensione $F \subset K \subset L$ il sottogruppo $\mathrm{Gal}(L/K)$ di G, e al sottogruppo $H < G$ l'estensione $F \subset L^H \subset L$.

Dimostrazione. Dobbiamo verificare che le applicazioni $f : K \mapsto \mathrm{Gal}(L/K)$ e $g : H \mapsto L^H$ sono una l'inversa dell'altra. Se H è un sottogruppo di G, poniamo $K = L^H$. Per il Lemma 4.7 abbiamo che $\mathrm{Gal}(L/L^H) = H$, quindi $f \circ g$ è l'identità.

Sia ora $F \subset K \subset L$ un'estensione intermedia, e poniamo $H = \mathrm{Gal}(L/K)$. H è chiaramente un sottogruppo di G, e l'estensione $L^H \subset L$ ha grado $|H|$. Per il Corollario 4.13 l'estensione $K \subset L$ è di Galois, quindi $|H| = [L : K]$. Il campo K è chiaramente contenuto in L^H, ed abbiamo visto come $[L : K] = [L : L^H] = |H|$. Questo mostra che $L^H = K$, e quindi che anche la composizione $g \circ f$ è l'identità. □

Osservazione. Nelle ipotesi del teorema appena dimostrato, si ha $[K : F] = [G : H]$ se H è il sottogruppo corrispondente al campo intermedio K. Infatti $[L : K] = |H|$, mentre $[L : F] = |G|$, e quindi $[K : F] = [L : F]/[L : K] = |G|/|H| = [G : H]$.

Mostreremo ora che nella corrispondenza tra sottogruppi ed estensioni intermedie, ai sottogruppi normali corrispondono le sottoestensioni di Galois, e viceversa.

Lemma 4.15. *Siano $F \subset K \subset L$ campi, $F \subset L$ un'estensione di Galois, $G = \mathrm{Gal}(L/F)$, $H = \mathrm{Gal}(L/K)$. Per ogni scelta di $\sigma \in G$ il sottogruppo $\mathrm{Gal}(L/\sigma(K))$ di G coincide con il coniugato $\sigma H \sigma^{-1}$ del sottogruppo $H < G$. In particolare H è un sottogruppo normale di G se e solo se $\sigma(K) = K$ per ogni $\sigma \in G$.*

Dimostrazione. Sia $K' = \sigma(K)$. Chiaramente K' è anch'esso un'estensione intermedia di $F \subset L$. Vogliamo mostrare che $\mathrm{Gal}(L/K') = \sigma H \sigma^{-1}$. Innanzitutto, se $\phi = \sigma h \sigma^{-1}$, con $h \in H$, allora $\phi(\sigma(k)) = \sigma h \sigma^{-1} \sigma(k) = \sigma(h(k))$. L'azione di $h \in H = \mathrm{Gal}(L/K)$ fissa ogni elemento del campo K, quindi $\sigma(h(k))$ appartiene a $K' = \sigma(K)$. Abbiamo quindi verificato che $\sigma H \sigma^{-1} \subset \mathrm{Gal}(L/K')$.

Per mostrare l'inclusione opposta, basta notare che $K = \sigma^{-1}(K)$ e quindi che $\sigma^{-1} \mathrm{Gal}(L/K')\sigma \subset H$, da cui $\mathrm{Gal}(L/K') \subset \sigma H \sigma^{-1}$. La seconda parte dell'enunciatoè allora evidente. □

Teorema 4.16. *Siano $F \subset K \subset L$ campi con la proprietà che $F \subset L$ è un'estensione di Galois. Allora K è un'estensione di Galois di F se e solo se $\mathrm{Gal}(L/K)$ è un sottogruppo normale di $\mathrm{Gal}(L/F)$. In tal caso $\mathrm{Gal}(K/F)$ è isomorfo al quoziente $\mathrm{Gal}(L/F)/\mathrm{Gal}(L/K)$.*

Dimostrazione. Per il lemma precedente, il sottogruppo $\mathrm{Gal}(L/K)$ è normale se e solo se $\sigma(K) = K$ per ogni $\sigma \in \mathrm{Gal}(L/F)$. Se $\sigma(K) = K$ per ogni $\sigma \in \mathrm{Gal}(L/F)$, possiamo allora costruire un omomorfismo di gruppi $\pi : \mathrm{Gal}(L/F) \to \mathrm{Gal}(K/F)$ che associa all'automorfismo σ la sua restrizione[2] $\pi(\sigma) = \sigma|_K$ al sottocampo K. Il nucleo di π è dato dagli automorfismi che fissano il sottocampo K, e cioè da $\mathrm{Gal}(L/K)$.

Ora, sia $F \subset L$ che $K \subset L$ sono estensioni di Galois, e quindi $|\mathrm{Gal}(L/F)| = [L : F], |\mathrm{Gal}(L/K)| = [L : K]$. Questo dimostra che l'ordine del quoziente $\mathrm{Gal}(L/F)/\mathrm{Gal}(L/K)$ è esattamente $[L : F]/[L : K] = [K : F]$. L'immagine di π è quindi un sottogruppo di $\mathrm{Gal}(K/F)$ di ordine $[K : F]$. Dal momento che l'ordine di $\mathrm{Gal}(K/F)$ divide $[K : F]$ deduciamo che l'immagine di π coincide con $\mathrm{Gal}(K/F)$, e che tale gruppo ha ordine $[K : F]$. In particolare, $F \subset K$ è un'estensione di Galois. Abbiamo quindi mostrato che se $\mathrm{Gal}(L/K)$ è un sottogruppo normale di $\mathrm{Gal}(L/F)$, allora $F \subset K$ è un'estensione di Galois.

---

[2] Se $\sigma(K)$ non coincide con K, allora σ non induce un automorfismo di K, perché "va fuori".

Viceversa, supponiamo che $F \subset K$ sia un'estensione di Galois, e scriviamo $K = F(\alpha)$ per mezzo del teorema dell'elemento primitivo. Un automorfismo di L deve mandare α in un suo coniugato, ma per la Proposizione 4.10 tutti i coniugati di α sono contenuti in K. Quindi ogni elemento di $\mathrm{Gal}(L/F)$ manda elementi di K in elementi di K. Di conseguenza, $\mathrm{Gal}(L/K)$ è un sottogruppo normale di $\mathrm{Gal}(L/F)$. □

Quest'ultimo risultato spiega quale dovrebbe essere la vera definizione di un'estensione di Galois: $F \subset K$ è di Galois se ogni automorfismo di L, $K \subset L$, che fissa F elemento per elemento, manda K in se stesso.

5. ALCUNE APPLICAZIONI CLASSICHE

5.1. **Estensioni ciclotomiche.**

5.2. **Costruzioni con riga e compasso.**

5.3. **Estensioni di Kummer.**

5.4. **Risolubilità di equazioni algebriche per radicali.**

5.5. **Reciprocità quadratica.**

E-mail address: dandrea@mat.uniroma1.it