

Introduzione alla Teoria di Galois

Andrea Caranti

Sandro Mattarei

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DEGLI STUDI DI TRENTO,
VIA SOMMARIVE 14, 38050 POVO (TRENTO)

Pagina Web: <http://www-math.science.unitn.it/~caranti/>

E-mail: caranti@science.unitn.it

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DEGLI STUDI DI TRENTO,
VIA SOMMARIVE 14, 38050 POVO (TRENTO)

Pagina Web: <http://www-math.science.unitn.it/~mattarei/>

E-mail: mattarei@science.unitn.it

Indice

Introduzione	7
Cosa sono queste note	8
Dove trovare queste note	8
Di cosa parla il corso	8
Bibliografia	9
Le lezioni	11
Capitolo 1. Richiami	13
1.1. Alcuni richiami dai corsi precedenti di Algebra	13
1.2. Isomorfismi	16
1.3. Altri esercizi	16
Capitolo 2. Campo di spezzamento	17
2.1. Campo di spezzamento di un polinomio	17
2.2. Esistenza	17
2.3. Unicità	20
2.4. Quanti isomorfismi?	22
Capitolo 3. Corrispondenza di Galois	25
3.1. Il gruppo di Galois	25
3.2. La corrispondenza di Galois	27
3.3. Gruppo di Galois e gruppo simmetrico	28
3.4. Estensioni normali	29
3.5. Un commento sul concetto di estensione normale	30
3.6. Sottogruppi e campi intermedi chiusi	30
3.7. Corrispondenze di Galois più generali	31
3.8. Una diseguaglianza	32
3.9. Casi particolari	32
3.10. Un commento sul Teorema di Lagrange	33
3.11. Un'altra diseguaglianza	34
3.12. Dedekind	35
3.13. Oggetti chiusi in estensioni di grado finito	36
3.14. Un commento	37
3.15. Un gruppo di Galois grande è una buona cosa	37
3.16. Altri esercizi	38
Capitolo 4. Estensioni normali e campi di spezzamento	39
4.1. Un lemma fondamentale	39

4.2.	Separabilità	40
4.3.	Radici multiple	41
4.4.	Campi finiti	41
4.5.	Unicità dei campi finiti	42
4.6.	Un campo di spezzamento non normale	43
4.7.	Altri esercizi	44
Capitolo 5.	Chiusure spezzanti e chiusure normali	45
5.1.	Una caratterizzazione dei campi di spezzamento	45
5.2.	Osservazioni	46
Capitolo 6.	Estensioni normali e sottogruppi normali	49
6.1.	Campi intermedi stabili	49
6.2.	Stabilità e normalità	49
6.3.	Una situazione più generale	50
6.4.	Altri esercizi	51
Capitolo 7.	Equazioni risolubili per radicali	53
7.1.	Caratteristica zero	53
7.2.	L'equazione di secondo grado	53
7.3.	Eliminare un coefficiente	54
7.4.	Estensioni radicali e gruppi risolubili	54
7.5.	Un commento	56
7.6.	E se non ci sono le radici dell'unità?	57
7.7.	Un commento	58
7.8.	Un'equazione non risolubile per radicali	59
7.9.	Un commento	61
7.10.	Permutazioni pari e dispari, e gruppo alterno	61
7.11.	Il gruppo simmetrico su cinque elementi non è risolubile	62
7.12.	Un commento	64
7.13.	L'equazione generale di n -simo grado	65
7.14.	Un commento	66
7.15.	Determinante di Vandermonde	66
7.16.	Un commento	67
7.17.	Da gruppi risolubili a estensioni radicali	67
7.18.	Un commento	69
7.19.	Un'altra dimostrazione	70
7.20.	Trovare una base normale	70
7.21.	E se non ci sono le radici dell'unità?	72
7.22.	Un esempio: L'equazione biquadratica generale	73
Capitolo 8.	L'equazione di terzo grado	75
8.1.	Discriminante	75
8.2.	Un commento	76
8.3.	Il gruppo di Galois dell'equazione di terzo grado	78
8.4.	Espressione esplicita per le radici cubiche	79
8.5.	Le formule di Cardano	81

8.6. Un altro modo di trovare le formule di Cardano	81
Capitolo 9. Casus Irreducibilis	83
9.1. La teoria	83
9.2. Un esempio	84
Capitolo 10. L'equazione di quarto grado	85
10.1. Cosa dice MAPLE	87
Capitolo 11. Teoria di Galois delle estensioni di dimensione infinita	89
11.1. Campi di spezzamento di famiglie di polinomi	89
11.2. Topologia di Krull sul gruppo di Galois	91
11.3. Chiusure	91
11.4. Un'osservazione finale	94
Capitolo 12. Numeri trascendenti	95
12.1. Cantor	95
12.2. Liouville	97
Bibliografia	99

Introduzione

Questa introduzione è scritta in prima persona da Andrea Caranti.

Cosa sono queste note

Ho cominciato a scrivere queste note per il corso di Algebra Superiore (primo modulo) nell'Anno Accademico 1997/98. Sono state le prime note di un corso che abbia scritto sistematicamente in \LaTeX . Ho continuato a lavorarci nell'A.A. 1998/99. L'idea non era quella di produrre un libro, ma di cercare di conservare un po' della freschezza di una lezione fatta in classe, "dal vivo".

Nell'A.A. 2001/02 il corso l'ha fatto Sandro Mattarei, e ora queste note incorporano diverse correzioni (errori di segno, ed altro...) e integrazioni da lui proposte, che spero di aver inserito correttamente nel testo. Modifiche ulteriori le ho fatte quando ho tenuto il corso negli A.A. 2002/03 e 2003/04. Altre modifiche e aggiunte le ho fatte durante il corso dell'A.A. 2004/05. Oggigiorno il corso si chiama, con guadagno di chiarezza, *Teoria di Galois*.

Il testo come è adesso contiene alcune argomenti in più rispetto a quelli che si svolgono nel corso (possono sempre essere utili per uno studente interessato); qualcuno degli argomenti trattato nel corso invece manca, o è trattato in maniera schematica: l'equazione di quarto grado, il calcolo esplicito di alcuni gruppi di Galois "facili", il metodo della riduzione modulo un primo per calcolare i gruppi di Galois. Magari quest'anno qualcosa in più lo scrivo – è quello che dico ogni anno ;-)

Dove trovare queste note

Una versione aggiornata di queste note è disponibile attraverso la pagina Web
<http://www-math.science.unitn.it/~caranti/>

Di cosa parla il corso

Il corso vuole essere una presentazione relativamente standard della Teoria di Galois, sostanzialmente basata su [Kap95], anche se anticipo il legame fra estensioni normali e campi di spezzamento. Questo perché i corsi di Algebra di base terminano in genere con la dimostrazione dell'esistenza del campo di spezzamento (e l'applicazione all'esistenza dei campi finiti); è quindi naturale riprendere il discorso parlando dell'unicità del campo di spezzamento, e a questo punto tanto vale contare gli automorfismi che si ottengono, ecc.

La teoria di Galois associa a una estensione di campi un gruppo finito, e permette di tradurre proprietà delle estensioni in proprietà dei gruppi corrispondenti, e viceversa.

Tempo permettendo si vorrebbe arrivare a trattare i seguenti argomenti.

La teoria delle equazioni risolubili per radicali. Come è noto già dall'antichità, l'equazione di secondo grado

$$x^2 + bx + c = 0$$

ha soluzioni

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

Questa formula esprime la soluzioni dell'equazione a partire dai suoi coefficienti, utilizzando le quattro operazioni, e una estrazione di radice. Formule analoghe si possono dare per le equazioni di terzo e quarto grado. La teoria che svilupperemo sarà in grado di farci ricavare queste formule, e di dimostrare l'impossibilità dell'esistenza di formule generali di questo tipo per equazioni di grado cinque e superiori.

La teoria delle estensioni di grado infinito, o Qui la cosa interessante è che queste estensioni si comprendono se si da ai gruppi associati la struttura di gruppi topologici.

Numeri trascendenti. In realtà ci sono diversi studenti del corso dell'A.A. 1998/99 che non hanno studiato topologia, e che quindi non potrebbero fruire come si deve questa parte del corso. Per cambiare, avrei voluto fare la dimostrazione della trascendenza di e e π , ma è troppo complicata per questo corso. Mi limiterò alla dimostrazione di Cantor dell'*esistenza* di numeri trascendenti, e alla *costruzione* esplicita di Liouville di alcuni numeri trascendenti. Una delle mie fonti è [CR71], che dopo tanti anni rimane sempre un magnifico libro di matematica.

Ringrazio Pino Vigna Suria per aver letto questa parte delle note, ed avere suggerito diverse correzioni e miglioramenti.

Bibliografia

Il filo conduttore della parte di Teoria di Galois è tendenzialmente quello di [Kap95]. Qualche argomento è tratto da [Jac85]; a volte, quando qualche argomento su quest'ultimo testo non è chiaro, può essere illuminante andare a vedere [vdW71] (o [vdW91]), che si basa in parte sulle lezioni originali di E. Artin e E. Noether. Per la parte dei gruppi topologici si segue [Hig74], mentre per le estensioni di grado infinito si utilizzano argomenti di [Lan84].

Le lezioni

CAPITOLO 1

Richiami

In questo capitolo diamo alcuni brevi cenni agli argomenti del primo corso di Algebra che ci sono utili in questo corso. Se necessario, è bene consultare un testo, ad esempio [Jac85] o [Lan84].

1.1. Alcuni richiami dai corsi precedenti di Algebra

Sia E un campo, e F un suo sottoanello che sia a sua volta un campo. Allora si dice che E è una *estensione di F* , ovvero che E/F è una estensione (di campi). Nonostante il simbolo, non c'è nessun quoziente! (Ricordate che un campo non ha altri ideali che lo $\{0\}$ e sé stesso.)

Se E/F è una estensione, e $\alpha \in E$, si può considerare il più piccolo sottoanello $F[\alpha]$ di E che contenga F e α . Si può vedere che esiste per ragioni generali, ma è facile vedere che esso ha la forma

$$\begin{aligned} F[\alpha] &= \\ &= \{ a_0 + a_1\alpha + \cdots + a_i\alpha^i + \cdots + a_n\alpha^n : n \in \mathbf{N}, a_i \in F \} = \\ &= \{ f(\alpha) : f(x) \in F[x] \}. \end{aligned}$$

In altre parole, $F[\alpha]$ è l'immagine del *morfismo valutazione in α* :

$$\begin{aligned} \varphi_\alpha : F[x] &\rightarrow E \\ f(x) &\mapsto f(\alpha). \end{aligned}$$

Dunque $\ker(\varphi_\alpha) = \{ f(x) \in F[x] : f(\alpha) = 0 \}$ è l'insieme di tutti i polinomi che si annullano su α . Se $\ker(\varphi_\alpha) = \{0\}$, ovvero l'unico polinomio in $F[x]$ che si annulla su α è il polinomio nullo, allora si dice che α è *trascendente su F* , e si ha $F[x] \cong F[\alpha]$. Se invece $\ker(\varphi_\alpha) \neq \{0\}$, ed esiste quindi almeno un polinomio non nullo in $F[x]$ che ha α per radice, si dice che α è *algebrico su F* . E' noto che gli ideali di $F[x]$ sono principali, per cui si può scrivere $\ker(\varphi_\alpha) = (m) = \{ m \cdot g : g \in F[x] \}$, ove m è il polinomio minimo di α su F , che è caratterizzato dalle seguenti proprietà:

1. $m(\alpha) = 0$;
2. m è monico;
3. m ha grado minimo fra tutti i polinomi non nulli che si annullano su α

Detto esplicitamente, il fatto che $\ker(\varphi_\alpha) = (m)$ vuol dire che un polinomio in $f \in F[x]$ si annulla su α se e solo se m divide f .

ESERCIZIO 1. Sia E/F una estensione di campi, $\alpha \in E$ un elemento, e $0 \neq f \in F[x]$ un polinomio monico (dunque non nullo) tale che $f(\alpha) = 0$.

Si mostri che sono equivalenti le due affermazioni:

1. f è il polinomio minimo di α su F , e
2. f è irriducibile in $F[x]$.

Da questo segue che se α è algebrico su F , allora $F[\alpha]$ è un campo, e coincide quindi con il più piccolo sottocampo $F(\alpha)$ di E che contenga F ed α . Infatti, sia $0 \neq f(\alpha) \in F[\alpha]$. Dunque $f \notin (m)$, e quindi f e m sono primi fra loro, dato che m è irriducibile. Ne segue che esistono $h, k \in F[x]$, che si possono trovare con l'algoritmo di Euclide, tali che

$$1 = f(x)h(x) + m(x)k(x).$$

Sostituendo α al posto di x , e tenendo conto che $m(\alpha) = 0$, si ottiene

$$1 = f(\alpha)h(\alpha),$$

e dunque $h(\alpha) \in F[\alpha]$ è l'inverso di $f(\alpha)$.

ESERCIZIO 2. Siano $K \subseteq F \subseteq E$ campi, e $\alpha \in E$. Si mostri che se α è algebrico su K , allora lo è anche su F , e il polinomio minimo di α su F è un divisore del polinomio minimo di α su K , e un multiplo di $x - \alpha$. Notate che $x - \alpha$ è il polinomio minimo di α su E .

Si mostri con un esempio che α può essere algebrico su F senza esserlo su K .

Se E/F è una estensione, allora si può vedere E come uno spazio vettoriale su F . La dimensione $\dim_F(E)$ si dice *grado di E su F* , e si indica con il simbolo $|E : F|$. Il nome è giustificato dal fatto che se α è *algebrico su F di grado n* , ovvero il suo polinomio minimo su F ha grado n , allora si ha

$$n = |F[\alpha] : F| = \dim_F(F[\alpha]),$$

una base di $F[\alpha]$ su F essendo formata da $1, \alpha, \dots, \alpha^{n-1}$.

ESERCIZIO 3. Se una estensione E/F ha grado finito, allora ogni elemento di E è algebrico su F , di grado un divisore di $|E : F|$.

(*Suggerimento:* Se $|E : F| = n$, e $\alpha \in E$,

$$1, \alpha, \alpha^2, \dots, \alpha^n$$

sono $n + 1$ elementi di uno spazio vettoriale di dimensione n , dunque ... Per la seconda parte, usare la formula dei gradi qui sotto.)

Il viceversa non vale, come suggerito dall'esercizio 5. Ricordiamo a questo proposito la formula dei gradi, che dice in sostanza che se $K \subseteq F \subseteq E$ sono campi, e il grado $|E : K|$ è finito, allora

$$|E : K| = |E : F| \cdot |F : K|.$$

ESERCIZIO 4. Dimostrare la formula dei gradi.

(*Suggerimento:* Si prendano una base u_1, \dots, u_n di E su F , e una base v_1, \dots, v_m di F su K . Si mostri che gli nm elementi $u_i \cdot v_j$ sono una base di E su K .)

Utilizzando questa formula, si può vedere che la somma e il prodotto di due numeri algebrici sono algebrici, e lo stesso vale per l'inverso di un numero algebrico non nullo. Usando questo fatto, si può fare il seguente ...

ESERCIZIO 5. Si consideri l'insieme

$$A = \{ \alpha \in \mathbf{C} : \alpha \text{ è algebrico su } \mathbf{Q} \}.$$

Si mostri che A è un sottocampo di \mathbf{C} , e che il grado $|A : \mathbf{Q}|$ non è finito. (*Suggerimento:* Si considerino gli elementi $\alpha_n = \sqrt[n]{2}$. Qual è il grado di α_n su \mathbf{Q} ?)

LEMMA 1.1.1 (Corollario del Lemma di Gauss).

Un polinomio primitivo $f(x) \in \mathbf{Z}[x]$ è irriducibile in $\mathbf{Q}[x]$ se e solo se lo è in $\mathbf{Z}[x]$.

Qui *primitivo* vuol dire che il massimo comun divisore fra i coefficienti è 1. Altrimenti si casca nel problema che il polinomio $2x$ è irriducibile in $\mathbf{Q}[x]$, dato che 2 è invertibile in \mathbf{Q} , mentre non lo è in $\mathbf{Z}[x]$. Se $f(x)$ è monico, allora è senz'altro primitivo.

DIMOSTRAZIONE. Omessa. □

PROPOSIZIONE 1.1.2 (Criterio di Eisenstein). $f(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbf{Z}[x]$, p primo. $p \mid a_{n-1}, a_{n-2}, \dots, a_1, a_0$, ma $p \nmid a_n$, e $p^2 \nmid a_0$, allora $f(x)$ è irriducibile in $\mathbf{Q}[x]$.

DIMOSTRAZIONE. Grazie al Lemma, basta dimostrare che $f(x)$ è irriducibile in $\mathbf{Z}[x]$. Se $f(x) = g(x)h(x)$ per certi $g(x) = b_r x^r + \dots + b_0$ e $h(x) = c_s x^s + \dots + c_0$ in $\mathbf{Z}[x]$, con $r, s > 0$, e $b_r c_s \neq 0$, da cui $r + s = n$, allora in $(\mathbf{Z}/p\mathbf{Z})[x]$ avremo $\bar{a}_n x^n = (\bar{b}_r x^r + \dots + \bar{b}_0)(\bar{c}_s x^s + \dots + \bar{c}_0)$. Ne segue che $p \mid b_{r-1}, \dots, b_0, c_{r-1}, \dots, c_0$, e quindi $p^2 \mid b_0 c_0 = a_0$, assurdo. □

Un'applicazione importante è l'irriducibilità in $\mathbf{Q}[x]$ del polinomio ciclotomico

$$x^{p-1} + \dots + x + 1 = \frac{x^p - 1}{x - 1},$$

dove p è un primo; il Criterio di Eisenstein non si applica direttamente ad esso, ma al polinomio

$$\frac{(x+1)^p - 1}{(x+1) - 1} = x^{p-1} + \binom{p}{p-1} x^{p-2} + \dots + \binom{p}{2} x + \binom{p}{1}$$

ottenuto da esso mediante una sostituzione (invertibile!).

L'utilizzo di tali polinomi è un suggerimento alternativo per lo svolgimento dell'Esercizio 3.

A questo proposito, un altro modo di svolgere l'Esercizio 5 potrebbe essere sfruttare il fatto che $|\mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_k}) : \mathbf{Q}| = 2^k$, dove i p_i sono primi distinti. Questo si può mostrare usando le estensioni ai numeri algebrici delle valutazioni p -adiche, ma non è certo un modo semplice.

In [Ric74] viene dimostrato, usando teoria di Galois elementare, che se p_1, \dots, p_k sono primi distinti, e $n > 1$, allora $|\mathbf{Q}(\sqrt[n]{p_1}, \dots, \sqrt[n]{p_k}) : \mathbf{Q}| = n^k$. Il caso particolare $n = 2$ qui sopra non è in realtà troppo difficile da fare per induzione, portandosi appresso il fatto che le estensioni di grado 2 qui dentro sono della forma $\mathbf{Q}(\sqrt{p_{i_1} \dots p_{i_s}})$.

1.2. Isomorfismi

Se A e B sono due anelli, una mappa $\varphi : A \rightarrow B$ si dice un *isomorfismo* se φ è biiettiva, e φ conserva le operazioni, ovvero

$$\varphi(x + y) = \varphi(x) + \varphi(y), \quad \varphi(xy) = \varphi(x)\varphi(y)$$

per ogni $x, y \in A$.

ESERCIZIO 6.

- Si mostri che l'inversa di un isomorfismo è un isomorfismo.
- Se C è un terzo anello, e $\psi : B \rightarrow C$ è un isomorfismo, allora la composizione $\psi \circ \varphi$ è un isomorfismo.

1.3. Altri esercizi

ESERCIZIO 7. Sia $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbf{Z}[x]$, con $a_n, a_0 \neq 0$.

- Sia $\alpha \in \mathbf{Q}$ una radice di f , e si scriva $\alpha = \frac{u}{v}$, con u, v interi coprimi. Si mostri che u divide a_0 , e v divide a_n .
- Si assuma ora f monico, cioè $a_n = 1$. Si mostri che se $\alpha \in \mathbf{Q}$ è una radice di f , allora $\alpha \in \mathbf{Z}$, e α divide a_0 .

CAPITOLO 2

Campo di spezzamento

2.1. Campo di spezzamento di un polinomio

Se F è un campo, e $f \in F[x]$ è monico, di grado positivo, allora una estensione E di F si dice *campo di spezzamento di f su F* se valgono

1. Esistono $\alpha_1, \alpha_2, \dots, \alpha_n \in E$ tali che

$$f(x) = (x - \alpha_1) \cdot (x - \alpha_2) \cdot \dots \cdot (x - \alpha_n).$$

2. Si ha

$$E = F(\alpha_1, \alpha_2, \dots, \alpha_n).$$

La prima condizione dice che in E ci sono tutte le radici di F . La seconda ha, come vedremo, lo scopo di assicurare l'unicità. Infatti se un campo contiene tutte le radici di un polinomio, anche ogni campo più grande le contiene. Per individuarne uno, la cosa sensata è pertanto prendere il minimo.

ESERCIZIO 8. Definiamo $F(\alpha_1, \alpha_2, \dots, \alpha_n)$ come *il più piccolo campo* (in una opportuna estensione) che contenga F e $\alpha_1, \alpha_2, \dots, \alpha_n$. Si mostri che

$$E = F(\alpha_1, \alpha_2, \dots, \alpha_n) = F(\alpha_1)(\alpha_2) \dots (\alpha_n),$$

dove l'ultimo termine va letto nel modo seguente:

$$\begin{array}{ll} \text{per } n = 2 & (F(\alpha_1))(\alpha_2) \\ \text{per } n = 3 & \left((F(\alpha_1))(\alpha_2) \right) (\alpha_3) \\ \text{per } n > 3 & \text{e così via} \end{array}$$

ESERCIZIO 9. Si mostri che

$$E = F(\alpha_1, \alpha_2, \dots, \alpha_n) = F(\alpha_{1\pi}, \alpha_{2\pi}, \dots, \alpha_{n\pi})$$

per ogni permutazione $\pi \in S_n$.

Si mostri che se gli α_i sono algebrici su F , allora ogni elemento di E si scrive come un polinomio negli α_i a coefficienti in F .

2.2. Esistenza

Cominciamo col mostrare l'*esistenza* del campo di spezzamento. Tutto si basa sul seguente

LEMMA 2.2.1. *Sia F un campo e f un polinomio monico non costante in $F[x]$.*

Allora esistono un anello commutativo B contenente F , e un elemento $\alpha \in B$ tali che f è il polinomio minimo di α su F .

Una volta trovato un B , non si perde niente a ridefinirlo come

$$B = F[\alpha] \cong F[x]/(f).$$

Con questa ridefinizione, si ha che B è un campo quando f è irriducibile su F , altrimenti non è neanche un dominio. Questo caso particolare è così importante, che tanto vale enunciarlo a parte:

LEMMA 2.2.2. *Sia F un campo e f un polinomio monico e irriducibile in $F[x]$. Allora esistono un campo K contenente F , e un elemento $\alpha \in K$ tali che f è il polinomio minimo di α su F .*

DIMOSTRAZIONE. Se B esiste, allora c'è un isomorfismo

$$\begin{aligned} F[x]/(f) &\rightarrow F[\alpha] \subseteq B \\ g + (f) &\mapsto g(\alpha) \end{aligned}$$

In particolare $x + (f) \mapsto \alpha$.

Allora prendiamo proprio $B = F[x]/(f)$, e $\alpha = x + (f)$. Abbiamo

$$f(\alpha) = f(x + (f)) = f(x) + (f(x)) = 0 + (f(x)).$$

Provare per credere! □

UN'ALTRA DIMOSTRAZIONE, PIÙ CONCRETA. Cominciamo col supporre che una simile estensione esista, e consideriamo $V = F[\alpha] \subseteq F$. Abbiamo visto che V è uno spazio vettoriale su F di dimensione n , ove n è il grado di f . Una base di V su F è data da

$$(2.2.1) \quad 1, \alpha, \alpha^2, \dots, \alpha^{n-1}.$$

La mappa

$$\begin{aligned} V &\rightarrow V \\ v &\mapsto v \cdot \alpha \end{aligned}$$

è una mappa lineare. La sua matrice rispetto alla base (2.2.1) è (i miei vettori sono vettori *riga*)

$$(2.2.2) \quad A = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & & & & \\ 0 & 0 & 0 & \dots & 1 \\ -a_0 & -a_1 & -a_2 & \dots & -a_{n-1} \end{bmatrix},$$

ove $f = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$. Infatti l'ultima riga di (2.2.2) corrisponde a

$$\alpha^{n-1} \cdot \alpha = \alpha^n = -a_0 - a_1\alpha - a_2\alpha^2 - \dots - a_{n-1}\alpha^{n-1}.$$

Ora notiamo che si può definire una mappa

$$\begin{aligned} F[\alpha] &\rightarrow \text{End}_F(F[\alpha]) \\ \beta &\mapsto (v \mapsto v \cdot \beta), \end{aligned}$$

e che questa mappa è un morfismo iniettivo, che manda α in A . Ne segue che $F[\alpha] \cong F[A]$.

A questo punto rivoltiamo la faccenda per costruire l'estensione E cercata. Consideriamo uno spazio vettoriale V di dimensione n su F , e fissiamone una base v_0, v_1, \dots, v_{n-1} . Sia A la matrice di (2.2.2). Affermo che A è l'elemento α cercato. Cominciamo a osservare che (2.2.2) significa

$$(2.2.3) \quad \begin{aligned} v_0 A &= v_1, v_1 A = v_2, \dots, v_{n-2} A = v_{n-1}, \\ v_{n-1} A &= -a_0 v_0 - a_1 v_1 - a_2 v_2 - \dots - a_{n-1} v_{n-1} \end{aligned}$$

La prima riga di (2.2.3) ci dice che V è un modulo *ciclico* rispetto ad A (per i dettagli si veda [Jac85]), cioè che partendo dal solo v_0 e applicando A ripetutamente si ottiene un sistema di generatori per V . Sia adesso $g \in F[x]$. Per verificare che $g(A) = 0$, cioè che $g(A)$ sia la mappa nulla su V , sarà sufficiente verificare che valga $v_0 g(A) = 0$. Infatti avremo allora

$$\begin{aligned} v_1 g(A) &= v_0 A g(A) = v_0 g(A) A = 0, \\ v_2 g(A) &= v_1 A g(A) = v_1 g(A) A = 0, \\ &\text{e così via,} \end{aligned}$$

dove abbiamo sfruttato il fatto che $A g(A) = g(A) A$.

Cominciamo allora col vedere che $v_0 f(A) = 0$. Infatti, applicando (2.2.3) si ottiene

$$\begin{aligned} v_0 f(A) &= v_0 (a_0 + a_1 A + \dots + a_{n-1} A^{n-1} + A^n) \\ &= a_0 v_0 + a_1 v_1 + \dots + a_{n-1} v_{n-1} + \\ &\quad - a_0 v_0 - a_1 v_1 - \dots - a_{n-1} v_{n-1} \\ &= 0. \end{aligned}$$

A questo punto saremmo a posto, per l'esercizio 1, dato che f è irriducibile. In realtà però f è il polinomio minimo di A anche se non è irriducibile. Infatti, se $g(x) = b_0 + b_1 x + \dots + b_{n-1} x^{n-1}$ è un polinomio di grado minore di n , grado di f , abbiamo

$$\begin{aligned} v_0 g(A) &= v_0 (b_0 + b_1 A + \dots + b_{n-1} A^{n-1}) \\ &= b_0 v_0 + b_1 v_1 + \dots + b_{n-1} v_{n-1}; \end{aligned}$$

dato che i v_i sono una base di V , questo può essere zero solo quando tutti i coefficienti b_i sono zero. Quindi f ha effettivamente grado minimo fra tutti i polinomi in A che si annullano su v_0 , e quindi su V .

Basta ora prendere $\alpha = A$ e $B = F[A]$.

ESERCIZIO 10. Sia f un polinomio monico di grado n sul campo F . Sia E un campo di spezzamento di f su F .

Si mostri che il grado $|E : F|$ divide $n!$

(*Suggerimento:* Procedere per induzione su n , distinguendo il caso f irriducibile dal caso f riducibile.)

Una volta in possesso del Lemma 2.2.2, è facile costruire un campo di spezzamento di un polinomio aggiungendo una per una le radici *dei suoi fattori irriducibili*. Si veda ad esempio [Jac85] per i dettagli.

2.3. Unicità

Più sottile è il discorso dell'unicità del campo di spezzamento, che ci porta alla teoria di Galois vera e propria. Il teorema sarebbe questo, ma ci interessano anche i dettagli della dimostrazione

TEOREMA 2.3.1 (Unicità). *Sia F un campo F , e $f \in F[x]$ un polinomio monico non costante. Siano E_1 e E_2 due campi di spezzamento di f su F . Allora esiste un isomorfismo da E_1 a E_2 su F .*

Con isomorfismo da E_1 a E_2 su F si intende un isomorfismo da $\varphi : E_1 \rightarrow E_2$ tale che $a\varphi = a$ per ogni $a \in F$. Notate infatti che per definizione F è contenuto sia in E_1 che in E_2 , e quindi ci può venire il dubbio su cosa succeda ai suoi elementi sotto φ .

Notate anche che gli isomorfismi (di anelli) di cui sopra sono anche isomorfismi di spazi vettoriali. C'è solo da controllare che si tratti di mappe lineari: se $u, v \in E_1$ e $a, b \in F$, abbiamo

$$(au + bv)\varphi = a\varphi \cdot u\varphi + b\varphi \cdot v\varphi = a(u\varphi) + b(v\varphi).$$

Questi isomorfismi sono l'ingrediente base della teoria di Galois, e nel corso della dimostrazione ci interessa anche *contarli*, cioè vedere quanti sono.

Cominciamo col richiamare un semplice

LEMMA 2.3.2. *Sia F un campo, $f \in F[x]$ monico e irriducibile. Allora gli unici ideali che contengano (f) sono (f) stesso e tutto $F[x]$.*

DIMOSTRAZIONE. $F[x]$ è un dominio a ideali principali, dunque ogni ideale è della forma (g) , per qualche $g \in F[x]$. Se $(g) \supseteq (f)$, si ha $g \mid f$. Dato che f è irriducibile, a meno di elementi invertibili si ha o $g = f$, e dunque $(g) = (f)$, o $g = 1$, e dunque $(g) = F[x]$. \square

Il primo passo è il seguente Lemma, in cui introduciamo anche uno strumento molto utile.

LEMMA 2.3.3. *Siano F e \overline{F} due campi.*

Sia $\bar{\cdot} : F \rightarrow \overline{F}$ un isomorfismo. Esso si estende a un ovvio isomorfismo (che continuiamo a chiamare con lo stesso nome) $\bar{\cdot} : F[x] \rightarrow \overline{F}[x]$, quello che manda

$$\begin{aligned} f = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n &\mapsto \\ \mapsto \bar{f} = \bar{a}_0 + \bar{a}_1x + \cdots + \bar{a}_{n-1}x^{n-1} + x^n. \end{aligned}$$

Sia $f \in F[x]$ un polinomio monico e irriducibile, e $\bar{f} \in \overline{F}[x]$ il polinomio corrispondente.

Sia K_1 una estensione di F , e K_2 una estensione di \overline{F} . Supponiamo ci sia una radice α_1 di f in K_1 , e una radice α_2 di \bar{f} in K_2 .

Allora esiste un unico isomorfismo

$$\varphi : F[\alpha_1] \rightarrow \overline{F}[\alpha_2]$$

tale che

1. φ manda α_1 in α_2
2. φ ristretto a F induce $\overline{\cdot}$

DIMOSTRAZIONE. L'idea è che abbiamo i morfismi

$$\begin{array}{ccc} F[\alpha_1] & & \overline{F}[\alpha_2] \\ g_1 \uparrow & & \uparrow g_2 \\ F[x]/(f) & & \overline{F}[x]/(\overline{f}) \\ \pi_f \uparrow & & \uparrow \pi_{\overline{f}} \\ F[x] & \xrightarrow{\quad \quad} & \overline{F}[x] \\ & & \overline{\cdot} \end{array}$$

Qui i g_i sono gli isomorfismi dati dai teoremi di struttura delle estensioni semplici $F[\alpha_1]$ e $\overline{F}[\alpha_2]$, e i π_i sono gli omomorfismi canonici. Consideriamo il morfismo composto (le mappe le scriviamo a destra, come si è già visto)

$$\vartheta = \overline{\cdot} \circ \pi_{\overline{f}} : F[x] \rightarrow \overline{F}[x]/(\overline{f})$$

Esso è evidentemente suriettivo, e ha nel nucleo f . Dunque $\ker(\vartheta)$ è un ideale contenente (f) . Per il Lemma 2.3.2, ci sono due possibilità. Una è $\ker(\vartheta) = F[x]$, cioè ϑ manda ogni elemento di $F[x]$ in zero. Ma $1\vartheta = 1\overline{\cdot} \circ \pi_{\overline{f}} = \overline{1}\pi_{\overline{f}} = \overline{1} + (\overline{f}) \neq 0$, dunque questo è impossibile. Allora vuol dire che $\ker(\vartheta) = (f)$: il primo teorema di isomorfismo ci fornisce un isomorfismo

$$\begin{aligned} \eta : F[x]/(f) &\rightarrow \overline{F}[x]/(\overline{f}) \\ h + (f) &\mapsto \overline{h} + (\overline{f}). \end{aligned}$$

Ora abbiamo isomorfismi

$$\begin{array}{ccc} F[\alpha_1] & & \overline{F}[\alpha_2] \\ g_1 \uparrow & & \uparrow g_2 \\ F[x]/(f) & \xrightarrow{\quad \quad \eta \quad} & \overline{F}[x]/(\overline{f}) \end{array}$$

e l'isomorfismo cercato sarà $g_1^{-1} \circ \eta \circ g_2$. In altre parole, l'isomorfismo ottenuto agisce come $\overline{\cdot}$ sugli elementi di F , e manda α_1 in α_2 . (Se serve si possono dare ulteriori dettagli.) \square

A questo punto possiamo dimostrare l'unicità. Passeremo attraverso un risultato che, a differenza del Teorema 2.3.1, si presta all'induzione.

PROPOSIZIONE 2.3.4. *Siano F e \overline{F} due campi.*

Sia $\overline{\cdot} : F \rightarrow \overline{F}$ un isomorfismo, e indichiamo ancora con $\overline{\cdot} : F[x] \rightarrow \overline{F}[x]$ la sua estensione agli anelli di polinomi.

Sia $f \in F[x]$ un polinomio monico non costante, e $\bar{f} \in \bar{F}[x]$ il polinomio corrispondente.

Sia E_1 un campo di spezzamento di f su F , e E_2 un campo di spezzamento di \bar{f} su \bar{F} .

Allora esiste un isomorfismo da E_1 a E_2 che ristretto a F induce $\bar{\cdot}$.

DIMOSTRAZIONE. La dimostrazione è facile, una volta che si ha il Lemma 2.3.3. Si procede per induzione sul grado $|E_1 : F|$. Se questo è 1, ovvero f ha tutte le sue radici già in F , non c'è niente da dire. Altrimenti f non ha tutte le sue radici in F , e dunque ha un fattore irriducibile g di grado $m > 1$.

Sia α_1 una radice di g in E_1 , e sia $\alpha_2 \in E_2$ una qualsiasi radice del polinomio \bar{g} corrispondente. Per il Lemma 2.3.3, possiamo estendere $\bar{\cdot}$ a un isomorfismo $\vartheta : F[\alpha_1] \rightarrow \bar{F}[\alpha_2]$. Ora E_1 è ancora un campo di spezzamento di f su $F[\alpha_1]$, e E_2 è un campo di spezzamento di \bar{f} su $\bar{F}[\alpha_2]$. Dato che $|F[\alpha_1] : F| = \text{grado}(g) = m > 1$, si avrà

$$|E_1 : F[\alpha_1]| < |E_1 : F|,$$

e possiamo quindi concludere per induzione. \square

Il Teorema 2.3.1 si ottiene ora ponendo $F = \bar{F}$, e $\bar{\cdot}$ eguale alla mappa identica.

2.4. Quanti isomorfismi?

E' interessante andare a vedere *quanti* isomorfismi diversi si possano ottenere attraverso la Proposizione 2.3.4. Parlando a braccio (l'argomento completo, più formale, si trova più sotto, nella Proposizione 2.4.1), quando dobbiamo selezionare α_2 , possiamo scegliere qualsiasi radice del polinomio irriducibile $\bar{g} \in \bar{F}[x]$, e otterremo un diverso isomorfismo, dato che stiamo scegliendo immagini diverse per il fissato elemento α_1 . Supponiamo che \bar{g} abbia $m = \text{grado}(g) = \text{grado}(\bar{g})$ radici distinte in E_2 . Allora le scelte possibili sono m . Quindi abbiamo m scelte, e nel passaggio dall'estensione E/F all'estensione $E/F[\alpha_1]$ il grado si divide per m .

Se questo avviene per ogni polinomio g che compare della dimostrazione, otteniamo quindi alla fine tanti isomorfismi quant'è il grado $|E_1 : F|$. Una condizione che garantisce che ogni g abbia radici distinte è naturalmente che f abbia radici distinte. In realtà basta meno, basta cioè supporre che i fattori irriducibili di f in $F[x]$ abbiano radici distinte. (Più avanti diremo che un polinomio con tale proprietà è *separabile*.) Infatti i polinomi g sono fattori di f , e sono irriducibili in $K[x]$, per qualche estensione K/F . Sfruttiamo allora il seguente

ESERCIZIO 11. Sia $f \in F[x]$. Sia K/F una estensione, e sia $g \in K[x]$ un polinomio che divide f , ed è irriducibile in $K[x]$.

Allora esiste un fattore irriducibile h di f in $F[x]$ tale che g divide h .

SUGGERIMENTO. Si scriva la fattorizzazione $f = f_1 \cdot f_2 \cdot \dots \cdot f_n$ di f in fattori irriducibili in $F[x]$. Ora g divide f , ed è irriducibile in $K[x]$. Dunque deve dividere uno dei fattori f_i . \square

Dunque se ogni fattore irriducibile di f in $F[x]$ ha radici distinte, lo stesso vale per ogni fattore irriducibile di f su qualsiasi estensione K/F .

Ecco come enunciare in modo formale il ragionamento solo accennato nelle Note sul conteggio degli isomorfismi fra due campi di spezzamento (ed in particolare degli automorfismi di un campo di spezzamento).

PROPOSIZIONE 2.4.1. *Nella situazione della Proposizione 2.3.4, il numero degli isomorfismi da E_1 a E_2 che estendono $\bar{\tau}$ è al più $|E : F|$, e se \bar{f} ha radici distinte in E_2 vale l'uguaglianza.*

Prendendo $\bar{F} = F$, $\bar{\tau}$ la mappa identica, ed $E_1 = E_2$, otteniamo come corollario che: se E è un campo di spezzamento su F di un polinomio f , allora $|\text{Gal}(E/F)| \leq |E : F|$ (notazione introdotta nel Capitolo 3), e se f ha radici distinte in E (o, più in generale, se f è separabile, vedi più sotto) vale l'uguaglianza.

In realtà di tutto ciò la sola cosa che useremo in seguito sarà il caso in cui f ha radici distinte, ed anzi in questo caso ci servirà solo la disuguaglianza $|\text{Gal}(E/F)| \geq |E : F|$ se f ha radici distinte; la disuguaglianza in senso contrario è infatti soddisfatta per qualunque estensione E/F , come vedremo nel Lemma 3.8.1 (vedi il ragionamento dopo la Proposizione 3.15.1). Comunque non ci costerà molto mostrare subito entrambi i versi, basterà avere l'accortezza seguente: dovremo non solo contare il numero degli isomorfismi che riusciamo a costruire “un pezzo alla volta”, ma dovremo anche assicurarci che tutti i possibili isomorfismi si ottengano con la nostra ricetta.

DIMOSTRAZIONE. Anzitutto, nelle ipotesi del Lemma 2.3.3, se $\varphi : F[\alpha_1] \rightarrow K_2$ è un monomorfismo che estende $\bar{\tau}$, allora $\alpha_1\varphi$ deve essere per forza una radice di \bar{f} , perché $\bar{f}(\alpha_1\varphi) = f(\alpha_1)\varphi = 0$ (vedi anche il Lemma 3.1.1). Dunque tali possibili monomorfismi sono tutti come descritti nel Lemma, e pertanto sono in numero pari al numero di radici distinte di \bar{f} in K_2 .

Nella situazione della Dimostrazione della Proposizione 2.3.4, le scelte per α_2 saranno esattamente le radici di \bar{g} , quindi in numero pari al numero di radici distinte di \bar{g} in E_2 , pertanto al più $m = \text{grado}(g)$. Inoltre, la restrizione ad $F[\alpha_1]$ di qualsiasi isomorfismo da E_1 a E_2 che estende $\bar{\tau}$ è un monomorfismo da $F[\alpha_1]$ a E_2 che estende $\bar{\tau}$, e quindi coincide con una delle estensioni ϑ considerate, per quanto osservato all'inizio. D'altra parte, per ipotesi induttiva, ciascuna di queste estensioni ϑ estende a sua volta in al più $|E_1 : F[\alpha_1]|$ modi ad un isomorfismo da E_1 a E_2 , e quindi complessivamente avrò al più $m \cdot |E_1 : F[\alpha_1]| = |E_1 : F|$ possibili isomorfismi da E_1 a E_2 che estendono $\bar{\tau}$.

Se poi \bar{f} ha radici distinte in E_2 anche il suo fattore \bar{g} avrà radici distinte, e di nuovo per ipotesi induttiva avrò che gli isomorfismi sono esattamente $|E_1 : F|$. \square

In realtà, come accennato nelle Note, per concludere che vale l'uguaglianza è sufficiente che tutti i fattori irriducibili di f in $F[x]$ abbiano radici distinte (cioè che f sia *separabile*); infatti il campo di spezzamento di f coincide con quello del polinomio prodotto dei fattori irriducibili *distinti* di f , e quest'ultimo ha radici distinte, se f è separabile. (Questo ragionamento può rimpiazzare l'uso dell'Esercizio 11.)

CAPITOLO 3

Corrispondenza di Galois

3.1. Il gruppo di Galois

Definiamo

$$(3.1.1) \quad \text{Gal}(E/F) = \{ \varphi : E \rightarrow E : \varphi \text{ è un isomorfismo,} \\ a\varphi = a \text{ per ogni } a \in F \}.$$

$\text{Gal}(E/F)$ è detto il *gruppo di Galois* dell'estensione.

ESERCIZIO 12. Si verifichi che $\text{Gal}(E/F)$ è effettivamente un gruppo.

È utile notare che nel caso particolare della Proposizione 2.3.4 in cui $F = \overline{F}$, τ è la mappa identica, e $E_1 = E_2 = E$ è un fissato campo di spezzamento di f su F , allora gli isomorfismi considerati sono in questo caso gli isomorfismi di E in se stesso (detti anche *automorfismi* di E) che fissano ogni elemento di F , cioè proprio gli elementi del gruppo di Galois.

Vediamo subito un esempio in cui il gruppo di Galois è banale. Prendiamo $F = \mathbf{Q}$, e $E = \mathbf{Q}[\sqrt[3]{2}]$. Dato che il polinomio minimo di $\sqrt[3]{2}$ su \mathbf{Q} è $x^3 - 2$, ogni elemento di E si scrive in modo unico come

$$a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{2}^2 \quad a_i \in \mathbf{Q},$$

e $|E : F| = 3$. Sia adesso φ un elemento di $\text{Gal}(E/F)$. Dato che φ è un morfismo, e fissa gli elementi di \mathbf{Q} , abbiamo

$$(a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{2}^2)\varphi = a_0 + a_1(\sqrt[3]{2}\varphi) + a_2(\sqrt[3]{2}\varphi)^2.$$

Dunque φ è determinato dal valore $\sqrt[3]{2}\varphi$. Ora abbiamo $(\sqrt[3]{2}\varphi)^3 - 2 = 0$. Applicando φ abbiamo

$$(\sqrt[3]{2}\varphi)^3 - 2 = 0,$$

cioè $\sqrt[3]{2}\varphi \in E$ è ancora una radice di $x^3 - 2$. Ma le radici di questo polinomio sono

$$\sqrt[3]{2}, \quad \sqrt[3]{2} \cdot \left(\frac{-1 - i\sqrt{3}}{2} \right), \quad \sqrt[3]{2} \cdot \left(\frac{-1 + i\sqrt{3}}{2} \right),$$

ove i due numeri complessi sono le due radici terze dell'unità diverse da 1, ovvero le radici di $x^2 + x + 1 = (x^3 - 1)/(x - 1)$. Delle tre radici, solo la prima è reale, e quindi le altre due non stanno in $E \subseteq \mathbf{R}$. La morale è che l'unica scelta possibile per $\sqrt[3]{2}\varphi$ è $\sqrt[3]{2}$, e dunque l'unica scelta possibile per φ è la mappa identica. Dunque $\text{Gal}(E/F)$ ha un unico elemento, mentre il grado $|E : F|$ è 3.

Più in generale, abbiamo visto nell'Esercizio 9 che ogni elemento di $E = F(\alpha_1, \dots, \alpha_n)$ è un polinomio negli α_i . Ne segue che un elemento di $\text{Gal}(E/F)$ è determinato dalla sua azione su $\alpha_1, \dots, \alpha_n$, e che l'immagine sotto φ di α_i deve essere una radice del polinomio minimo di α_i su F che sia contenuta in E .

In altre parole

LEMMA 3.1.1. *Sia E/F una estensione, $f \in F[x]$ un polinomio monico e irriducibile. Sia $\alpha \in E$ una radice di F . Dunque f è il polinomio minimo di α su F .*

Sia $\varphi : E \rightarrow E$ un isomorfismo che ristretto a F induca la mappa identica.

Allora l'immagine $\alpha\varphi$ di α sotto φ è ancora una radice di f .

In realtà il risultato vale anche se f non è irriducibile, ma vogliamo sottolineare il fatto che tanto φ non può mandare α in nient'altro che altre radici del suo polinomio minimo.

DIMOSTRAZIONE. Facile: scriviamo esplicitamente

$$f = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + x^n,$$

con $a_i \in F$. Abbiamo

$$0 = f(\alpha) = a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} + \alpha^n.$$

Applichiamo φ , tenendo presente che è un morfismo, e che $a\varphi = a$ per ogni $a \in F$, ottenendo proprio

$$0 = a_0 + a_1(\alpha\varphi) + \dots + a_{n-1}(\alpha\varphi)^{n-1} + (\alpha\varphi)^n = f(\alpha\varphi).$$

□

ESERCIZIO 13 (Vedi sotto (e la lezione) per i dettagli).

Costruire i campi di spezzamento E_1 di $(x^2 - 2)(x^2 - 3)$ su \mathbf{Q} e E_2 di $x^3 - 2$ su \mathbf{Q} . Si tratta quindi di estensioni normali.

Si calcolino i gruppi di Galois $\text{Gal}(E_i/\mathbf{Q})$, si costruiscano tutti i sottogruppi e campi intermedi, e si determini esplicitamente la corrispondenza di Galois.

Se $E = F(\alpha_1, \dots, \alpha_n)$, allora ogni elemento di $\text{Gal}(E/F)$ è determinato dalla sua azione su $\alpha_1, \dots, \alpha_n$. Per vederlo, anziché sfruttare l'Esercizio 9 (che dice che ogni elemento di E è un "polinomio" in $\alpha_1, \dots, \alpha_n$), si può anche ragionare nel modo seguente. Se φ e ψ sono due elementi di $\text{Gal}(E/F)$ tali che $\alpha_j\varphi = \alpha_j\psi$ per ogni j , allora l'automorfismo composto (letto da sinistra verso destra) $\varphi\psi^{-1}$ fissa ciascun α_j (e gli elementi di F). Si vede immediatamente che in generale l'insieme degli elementi fissati (cioè mandati in se stessi) da un automorfismo di un anello (risp. campo) è un sottoanello (risp. sottocampo). Nel nostro caso tale sottocampo degli elementi fissati da $\varphi\psi^{-1}$ contiene F e gli α_i , dunque coincide con l'intero E , e quindi $\varphi = \psi$.

Nell'esercizio 13, per dimostrare direttamente (cioè senza usare il Teorema fondamentale della Teoria di Galois, Teorema 3.13.3, che non abbiamo ancora a disposizione) che i campi intermedi fra \mathbf{Q} e il campo di spezzamento E_1 di $(x^2 - 2)(x^2 - 3)$ su \mathbf{Q} sono solo quelli che uno si aspetta (cioè quelli ottenuti come *primo* di sottogruppi del gruppo di Galois), bisogna prima esprimere E_1 come generato

su \mathbf{Q} da un singolo elemento (detto un'elemento primitivo dell'estensione), ad esempio $\sqrt{2} + \sqrt{3}$, e poi svolgere il ragionamento visto a lezione.

Generalizzando dall'esempio particolare, possiamo formalizzare la conclusione di quel ragionamento nella seguente proposizione.

PROPOSIZIONE 3.1.2. *Se $E = F[\alpha]$ per qualche α con polinomio minimo $g(x)$ su F , allora qualsiasi campo intermedio dell'estensione E/F è generato su F dai coefficienti di un opportuno fattore di $g(x)$ (in $E[x]$).*

In particolare, concludiamo che se un'estensione di grado finito E/F ha un elemento primitivo, (il che risulterà essere sempre vero per estensioni (di grado finito) separabili, ad esempio in caratteristica zero,) i campi intermedi sono in numero finito. (E sono al più 2^{n-1} , se n è il grado di $g(x)$, tenendo conto che i coefficienti di un fattore $h(x)$ di $g(x)$ generano lo stesso sottocampo dei coefficienti di $g(x)/h(x)$; è una stima molto rozza.) Nel caso speciale di estensioni normali di grado finito, questo sarà anche una conseguenza immediata del Teorema fondamentale della Teoria di Galois, Teorema 3.13.3 (perché i campi intermedi saranno in corrispondenza biunivoca con i sottogruppi del gruppo di Galois, finito). (Ed infatti il gruppo di Galois G , avendo ordine n , ha al più 2^{n-1} sottogruppi, essendo questo il numero di sottoinsiemi di G che contengono 1; come nel caso dei campi, anche questa è una stima molto rozza).

In modo analogo, sempre nell'Esercizio 13, per dimostrare (sempre senza usare il Teorema fondamentale della Teoria di Galois) che i sottocampi del campo $E = \mathbf{Q}[\sqrt[3]{2}, \omega]$, dove $\omega = (-1 + \sqrt{-3})/2$, che è il campo di spezzamento di $x^3 - 2$ su \mathbf{Q} , sono solo quelli ottenuti come punti fissi di qualche automorfismo di E/\mathbf{Q} , bisogna anzitutto esprimere E come un'estensione semplice $E = \mathbf{Q}[\alpha]$, ad esempio prendendo $\alpha = \omega\sqrt[3]{2} - \bar{\omega}\sqrt[3]{2} = \sqrt{-3}\sqrt[3]{2}$, che ha polinomio minimo $x^6 + 27 \cdot 4$ su \mathbf{Q} . Infatti si verifica che tale α non è fissato da alcun elemento del gruppo di Galois, e quindi, se ci fidiamo di ciò che vogliamo dimostrare, non dovrebbe appartenere ad alcun sottocampo proprio di E , e quindi dovrebbe generare E su \mathbf{Q} , e perciò avere polinomio minimo di grado 6. Ma poiché non è permesso usare la tesi per dimostrare la stessa (anche se è permesso, anzi spesso importante, usarla per orientarsi), propongo il seguente

ESERCIZIO. Dimostrare che il polinomio $x^6 + 27 \cdot 4$ è irriducibile su \mathbf{Q} (o, equivalentemente, che $\alpha = \sqrt{-3}\sqrt[3]{2}$ ha grado 6 su \mathbf{Q}). (*Suggerimento:* Anzitutto verificate che $\mathbf{Q}[\alpha]$ contiene $\mathbf{Q}[\omega]$. Poi trovate il polinomio minimo (e quindi il grado) di α su $\mathbf{Q}[\omega]$).

Una volta svolto l'esercizio, per concludere che i campi intermedi sono solo quelli trovati, basta applicare la Proposizione appena vista a tutte le fattorizzazioni di $x^6 + 27 \cdot 4$, il che è certo fattibile ma sicuramente molto lungo. Accetto da voi suggerimenti su come semplificare/sistematizzare questa verifica.

3.2. La corrispondenza di Galois

Sia E/F una qualsiasi estensione di campi. (Potrebbe ben essere di grado infinito, o non algebrica.) Sia $G = \text{Gal}(E/F)$ il gruppo di Galois. Consideriamo

l'insieme \mathcal{H} dei sottogruppi di G , e l'insieme \mathcal{L} dei campi L cosiddetti intermedi, $F \subseteq L \subseteq E$. Definiremo due mappe con lo stesso nome “primo”, una da \mathcal{H} a \mathcal{L} , e una viceversa da \mathcal{L} a \mathcal{H} .

La mappa $' : \mathcal{H} \rightarrow \mathcal{L}$ è definita, così, per $H \in \mathcal{H}$,

$$(3.2.1) \quad H' = \{ a \in E : ah = a \text{ per ogni } h \in H \}.$$

Cioè H' consiste degli elementi di F che sono fissati da ogni elemento di H . E' facile, ma istruttivo, vedere che H' sia in effetti un sottocampo di E . Notate che ogni elemento di G fissa ogni elemento di F , per la definizione (3.1.1) di $G = \text{Gal}(E/F)$, e dunque ogni elemento di $H \leq G$ fa altrettanto. Dunque $H' \supseteq F$, e quindi $H' \in \mathcal{L}$.

Viceversa la mappa $' : \mathcal{L} \rightarrow \mathcal{H}$ è definita, per $L \in \mathcal{L}$, mediante

$$(3.2.2) \quad L' = \{ g \in G : ag = a \text{ per ogni } a \in L \}.$$

Qui L' è quindi l'insieme degli elementi di G che fissano ogni elementi di L . Di nuovo, sarebbe facile verificare che L' è un sottogruppo di G , ma se si è fatto già l'Esercizio 12, basta notare il fatto (comunque utile)

$$L' = \text{Gal}(E/L).$$

Cominciamo col vedere che succede ad applicare il “primo” agli oggetti E , F , $\{1\}$ e G , ove $\{1\}$ è il sottogruppo di G consistente del solo elemento neutro 1, ovvero della mappa identica su E .

Si ha $E' = \{ g \in G : ag = a \text{ per ogni } a \in E \} = \{1\}$. dato che gli elementi di G sono automorfismi di E , ovvero mappe da E ad E , e l'unica mappa che fissi tutti gli elementi di E è proprio la mappa identica.

Sia ha poi $F' = \{ g \in G : ag = a \text{ per ogni } a \in F \} = G$, dato che per la definizione (3.1.1) tutti gli elementi di G fissano tutti gli elementi di F .

Ancora, si ha immediatamente $\{1\}' = \{ a \in E : a1 = a \} = E$.

Invece quando si considera $G' = \{ a \in E : ag = a \text{ per ogni } g \in G \}$ abbiamo un problema. Per completezza ci si aspetterebbe $G' = F$. Ma mentre è chiaro che $G' \supseteq F$, dato che ogni elemento di G fissa ogni elemento di F , per la solita definizione (3.1.1), ma nell'esempio $F = \mathbf{Q}$, $E = \mathbf{Q}(\sqrt[3]{2})$ si ha $G = \text{Gal}(E/F) = \{1\}$, e dunque $G' = \{1\}' = E \neq F$.

Talvolta H' (ad esempio in [Jac85]) è indicato con $\text{Inv}(H)$; la notazione, di uso più generale, sta a significare che si tratta dell'insieme dei punti *fissi* sotto l'azione di H .

Notate anche che L' è l'insieme degli automorfismi di E che estendono l'identità su L , e quindi è semplicemente $\text{Gal}(E/L)$.

3.3. Gruppo di Galois e gruppo simmetrico

Finiamo l'esercizio 13, calcolando $\text{Gal}(\mathbf{Q}(\sqrt[3]{2}, \omega)/\mathbf{Q})$, ove $\omega^2 + \omega + 1 = 0$. Questo è il campo di spezzamento su \mathbf{Q} di $x^3 - 2$. Fra le altre cose, si nota che il gruppo di Galois viene rappresentato come gruppo di permutazioni sulle radici di $x^3 - 2$, e dunque il gruppo in questo caso viene isomorfo a S_3 . Prefiguriamo quindi il seguente argomento generale.

Sia F un campo, $f \in F[x]$ monico e non costante. Sia E il campo di spezzamento di f su F , sia $G = \text{Gal}(E/F)$, e sia $\Omega = \{\alpha_1, \dots, \alpha_n\}$ le radici di f in E . Per il Lemma 3.1.1, ogni elemento di G manda elementi di Ω in elementi di Ω . E' dunque definita una mappa

$$\begin{aligned} \varphi : G &\rightarrow S(\Omega) \\ g &\mapsto (\alpha \rightarrow \alpha g). \end{aligned}$$

Qui $S(\Omega)$ è il gruppo delle permutazioni sull'insieme Ω . Per la parte finale dell'Esercizio 9, ogni elemento di E si scrive come una espressione polinomiale negli α_i . Dunque un elemento di G è determinato dalla sua azione sugli α_i . In altre parole la mappa φ è iniettiva. Abbiamo dunque ottenuto

PROPOSIZIONE 3.3.1. *Il gruppo di Galois di un campo di spezzamento è isomorfo a un gruppo di permutazioni sull'insieme delle radici.*

3.4. Estensioni normali

Sia E/F una estensione, $G = \text{Gal}(E/F)$, e consideriamo la corrispondenza di Galois. Sia L un campo intermedio. Ricordiamo che $L' = \text{Gal}(E/L)$.

Ora, la condizione che $G' = F$ è proprio cruciale. Introduciamo la seguente definizione.

DEFINIZIONE 3.4.1. *L'estensione E/F si dice normale (o si dice anche che E è normale su F) quando vale $\text{Gal}(E/F)' = F$.*

A parole (la prima volta fa girare un po' la testa), un'estensione E/F è normale quando i soli elementi di E , che siano fissati da tutti gli automorfismi di E che fissano tutti gli elementi di F , sono proprio gli elementi di F . In generale potrebbero essercene di più, come mostra l'esempio appena visto di $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$.

Daremo tra poco due risultati di base che ci permetteranno di comprendere bene la struttura delle estensioni normali. Cominciamo con alcune osservazioni elementari, ma che la prima volta richiedono un po' di riflessione. Siano $H \leq K \leq G$ due sottogruppi di G uno dentro l'altro. Allora $H' \supseteq K'$. Infatti ogni elemento di E che sia fissato da ogni elemento di K è in particolare fissato da ogni elemento di $H \leq K$. Similmente (istruttivo esercizio) se $F \subseteq L \subseteq M \subseteq E$, allora $L' \supseteq M'$. Non è poi difficile (ma ancora istruttivo) vedere che

$$(3.4.1) \quad X'' \supseteq X \quad \text{se } X \in \mathcal{H}, \text{ o } X \in \mathcal{L}.$$

A questo punto possiamo fare un'osservazione del tutto formale. Applicando di nuovo il primo abbiamo $X''' \subseteq X'$. D'altra parte applicando (3.4.1) con X' al posto di X otteniamo $X''' \supseteq X'$, e dunque $X''' = X'$.

Notiamo

LEMMA 3.4.2. *Qualunque sia l'estensione E/F , allora l'estensione E/F'' è normale, e $\text{Gal}(E/F'') = \text{Gal}(E/F)$.*

DIMOSTRAZIONE. Dato che $F \subseteq F''$, si ha $\text{Gal}(E/F'') \leq \text{Gal}(E/F)$. D'altra parte ogni F'' è proprio l'insieme degli elementi di E fissato da ogni elemento di

$F' = \text{Gal}(E/F)$, dunque $\text{Gal}(E/F'') \geq \text{Gal}(E/F)$, e i due gruppi coincidono. Poi F'' è chiuso per definizione. \square

Questo lemma fornisce un modo, che utilizzeremo più avanti, per *rimediare* alla non normalità di certe estensioni. Naturalmente il risultato può essere deludente, ad esempio se si parte da $F = \mathbf{Q}$ e $E = \mathbf{Q}(\sqrt[3]{2})$, si ottiene $F'' = \mathbf{Q}(\sqrt[3]{2})$, e banalmente l'estensione E/E è normale. Vedremo che c'è una ricetta ben più intelligente per passare da una estensione non normale a una normale, quando possibile.

3.5. Un commento sul concetto di estensione normale

Su vari testi, (ad esempio [Jac85]) *normale* ha un significato più debole di quello usato qui. La nostra definizione di *normale* corrisponde a quello che altrove viene detto *estensione di Galois*. Ad esempio, [Jac85] chiama *normale* un'estensione E/F se ogni polinomio irriducibile in $F(x)$ che abbia una radice in E è un prodotto di fattori lineari in $E(x)$ (cioè ha “tutte” le sue radici in E , che è la seconda delle condizioni equivalenti del Lemma 5.1.1), e la chiama *separabile* se il polinomio minimo su F di ogni elemento di E è separabile (cioè ha radici distinte in E); un'estensione risulta essere *di Galois* (cioè *normale* nel nostro senso) se e solo se è *normale e separabile* nel senso di [Jac85]. (Per estensioni di grado finito ciò segue mettendo insieme il Teorema 4.2.1 ed il Lemma 5.1.1 delle Note.) La dicitura *estensione di Galois* sarebbe forse quella preferibile, visto che ha un significato univoco, comunque in questo corso la chiameremo *estensione normale*, come dalla Definizione 3.4.1 (e come in [Kap95]).

In caratteristica zero non fa comunque differenza, visto che la separabilità è automatica in quel caso.

3.6. Sottogruppi e campi intermedi chiusi

Introduciamo ora una terminologia di sapore topologico; per ora è solo una questione di parole, ma vedremo verso la fine del corso che corrisponde veramente a questioni topologiche. Diciamo che $X \in \mathcal{H} \cup \mathcal{L}$ è *chiuso* nella corrispondenza di Galois se $X'' = X$. Dunque se X è chiuso si ha $X = (X)'$, cioè X è il primo di qualcosa. Viceversa, se $X = Y'$ per qualche Y , otteniamo $X'' = Y''' = Y' = X$, e quindi X è chiuso. Quindi essere chiuso vuol dire esattamente essere il primo di qualcosa.

X'' viene detto la *chiusura* di X . In effetti X'' è chiuso, ed è il minimo oggetto chiuso che contenga X . Infatti se Y è chiuso, e $X \subseteq Y$, allora $X'' \subseteq Y'' = Y$.

Notiamo ancora che dire che F è chiuso significa $F = F'' = G'$, cioè che E/F è normale.

Enunciamo adesso un primo risultato sulla *corrispondenza di Galois* fra sottogruppi e campi intermedi. Per ora si tratta di un risultato povero di significato, finché non abbiamo criteri per decidere quanti e quali oggetti siano chiusi.

TEOREMA 3.6.1 (Corrispondenza di Galois I). *Sia E/F una estensione, e sia $G = \text{Gal}(E/F)$ il suo gruppo di Galois.*

Allora le operazioni “primo” stabiliscono una corrispondenza biunivoca fra gli oggetti chiusi di \mathcal{H} e \mathcal{L} .

La dimostrazione l’abbiamo in realtà già vista. Infatti il primo di qualsiasi cosa è un oggetto chiuso, e per un oggetto chiuso X vale $X = X''$, cioè le due mappe primo sono una l’inversa dell’altra.

Lo strumento fondamentale per individuare oggetti chiusi sono due Lemmi, che forniscono due disequaglianze chiave.

3.7. Corrispondenze di Galois più generali

La *corrispondenza di Galois* fra campi e loro gruppi di automorfismi, nata naturalmente con la teoria di Galois, è uno di vari esempi di corrispondenze fra due insiemi parzialmente ordinati, spesso chiamate anch’esse *corrispondenze di Galois*: basta avere due insiemi parzialmente ordinati \mathcal{A} e \mathcal{B} e due mappe *primo* da \mathcal{A} a \mathcal{B} e viceversa, con le proprietà che $X \supseteq Y$ implica $X' \subseteq Y'$ per $X, Y \in \mathcal{A} \cup \mathcal{B}$, e vale $X \subseteq X''$ per $X \in \mathcal{A} \cup \mathcal{B}$, per poterne dedurre formalmente che $X''' = X$, e quindi che le due mappe *primo* danno una biiezione e la sua inversa fra gli elementi *chiusi* (cioè tali che $X' = X$) di \mathcal{A} e quelli di \mathcal{B} .

Un esempio è la mappa che associa ad un sottogruppo (risp. sottoanello, sottoalgebra) di un gruppo (anello, algebra (associativa, di Lie o altro)) il suo centralizzante nell’intero gruppo (risp...). Come sopra segue del tutto formalmente che un sottogruppo che sia il centralizzante di un altro è *chiuso* nella corrispondenza, cioè eguaglia il suo *doppio centralizzante*.

Un altro esempio importante è in geometria algebrica, e riguarda la corrispondenza fra sottovarietà di una varietà algebrica e certi ideali nell’algebra delle funzioni *polinomiali* sulla varietà. Nel caso più semplice, $\mathcal{A} = \{\text{sottoinsiemi di } \mathbf{C}^n\}$, $\mathcal{B} = \{\text{sottoinsiemi di } \mathbf{C}[x_1, \dots, x_n]\}$, entrambi parzialmente ordinati per inclusione, la mappa *primo* associa ad ogni sottoinsieme A di \mathbf{C}^n l’insieme I (che poi è un ideale di $\mathbf{C}[x_1, \dots, x_n]$) dei polinomi in x_1, \dots, x_n che si annullano su ogni punto di V , e ad ogni insieme B di polinomi in $\mathbf{C}[x_1, \dots, x_n]$ l’insieme dei loro zeri comuni. Ne è indotta una biiezione fra i chiusi di \mathcal{A} , che sono le varietà affini in \mathbf{C}^n , ed i chiusi di \mathcal{B} , che sono gli ideali *radicali* di $\mathbf{C}[x_1, \dots, x_n]$ (Nullstellensatz di Hilbert).

Un altro esempio è in uno spazio vettoriale (di dimensione finita) dotato di prodotto scalare, dove la mappa “primo” manda un sottoinsieme nel suo (sottospazio) ortogonale (se il prodotto scalare è non degenere, X'' sarà il sottospazio generato da X); ma anche se ci limitiamo a far variare X fra i sottospazi abbiamo esempi non banali, basta farlo in uno spazio di Hilbert di dimensione infinita (X' sarà sempre chiuso, anche se X non lo è, ed X'' sarà la chiusura di X).

Un ulteriore esempio riguarda l’estensione e la contrazione di ideali in algebra commutativa, vedi ad esempio il libro [AM69] (in quest’ultimo caso l’ordine parziale su uno dei due insiemi (gli ideali di un anello e quelli di un suo sottoanello) va rovesciato rispetto a quello naturale).

Ancora un esempio, e poi mi fermo, anche se ce ne sono tanti altri, è in teoria dei reticoli. Fissati due elementi a e b di un reticolo \mathcal{L} , e presi come \mathcal{A} e \mathcal{B} gli intervalli $[a \wedge b, b]$ ed $[a, a \vee b]$, le mappe *primo* sono $\cdot \wedge b : \mathcal{A} \rightarrow \mathcal{B}$ e $\cdot \vee a : \mathcal{B} \rightarrow \mathcal{A}$.

Entrambe le mappe *primo* sono biiezioni se il reticolo è modulare (ad esempio se \mathcal{L} è il reticolo dei sottogruppi normali di un gruppo, dove $H \vee K = \langle H, K \rangle$ e $H \wedge K = H \cap K$, o quello dei sottomoduli di un modulo, vedi ad esempio [Jac85]).

3.8. Una diseguaglianza

LEMMA 3.8.1. *Sia E/F un'estensione, e consideriamo due campi intermedi uno dentro l'altro*

$$F \subseteq L \subseteq M \subseteq E.$$

Supponiamo che il grado $|M : L|$ sia finito. Allora anche l'indice $|L' : M'|$ è finito, e si ha

$$|M : L| \geq |L' : M'|.$$

Un caso particolare utile di questo lemma è la seguente stima, se il grado $|E : F|$ è finito

$$(3.8.1) \quad |E : F| \geq |F' : E'| = |G : \{1\}| = |G|.$$

DIMOSTRAZIONE. Procedendo per induzione sul grado dell'estensione, come in [Kap95, Theorem 6], si vede subito che si può supporre $M = L(\alpha)$, per qualche α .

Supponiamo infatti che esista un campo intermedio K fra L e M , con $K \neq L, M$. Per induzione, si ha

$$|K : L| \geq |L' : K'|, \quad |M : K| \geq |K' : M'|.$$

Usando la formula dei gradi e qualcosa del genere del teorema di Lagrange (vedi la Proposizione 3.10.3 subito dopo la fine di questa dimostrazione) si ottiene

$$|M : L| = |M : K| \cdot |K : L| \geq |K' : M'| \cdot |L' : K'| = |L' : M'|.$$

Allora non vi sono campi intermedi fra L ed M . Se ora $\alpha \in M \setminus L$, si ha $L(\alpha) \neq L$, e dunque $L(\alpha) = M$.

Sia $f \in L[x]$ il polinomio minimo di α su L , e sia Ω l'insieme delle radici di f in M . Chiaramente abbiamo $|\Omega| \leq \text{grado}(f) = |M : L|$.

Ora per un argomento già visto L' agisce su Ω , dato che manda una radice di f in un'altra radice di f . Lo stabilizzatore di α quest'azione è M' , dato che fissare α equivale a fissare tutto $M = L(\alpha)$. Dunque per il Teorema orbita-stabilizzatore si ha che $|L' : M'|$ è eguale alla grandezza dell'orbita di α sotto L' . Ma quest'orbita è contenuta in Ω . e quindi questo numero è minore di $|M : L|$, come richiesto. \square

3.9. Casi particolari

Notate che del Lemma 3.8.1, o meglio, del suo caso particolare $|E : F| \geq |\text{Gal}(E/F)|$ enunciato subito dopo, già conosciamo un paio di casi particolari: uno è il caso in cui E è il campo di spezzamento di un polinomio su F , che abbiamo enunciato nella Sezione 2.3 di queste Note; l'altro (da cui abbiamo dedotto per induzione il caso precedente nella dimostrazione della Proposizione della Sezione 2.3) è il caso in cui $E = F(\alpha)$ con α algebrico su F .

Un commento metodologico all'ultima parte della dimostrazione del Lemma 3.6.1: assomiglia vagamente al fatto, già usato nella dimostrazione della Proposizione della Sezione 2.3, che l'automorfismo identico di L estende in al più $|L(\alpha) : L|$ modi ad un omomorfismo di $L(\alpha)$ in E . Certo, l'idea è la stessa, ma poi dobbiamo collegare questi ultimi omomorfismi di $L(\alpha)$ in E ad automorfismi di E , che sono quelli che stiamo contando, e diventa complicato da dire. Il modo giusto di fare le cose è usare le azioni, come nella dimostrazione.

3.10. Un commento sul Teorema di Lagrange

La forma tradizionale è

TEOREMA 3.10.1 (Lagrange). *Sia G un gruppo finito, e $H \leq G$. Allora*

$$|G| = |H| \cdot |G : H|.$$

Qui $|G : H|$ indica il numero di classi laterali di H in G . Una facile conseguenza è

COROLLARIO 3.10.2. *Sia G un gruppo finito, e $H \leq K \leq G$. Allora*

$$|G : H| = |G : K| \cdot |K : H|.$$

Basta calcolare, usando tre volte il Teorema di Lagrange

$$|G : H| = \frac{|G|}{|H|} = \frac{|K| \cdot |G : K|}{|H|} = |G : K| \cdot \frac{|K|}{|H|} = |G : K| \cdot |K : H|.$$

In realtà vale un risultato appena un po' più generale, che abbiamo usato nella dimostrazione del Lemma 3.8.1. Enunciato e dimostrazione somigliano molto alla formula dei gradi.

PROPOSIZIONE 3.10.3. *Sia G un gruppo qualsiasi, e $H \leq K \leq G$.*

1. *Se il numero $|G : H|$ di classi laterali di H in G è finito, allora sono finiti anche $|G : K|$ e $|K : H|$.*
2. *Se sono finiti i numeri $|G : K|$ e $|K : H|$, allora anche $|G : H|$ è finito.*
3. *Se i tre numeri sono finiti, allora vale*

$$|G : H| = |G : K| \cdot |K : H|.$$

DIMOSTRAZIONE. Le classi laterali di H in K sono un sottoinsieme delle classi laterali di H in G , per cui che $|K : H|$ sia finito è chiaro. Consideriamo la mappa

$$gH \mapsto gK,$$

che associa a ogni classe laterale di H in G una classe laterale di K in G . Si tratta di una mappa ben definita perché se $g_1H = g_2H$ allora $g_1^{-1}g_2 \in H \leq K$, e dunque $g_1K = g_2K$. Dato che la mappa è ovviamente suriettiva, abbiamo anche qui che $|G : K|$ è finito.

Ora resta da notare che se

$$g_1K, g_2K, \dots, g_nK$$

sono le classi laterali distinte di K in G , e

$$k_1H, k_2H, \dots, k_mH$$

sono le classi laterali distinte di H in K , allora

$$g_ik_jH, \quad 1 \leq i \leq n, 1 \leq j \leq m,$$

sono le classi laterali distinte di H in G .

Infatti esauriscono certamente tutto G , dato che

$$\begin{aligned} G &= \bigcup \{g_iK : 1 \leq i \leq n\} \\ &= \bigcup \left\{ g_i \cdot \left(\bigcup \{k_jH : 1 \leq j \leq m\} \right) : 1 \leq i \leq n \right\} \\ &= \bigcup \{g_ik_jH : 1 \leq i \leq n, 1 \leq j \leq m\}. \end{aligned}$$

Vediamo che sono distinte fra loro. Se $g_ik_jH = g_{i'}k_{j'}H$, allora $k_j^{-1}g_i^{-1}g_{i'}k_{j'} \in H \leq K$. In particolare $g_i^{-1}g_{i'} \in k_jKk_{j'}^{-1} = K$, e dunque $g_i = g_{i'}$. A questo punto $k_jH = k_{j'}H$, e quindi anche $k_j = k_{j'}$. \square

3.11. Un'altra diseuguaglianza

LEMMA 3.11.1. *Sia E/F un'estensione, e $G = \text{Gal}(E/F)$. Siano $H \leq K \leq G$ sottogruppi di G uno dentro l'altro.*

Supponiamo che l'indice $|K : H|$ sia finito. Allora anche il grado $|H' : K'|$ è finito, e si ha

$$|K : H| \geq |H' : K'|.$$

La dimostrazione è ripresa da [Kap95, Theorem 7].

DIMOSTRAZIONE. Per ogni $\alpha \in H'$, e $k \in K$, si può considerare l'elemento αk , che in generale sarà in E , non necessariamente ancora in H' . Se poi $h \in H$, chiaramente $\alpha h = \alpha$. Dunque se $k_1, k_2 \in K$ sono elementi nella stessa classe laterale $Hk_1 = Hk_2$, si ha $k_1 = hk_2$ per qualche $h \in H$, e quindi per ogni $\alpha \in H'$ vale

$$\alpha k_1 = \alpha h k_2 = \alpha k_2.$$

In altre parole, si può definire in modo non ambiguo, per ogni $k \in K$, l'azione $\alpha(Hk) = \alpha k$ della classe laterale Hk di K rispetto ad H su ogni $\alpha \in H'$.

Supponiamo adesso per assurdo che sia $n = |K : H| < |H' : K'|$. Siano $\alpha_1, \alpha_2, \dots, \alpha_{n+1} \in H'$ indipendenti su K' . Siano τ_1, \dots, τ_n le classi laterali di H in K - diciamo che sia $\tau_1 = H$. Consideriamo il sistema di n equazioni lineari nelle $n + 1$ incognite x_1, \dots, x_{n+1} :

$$(3.11.1) \quad \begin{cases} x_1 \cdot (\alpha_1\tau_1) + x_2 \cdot (\alpha_2\tau_1) + \dots + x_{n+1} \cdot (\alpha_{n+1}\tau_1) = 0 \\ x_1 \cdot (\alpha_1\tau_2) + x_2 \cdot (\alpha_2\tau_2) + \dots + x_{n+1} \cdot (\alpha_{n+1}\tau_2) = 0 \\ \dots \\ x_1 \cdot (\alpha_1\tau_n) + x_2 \cdot (\alpha_2\tau_n) + \dots + x_{n+1} \cdot (\alpha_{n+1}\tau_n) = 0 \end{cases}$$

Dato che è un sistema di n equazioni lineari omogenee in $n + 1$ incognite c'è senz'altro una soluzione $x_1, \dots, x_{n+1} \in E$, con gli x_i non tutti nulli. Prendiamone

una in cui il numero r di x_i diversi da zero sia minimo. Scambiando fra loro gli x_i , possiamo senz'altro supporre che sia $x_1 \neq 0, x_2 \neq 0, \dots, x_r \neq 0$, e $x_{r+1} = \dots = x_{n+1} = 0$. Dato che il sistema è omogeneo, possiamo anche moltiplicare la soluzione per x_1^{-1} , e assumere quindi $x_1 = 1$.

Se fosse $x_i \in K'$ per ogni i , avrei già ottenuto una contraddizione. Infatti $\tau_1 = H$, e dunque per ogni $\alpha_i \in H'$ avrei $\alpha_i \tau_1 = \alpha_i H = \alpha_i$, per cui la prima equazione di (3.11.1) diventa

$$x_1 \cdot \alpha_1 + x_2 \cdot \alpha_2 + \dots + x_{n+1} \cdot \alpha_{n+1} = 0.$$

Questa sarebbe una relazione di dipendenza lineare su K' degli α_i , contro l'ipotesi.

Dunque uno degli x_i non sarà in K' . Al solito, scambiando gli indici, possiamo supporre che sia $x_2 \notin K'$. Dunque esisterà $k \in K$ tale che $x_2 k \neq x_2$. Applichiamo k a tutte le equazioni in (3.11.1). Otteniamo

(3.11.2)

$$\begin{cases} (x_1 k) \cdot (\alpha_1 \tau_1 k) + (x_2 k) \cdot (\alpha_2 \tau_1 k) + \dots + (x_{n+1} k) \cdot (\alpha_{n+1} \tau_1 k) = 0 \\ (x_1 k) \cdot (\alpha_1 \tau_2 k) + (x_2 k) \cdot (\alpha_2 \tau_2 k) + \dots + (x_{n+1} k) \cdot (\alpha_{n+1} \tau_2 k) = 0 \\ \dots \\ (x_1 k) \cdot (\alpha_1 \tau_n k) + (x_2 k) \cdot (\alpha_2 \tau_n k) + \dots + (x_{n+1} k) \cdot (\alpha_{n+1} \tau_n k) = 0 \end{cases}$$

Ora se τ_1, \dots, τ_n sono le classi laterali di H in K , la moltiplicazione per k (a destra) non fa altro che permutarle. Dunque $\tau_1 k, \dots, \tau_n k$ sono ancora le classi laterali di H in K , magari in un ordine diverso. Ma allora la matrice dei coefficienti del sistema (3.11.2) è la stessa di quella del sistema (3.11.1): è solo che le righe sono scambiate. Dunque in (3.11.2) c'è scritto che oltre a

$$x_1, x_2, \dots, x_r, 0, \dots, 0,$$

anche

$$x_1 k, x_2 k, \dots, x_r k, 0, \dots, 0$$

è una soluzione di (3.11.1). Dato che si tratta di un sistema omogeneo, anche la differenza

$$(3.11.3) \quad x_1 - x_1 k, x_2 - x_2 k, \dots, x_r - x_r k, 0, \dots, 0$$

è una soluzione. Non si tratta della soluzione fatta di tutti zeri, perché abbiamo visto che $x_2 - x_2 k \neq 0$. Però dato che $x_1 = 1$, si ha $x_1 - x_1 k = 1 - 1k = 0$. Dunque la soluzione (3.11.3) ha un numero di componenti non nulle minore di quello di $x_1, x_2, \dots, x_r, 0, \dots, 0$. Questa è una contraddizione. \square

3.12. Dedekind

C'è un altro teorema che si dimostra in modo molto simile alla dimostrazione del Lemma 3.11.1, il Lemma di Dedekind sull'indipendenza dei caratteri, vedi ad esempio [Jac85], che si può enunciare nel modo seguente:

LEMMA 3.12.1. *Omomorfismi distinti di un gruppo finito G nel gruppo moltiplicativo di un campo E sono linearmente indipendenti su E .*

Il fatto che nel nome del Lemma di Dedekind siano menzionati i caratteri rivela un legame con la teoria delle rappresentazioni. In effetti, gli omomorfismi di G in E^\times sono esattamente i caratteri *lineari* di G (cioè caratteri di rappresentazioni di grado uno). Pertanto, il Lemma di Dedekind è un caso speciale del fatto più generale che caratteri di rappresentazioni inequivalenti (ovvero non simili, ovvero corrispondenti ad EG moduli non isomorfi) di G sono linearmente indipendenti.

3.13. Oggetti chiusi in estensioni di grado finito

Otteniamo subito il seguente importante

COROLLARIO 3.13.1. *Sia E/F un'estensione, e $G = \text{Gal}(E/F)$.*

1. *I sottogruppi finiti di G sono chiusi.*
2. *Se M è un campo intermedio chiuso, $L \supseteq M$, e $|L : M|$ è finito, allora L è chiuso.*
3. *In particolare, se E/F è normale, e L è un campo intermedio tale che $|L : F|$ sia finito, allora L è chiuso.*

DIMOSTRAZIONE. Sia $H \leq G$ di ordine finito. Allora

$$|H| = |H : \{1\}| \geq |\{1\}' : H'| = |E : H'| \geq |H'' : E'| = |H'' : \{1\}| = |H''|.$$

D'altra parte $H \leq H''$, e dunque $|H| \leq |H''|$, per cui $H = H''$.

Per la seconda parte,

$$|L : M| \geq |M' : L'| \geq |L'' : M''| = |L'' : M|.$$

Dato che $L \subseteq L''$, si ha che $L = L''$.

□

E' istruttivo considerare la dimostrazione dell'equivalente della seconda affermazione del Corollario 3.13.1 nel caso dei gruppi. (Ciò costituisce una affermazione più generale della prima del Corollario 3.13.1.) Cioè

LEMMA 3.13.2. *Se $H \leq K \leq G$, l'indice $|K : H|$ è finito, e H è chiuso, allora K è chiuso.*

DIMOSTRAZIONE. Come nel caso dei campi, arriviamo a

$$|K : H| = |K'' : H|, \quad \text{e} \quad K \subseteq K''.$$

Se K fosse finito, dedurremmo subito da Lagrange che K e K'' hanno lo stesso ordine, e dunque coincidono. In generale, basta comunque notare che K è unione di $|K : H|$ classi laterali di H , e $K'' \supseteq K$ è unione dello stesso numero di classi laterali di H : dunque le prime esauriscono già K'' , e quindi $K = K''$. □

Otteniamo subito

TEOREMA 3.13.3 (Teorema fondamentale della teoria di Galois).

Sia E/F una estensione normale di grado finito, e $G = \text{Gal}(E/F)$.

Allora tutti i sottogruppi di G e i sottocampi intermedi sono chiusi nella corrispondenza di Galois, e le operazioni "primo" stabiliscono una corrispondenza biunivoca fra i due insiemi.

Tali corrispondenze mandano gradi di campi in indici di sottogruppi e viceversa. In particolare

$$|G| = |E : F|.$$

DIMOSTRAZIONE. Resta solo da vedere l'ultima affermazione. Per sempio se $F \subseteq L \subseteq M \subseteq E$, abbiamo

$$|M : L| \geq |L' : M'| \geq |M'' : L''| = |M : L|,$$

dove l'ultima eguaglianza segue dal fatto che L e M sono chiusi. Dunque otteniamo $|M : L| = |L' : M'|$. In particolare

$$|E : F| = |F' : E'| = |G : \{1\}| = |G|,$$

dove $F' = G$ è l'ipotesi di normalità.

La dimostrazione nel caso dei sottogruppi è del tutto analoga, o addirittura la stessa, tenendo presente che ogni sottogruppo si può scrivere come il "primo" di qualcosa. \square

3.14. Un commento

Il Corollario 3.13.1 è piú simmetrico di quanto sembri. Eccone una formulazione piú simmetrica (che include anche le disuguaglianze necessarie a concludere la dimostrazione del Teorema 3.13.3). In sostanza il Corollario afferma che "la proprietà di essere chiuso si conserva salendo di una *distanza finita*", dove *distanza* va interpretato come *grado* o *indice* a seconda che si parli di campi o gruppi.

COROLLARIO 3.14.1. Sia E/F un'estensione, e $G = \text{Gal}(E/F)$.

1. Se $H \leq K \leq G$, l'indice $|K : H|$ è finito, e H è chiuso, allora anche K è chiuso, e $|H' : K'| = |K : H|$ (vedi il Lemma 3.9.2).
2. Se $F \subseteq K \subseteq L \subseteq G$, il grado $|L : K|$ è finito, e K è chiuso, allora anche L è chiuso, e $|K' : L'| = |L : K|$.

3.15. Un gruppo di Galois grande è una buona cosa

L'ultima affermazione del Teorema 3.13.3 si può invertire.

PROPOSIZIONE 3.15.1. Sia E/F un'estensione di grado finito.

Supponiamo che l'ordine di $G = \text{Gal}(E/F)$ eguagli il grado $|E : F|$. Allora E/F è normale.

DIMOSTRAZIONE. Abbiamo visto nel Lemma 3.4.2 che qualunque sia l'estensione E/F , e posto come al solito $G = \text{Gal}(E/F)$, si ha che l'estensione E/G' è normale, e $\text{Gal}(E/G') = \text{Gal}(E/F)$. Pertanto

$$|E : G'| = |G| = |E : F|,$$

e dunque $|G' : F| = 1$, ovvero $G' = F$, e E/F è normale. \square

Abbiamo visto nel capitolo precedente se E/F è il campo di spezzamento di un polinomio i cui fattori irriducibili hanno radici distinte, allora

$$|\text{Gal}(E/F)| \geq |E : F|.$$

Dato che in generale

$$|\text{Gal}(E/F)| \leq |E : F|.$$

otteniamo che i due numeri sono uguali, e dunque l'estensione è normale. Abbiamo ottenuto quella che in realtà vedremo essere la caratterizzazione delle estensioni normali di grado finito.

ESERCIZIO 14. Si consideri l'estensione $\mathbf{Q}(x)/\mathbf{Q}$, ove $\mathbf{Q}(x)$ è il campo delle funzioni razionali. Si mostri che il sottocampo $\mathbf{Q}(x^2)$ è chiuso, mentre non lo è $\mathbf{Q}(x^3)$.

3.16. Altri esercizi

ESERCIZIO 15. Determinate il campo di spezzamento di $x^5 - 1$ su \mathbf{Q} , costruite i campi ed i sottogruppi intermedi, e determinate esplicitamente la corrispondenza di Galois.

(*Suggerimento:* Ricordate che $(x^5 - 1)/(x - 1)$ è irriducibile su \mathbf{Q} . Il gruppo di Galois è ciclico di ordine 4.)

ESERCIZIO 16. Determinate il campo di spezzamento di $x^8 - 1$ su \mathbf{Q} , costruite i campi ed i sottogruppi intermedi, e determinate esplicitamente la corrispondenza di Galois.

(*Suggerimento:* Anche qui il gruppo di Galois ha ordine 4, (e quindi) è abeliano, ma non è ciclico. Esso ha tre sottogruppi di ordine 2.)

Il fatto che il gruppo di Galois non sia ciclico in questo caso, a differenza del caso precedente, è espressione di un fenomeno generale che conoscete dal corso di Teoria dei Numeri e Crittografia. Infatti, probabilmente non lo vedremo in questo corso, ma il gruppo di Galois di $x^n - 1$ su \mathbf{Q} è in generale isomorfo al gruppo degli automorfismi di un gruppo ciclico di ordine n , o, equivalentemente, al gruppo degli elementi invertibili dell'anello $\mathbf{Z}/n\mathbf{Z}$. Sappiamo che quest'ultimo è ciclico nel caso in cui n è una potenza di un primo dispari, mentre non è ciclico se n è una potenza di 2.

ESERCIZIO 17. Determinate il campo di spezzamento di $x^5 - 2$ su \mathbf{Q} , costruite i campi ed i sottogruppi intermedi, e determinate esplicitamente la corrispondenza di Galois.

(*Suggerimento:* Svolgetelo in modo simile all'esercizio sul campo di spezzamento di $x^3 - 2$ su \mathbf{Q} ; naturalmente ora servono meno verifiche, perché conoscete il Teorema fondamentale della teoria di Galois. Il grado dell'estensione, e quindi l'ordine del gruppo di Galois, stavolta viene 20.)

Estensioni normali e campi di spezzamento

4.1. Un lemma fondamentale

Il seguente risultato comincia a mostrare come una estensione normale algebrica sia legata ai campi di spezzamento.

TEOREMA 4.1.1. *Sia E/F una estensione normale.*

Sia $f \in F[x]$ un polinomio monico e irriducibile.

Se f ha una radice α in E , allora f si spezza in $E[x]$ nel prodotto di fattori distinti di primo grado.

In particolare, dunque, E contiene un campo di spezzamento per f , e f ha tutte le sue radici distinte.

DIMOSTRAZIONE. Sia $\Omega = \{\alpha_1, \dots, \alpha_m\}$ (con $\alpha = \alpha_1$) l'insieme delle immagini distinte di α sotto gli elementi di $G = \text{Gal}(E/F)$ radici di f in E ; dunque $\alpha_i \neq \alpha_j$ per $i \neq j$. Consideriamo il polinomio in $E[x]$

$$(4.1.1) \quad \tilde{f} = (x - \alpha_1) \cdots (x - \alpha_m)$$

Esso divide f , dato che gli α_i sono distinti, e dunque $\text{grado}(\tilde{f}) = m \leq n = \text{grado}(f)$.

Chi sono i coefficienti di f in termini degli α_i ? Il coefficiente di x^m è 1. Il coefficiente di x^{m-1} è, lasciando perdere i segni per il momento,

$$\alpha_1 + \alpha_2 + \cdots + \alpha_m.$$

Il coefficiente di x^{m-2} è

$$\alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{m-1}\alpha_m,$$

ovvero è la somma di tutti i prodotti a due a due degli α_i (distinti). In generale, il coefficiente di x^{m-k} è

$$(-1)^k \sum \{ \alpha_{i_1} \cdot \alpha_{i_2} \cdots \alpha_{i_k} : 1 \leq i_1 < i_2 < \cdots < i_k \leq m \}.$$

Come ulteriore illustrazione, il coefficiente costante è semplicemente il prodotto di tutti gli α_i .

Ora tutti questi coefficienti di \tilde{f} sono *funzioni simmetriche* negli α_i , nel senso che non cambiano se si permutano fra loro gli α_i . Dunque essi sono invarianti sotto G , dato che G non fa altro, appunto, che permutare gli α_i . Dato che E/F è normale, ho che $G' = F$, e dunque i coefficienti di \tilde{f} sono in F , cioè $\tilde{f} \in F[x]$.

Ora f è monico e irriducibile, e \tilde{f} è un suo divisore monico non costante. Dunque $f = \tilde{f}$, e abbiamo ottenuto la fattorizzazione (4.1.1) cercata. \square

Notate che il discorso sulle funzioni simmetriche, per quanto interessante (e verrà comunque ripreso in seguito), non è indispensabile a questo punto: è sufficiente notare che qualsiasi elemento di G estende in modo naturale ad un automorfismo dell'anello dei polinomi $E[x]$ (agendo sui coefficienti e lasciando invariata l'indeterminata x), che evidentemente lascia invariato \tilde{f} , cioè lascia invariati tutti i suoi coefficienti.

Notate inoltre che il numero di addendi nel coefficiente di x^{m-k}

$$(-1)^k \sum \{\alpha_{i_1} \alpha_{i_2} \cdots \alpha_{i_k} : 1 \leq i_1 < i_2 < \cdots < i_k \leq m\}.$$

è, in generale, il coefficiente binomiale $\binom{m}{k}$ (cioè il coefficiente di x^{m-k} , o equivalentemente di x^k , nell'espansione di $(1+x)^m$): basta guardare al caso in cui tutti gli α_i valgono 1. Infatti $\binom{m}{k}$ è anche il numero di combinazioni di m oggetti (gli α_i) presi k alla volta.

4.2. Separabilità

Un polinomio irriducibile $f \in F[x]$ si dice separabile se ha radici distinte nel suo campo di spezzamento. Ciò equivale a dire che $(f, f') = 1$. Sia E/F una estensione algebrica. Un elemento $a \in E$ si dice separabile su F se il suo polinomio minimo su F è separabile. L'intera estensione è separabile se ogni suo elemento lo è. Contrariamente a quel che scrive Kaplansky, non mi pare inoltre che ci sarebbe niente di male a dire che un polinomio $f \in F[x]$ è separabile se i suoi fattori irriducibili in $F[x]$ lo sono.

Abbiamo già visto una parte del seguente

TEOREMA 4.2.1. *Sia E/F un'estensione di grado finito, dunque algebrica. Sono equivalenti*

1. E/F è normale.
2. E è il campo di spezzamento su F di un polinomio i cui fattori irriducibili sono separabili.
3. E/F è separabile, ed E è un campo di spezzamento su F .

DIMOSTRAZIONE. Abbiamo già visto nella parte finale del capitolo sui campi di spezzamento che la seconda condizione implica la prima. E' facile vedere che la terza implica la seconda. Resta da vedere che la prima implichi la terza.

Mostriamo intanto che E/F è separabile. per ogni $\alpha \in E$, se g è il polinomio minimo su F di $\alpha \in E$, allora g ha radici distinte nel suo campo di spezzamento (che poi in questo caso è contenuto in E) grazie al Teorema 4.1.1.

Ora, dato che E ha grado finito su F , si può scrivere $E = F(\alpha_1, \dots, \alpha_n)$, per esempio prendendo gli α_i come una base di E su F . Sia f_i il polinomio minimo di α_i su F . Per il Teorema 4.1.1, tutte le radici di tutti gli f_i sono in E . Dunque E è il campo di spezzamento su F del polinomio $f = f_1 \cdots f_n$. \square

4.3. Radici multiple

Ricordiamo dal corso di Algebra che vale il seguente

LEMMA 4.3.1. *Sia F un campo, $f \in F[x]$. Un elemento α in una estensione E di F è una radice multipla di f se e solo se α è radice sia di f che di f' , e quindi è radice del massimo comun divisore (f, f') .*

Ne segue che f ha radici multiple nel suo campo di spezzamenti se e solo se $(f, f') \neq 1$.

Sia $f \in F[x]$ irriducibile. Se $f' \neq 0$, allora $\text{grado}(f') < \text{grado}(f)$, dunque anche il grado del massimo comune divisore (f, f') è minore del grado di f . Dato che f è irriducibile, ne segue che $(f, f') = 1$, e dunque f non ha radici multiple. Pertanto se un polinomio irriducibile ha radici multiple, la sua derivata deve essere zero. Dunque si ha

$$\begin{aligned} f &= x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0, \\ f' &= nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1 = 0, \\ n &= (n-1)a_{n-1} = \cdots = ia_i = \cdots a_1 = 0. \end{aligned}$$

Ora già $n = 0$ è impossibile in caratteristica zero, mentre se la caratteristica di F è un primo p le eguaglianze sono verificate quando $a_i = 0$ se p non divide i . Dunque f ha derivata zero se è della forma

$$f(x) = x^{pm} + b_{m-1}x^{p(m-1)} + \cdots + b_1x^p + b_0,$$

ovvero $f(x) = g(x^p)$, ove

$$g(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0.$$

4.4. Campi finiti

Ricordiamo dal corso di Algebra che un campo finito E ha ordine p^n , ove p è un primo, contiene il campo F con p elementi, ed è il campo di spezzamento su F del polinomio $f = x^{p^n} - x$. Dai risultati generali sui campi di spezzamento, segue l'unicità, a meno di isomorfismi su F , del campo con p^n elementi.

Ora $f' = p^n x^{p^n-1} - 1 = -1$, dunque $(f, f') = 1$, e f ha radici distinte. Per il Teorema 4.2.1, E/F è una estensione normale, di grado n . Il gruppo di Galois $G = \text{Gal}(E/F)$ ha dunque ordine n . La regola del binomio in caratteristica p ci dice che la mappa (morfismo di Frobenius)

$$\begin{aligned} \varphi : E &\rightarrow E \\ a &\mapsto a^p \end{aligned}$$

è un automorfismo di E , e fissa gli elementi di F , per il Teorema di Eulero-Fermat. Dunque $\varphi \in G$. Si vede subito che $a\varphi^i = a^{p^i}$. Dunque se $0 < i < n$ gli elementi $a \in E$ fissati da φ^i sono le radici del polinomio $x^{p^i} - x$. Dato che questo polinomio ha al più $p^i < p^n$ radici, φ^i non è la mappa identica su E . Invece φ^n lo è, dato che si vede in Algebra che ogni elemento di E è radice di $x^{p^n} - x$. Dunque φ ha periodo n , e quindi $G = \langle \varphi \rangle$ è ciclico.

E' ora facile vedere chi sono i campi intermedi fra F e E . Infatti ricordiamo da Algebra che il gruppo ciclico G ha uno e un solo sottogruppo di indice m , per ogni divisore m di n , e questo sottogruppo è $\langle \varphi^m \rangle$. Dunque c'è un sottocampo L di grado $|L : F| = m$ per ogni divisore m di n . Dato che $|L| = p^m$, si ha che L deve essere l'unico campo finito con p^m elementi. In effetti per la teoria si ha

$$\begin{aligned} L &= \langle \varphi^m \rangle' \\ &= \{ a \in E : a\varphi^m = a \} \\ &= \{ a \in E : a \text{ è radice di } x^{p^m} - x \} \end{aligned}$$

ESERCIZIO 18. Si provi a dimostrare *direttamente* questo fatto, che segue dalla teoria appena vista.

Sia p un primo, F il campo con p elementi. Sono equivalenti:

1. $x^{p^m} - x$ divide $x^{p^n} - x$ in $F[x]$;
2. $p^m - 1$ divide $p^n - 1$;
3. m divide n

Sia F il campo con p elementi, e $f \in F[x]$ un polinomio irriducibile di grado n . Sia $E = F(\alpha)$, con $f(\alpha) = 0$, Dunque $|E : F| = n$, e E è il campo con p^n elementi. Dato che E/F è normale, e f ha una radice in E , ne segue dal Teorema 4.1.1 che f ha tutte le sue radici in E , e queste sono distinte. Quindi su un campo con un numero primo di elementi tutti i polinomi irriducibili sono separabili.

E' facile generalizzare il ragionamento per mostrare che tutti i polinomi su un campo finito sono separabili. Infatti, se f è un polinomio irriducibile di grado n sul campo K con $q = p^f$ elementi, ed $E = K(\alpha)$ con $f(\alpha) = 0$, allora E è il campo con $q^n = p^{fn}$ elementi. Dal fatto che E/F è normale, dove F è il campo con p elementi, segue che anche E/K è normale (essendo K chiuso nella corrispondenza di Galois per E/F , grazie al Teorema 3.13.3), ed ora basta applicare il Teorema 4.1.1 come nelle Note.

4.5. Unicità dei campi finiti

Abbiamo ricordato che un campo finito ha ordine p^n , per qualche primo p , e che è campo di spezzamento del polinomio $x^{p^n} - x$. Dal risultato generale per l'unicità di un campo di spezzamento segue anche l'unicità del campo finito di ordine p^n .

C'è anche un modo più elementare di vedere questa unicità, che si basa sul risultato visto ad Algebra che il gruppo moltiplicativo di un campo finito è ciclico, e dunque il campo è estensione semplice, della forma $F(\alpha)$.

Sia $g \in F[x]$ un polinomio monico e irriducibile di grado n , ove $F = \mathbf{Z}/p\mathbf{Z}$ è il campo con p elementi. Sia α una sua radice in qualche estensione. Dunque $F(\alpha)$ è un campo con p^n elementi. Ogni elemento di $F(\alpha)$ è radice di $x^{p^n} - x$. Dunque $x^{p^n} - x$ e g hanno in comune il fattore $x - \alpha$. Dato che g è irriducibile in $F[x]$, vuole dire che g divide $x^{p^n} - x$. Abbiamo visto che ogni polinomio irriducibile di grado n divide $x^{p^n} - x$. Dunque un qualsiasi campo di spezzamento di $x^{p^n} - x$ contiene tutte le radici dei polinomi irriducibili di grado n , e quindi tutti i campi finiti di ordine p^n , che abbiamo visto essere della forma $F(\alpha)$, per queste radici α .

In altre parole: un campo finito con p^n elementi è un'estensione semplice $F(\alpha)$ del campo F con p elementi, basta prendere come α un generatore del suo gruppo moltiplicativo, che sappiamo essere ciclico. Naturalmente $F(\alpha) \cong F[x]/(g)$, dove $g \in F[x]$ è il polinomio minimo di α su F . D'altra parte, come mostrato nelle Note, essendo g irriducibile su F , esso divide il polinomio $x^{p^n} - x$, e quindi un qualsiasi campo di spezzamento E di $x^{p^n} - x$ contiene una radice β di g (anzi, tutte). Per ragioni di grado avremo $E = F(\beta)$, ma $F(\beta)$ è isomorfo a $F(\alpha)$ su F (entrambi sono isomorfi a $F[x]/(g)$). Ciò mostra che ogni campo con p^n elementi è isomorfo al campo E che abbiamo fissato.

4.6. Un campo di spezzamento non normale

Abbiamo visto che per avere un polinomio irriducibile con radici non distinte bisogna essere in caratteristica $p > 0$. Però i campi finiti, pur avendo caratteristica un primo p , danno estensioni normali. Per vedere un esempio di campo di spezzamento non normale, occorre quindi passare a campi infiniti.

Sia $K = \text{GF}(p)$ il campo con p elementi, p un numero primo. Sia $E = K(t)$ il campo delle funzioni razionali nell'indeterminata t . Sia $F = K(t^p)$. Notiamo che $t \notin F$. Se infatti

$$t = \frac{f(t^p)}{g(t^p)}, \quad \text{con } f, g \in K[t], \text{ e } g \neq 0$$

allora $tg(t^p) = f(t^p)$. Se adesso $n = \text{grado}(f)$, e $m = \text{grado}(g)$, otteniamo $1 + mp = np$, un assurdo.

Ora $E = F(t)$, con t algebrico su F , dato che t è radice del polinomio $\psi(x) = x^p - t^p \in F[x]$. Dico che $\psi(x)$ è irriducibile in $F[x]$. Questo seguirà da un risultato più generale che vedremo più avanti (Lemma 9.1.2); ne diamo qui una semplice dimostrazione ad hoc. Per la nota proprietà del binomio di Newton in caratteristica p prima abbiamo $\psi(x) = (x - t)^p$ in $E[x]$. Dunque se ψ si fattorizza propriamente in $F[x]$, dovremo avere

$$\psi(x) = (x - t)^\alpha \cdot (x - t)^\beta,$$

con $0 < \alpha, \beta < p$, e $(x - t)^\alpha, (x - t)^\beta \in F[x]$. Ma allora $(x - t)^\alpha = x^\alpha - \alpha t x^{\alpha-1} + \dots \in F[x]$, e dunque $\alpha t \in F$. Ma $\alpha \neq 0$ in K , e dunque $t \in F$, una contraddizione.

Dato che ψ è irriducibile in $F[x]$, ne segue che ψ è il polinomio minimo di t su F . Quindi $|E : F| = |F(t) : F| = p$. Dato che $\psi(x) = (x - t)^p$, si ha che t è l'unica radice di ψ in E , con molteplicità p . Dato che un elemento di $G = \text{Gal}(E/F)$ deve mandare t in un'altra radice del suo polinomio minimo, abbiamo $G = \{1\}$.

E/F è quindi un esempio di campo di spezzamento non normale, dato che $|E : F| = p$, e $|G| = 1$. La ragione, come abbiamo visto, è che il polinomio irriducibile ψ non ha radici distinte.

Il fatto che il polinomio $x^p - t^p \in F[x]$ sia irriducibile in $F[x]$ (essendo $t \notin F$) si può mostrare in vari modi. Il più efficiente a questo punto è forse il seguente.

LEMMA 4.6.1. *Se F ha caratteristica p ed $a \in F$, allora o $x^p - a$ è irriducibile in $F[x]$, oppure a è una p -esima potenza in F , e dunque $x^p - a$ è una p -esima potenza in $F[x]$.*

DIMOSTRAZIONE. Se b è una radice di $x^p - a$ in un'estensione E di F , allora $b^p = a$, e quindi $x^p - a = x^p - b^p = (x - b)^p$ in $E[x]$, ed E è un campo di spezzamento per $x^p - a$ su F . Ora, poiché $x^p - a$ ha una sola radice nel suo campo di spezzamento E (con molteplicità p), qualsiasi suo fattore irriducibile non lineare g ha radici multiple in E , e quindi ha grado multiplo di p per quanto visto nella Sezione 4.3. Di conseguenza, o $x^p - a$ è irriducibile in $F[x]$, o è prodotto di fattori lineari (necessariamente uguali) in $F[x]$. \square

Abbiamo visto che i campi di caratteristica zero ed i campi finiti condividono una proprietà: sono campi *perfetti*, termine che ora definiamo. Un campo F si dice *perfetto* se ogni polinomio a coefficienti in F è separabile (cioè ogni suo fattore irriducibile ha radici distinte); equivalentemente, F è perfetto se ogni sua estensione algebrica è separabile su F .

Ecco un criterio per decidere se un campo di caratteristica positiva è perfetto.

TEOREMA 4.6.2. *Un campo di caratteristica $p > 0$ è perfetto se e solo se F coincide con F^p , il sottocampo costituito dalle p -esime potenze degli elementi di F .*

DIMOSTRAZIONE. Notiamo anzitutto che F^p è un sottocampo, essendo l'immagine di un omomorfismo di campi, l'*endomorfismo di Frobenius* $a \mapsto a^p$; come ogni omomorfismo fra campi, esso è sempre iniettivo, ma non è detto che sia suriettivo.

Se F^p è un sottocampo proprio di F , ed $a \in F \setminus F^p$, allora grazie al Lemma $x^p - a$ è un polinomio irriducibile con radici multiple, quindi inseparabile.

Viceversa, supponiamo che f sia un polinomio monico irriducibile inseparabile in $F[x]$. Come abbiamo visto nella Sezione 4.3, f deve avere la forma $f(x) = x^{pm} + a_{m-1}x^{p(m-1)} + \dots + a_1x^p + a_0$. Almeno uno di questi coefficienti a_i non è una p -esima potenza di un elemento di F . Infatti, se fosse $a_i = b_i^p$ per ogni i , per opportuni $b_i \in F$, avremmo $f(x) = x^{pm} + b_{m-1}^p x^{p(m-1)} + \dots + b_1^p x^p + b_0^p = (x^m + b_{m-1}x^{(m-1)} + \dots + b_1x + b_0)^p$, in contraddizione col fatto che f è irriducibile su F . Non ci resta che concludere che $F \neq F^p$. \square

Una conseguenza immediata del Teorema è il fatto (che avevamo già dimostrato in precedenza) che i campi finiti sono perfetti: infatti l'endomorfismo di Frobenius $a \mapsto a^p$ in questo caso è necessariamente suriettivo.

4.7. Altri esercizi

ESERCIZIO 19. Determinate il campo di spezzamento di $x^{13} + 1$ sul campo con 3 elementi \mathbb{F}_3 , costruite i campi ed i sottogruppi intermedi, e determinate esplicitamente la corrispondenza di Galois.

(*Suggerimento:* Non serve trovare i fattori irriducibili di $x^{13} + 1$ su \mathbb{F}_3 , basta usare la teoria dei campi finiti.)

Chiusure spezzanti e chiusure normali

5.1. Una caratterizzazione dei campi di spezzamento

Notiamo intanto il seguente utile Lemma, che caratterizza i campi di spezzamento senza che si debba nominare esplicitamente un polinomio.

LEMMA 5.1.1. *Sia E/F una estensione di grado finito. Sono equivalenti*

1. *E è un campo di spezzamento su F*
2. *Se un polinomio monico e irriducibile $f \in F[x]$ ha una radice in E , allora le ha tutte.*

DIMOSTRAZIONE. Mediante argomenti simili a quelli usati per la caratterizzazione delle estensioni normali, si vede facilmente che la seconda condizione implica la prima.

Supponiamo adesso che E sia il campo di spezzamento su F di un polinomio $g \in F[x]$. Sia per assurdo $f \in F[x]$ un polinomio monico e irriducibile che abbia una radice $\alpha \in E$, ma una radice $\beta \notin E$. Consideriamo i campi $F(\alpha) \subseteq E$, $F(\beta)$, ed $E(\beta) \neq E$. Come al solito, c'è un isomorfismo su F fra $F(\alpha)$ e $F(\beta)$, dato che α e β sono radici dello stesso polinomio irriducibile f . Inoltre E è ancora il campo di spezzamento su $F(\alpha)$ di g , e $E(\beta)$ è il campo di spezzamento su $F(\beta)$ di g . Per il Teorema di unicità 2.3.1, l'isomorfismo su F fra $F(\alpha)$ ed $F(\beta)$ si estende a un isomorfismo fra E e $E(\beta)$. Ma questo è un isomorfismo su F , e quindi dovrebbe in particolare essere un isomorfismo di spazi vettoriali su F , e quindi conservare le dimensioni, dunque i gradi. Ma

$$|E(\beta) : F| = |E(\beta) : E| \cdot |E : F| \neq |E : F|,$$

dato che $E(\beta) \neq E$, e dunque $|E(\beta) : E| \neq 1$. □

VARIANTE. C'è una leggera variante, non tanto diversa, ma appena un po' più concettuale, per la seconda parte dell'argomento.

Consideriamo il campo di spezzamento L di $f \cdot g$ su F . Dato che E è un campo di spezzamento su F , è stabile in L/F . Ora $\text{Gal}(L/F)$ agisce transitivamente sulle radici del polinomio irriducibile $f \in F[x]$ (se non l'ho scritto da nessuna parte su queste note, questo è il momento), dunque tutte le radici di f sono in E . □

Come accennato, molta della teoria finora trattata si può estendere a estensioni algebriche, di grado anche infinito. Per esempio per il risultato appena visto occorre sostituire l'argomento sulle dimensioni, che perde significato, con il seguente, che comunque si dimostra riducendosi al caso di grado finito.

LEMMA 5.1.2. *Sia E/F una estensione algebrica. Sia φ un morfismo iniettivo di E in E su F ,*

Allora φ è suriettivo.

In realtà dato che nei campi gli unici ideali sono lo zero e tutto, la condizione che il morfismo sia iniettivo è superflua, dato che chiediamo già che sia l'identità su F , e quindi non sia nullo.

DIMOSTRAZIONE. Sia $\alpha \in E$, e sia $f \in F[x]$ il suo polinomio minimo su F . Siano $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ le radici di f in E , e sia $L = F(\alpha_1, \alpha_2, \dots, \alpha_n)$. Dato che φ fissa gli elementi di F , per un argomento familiare deve mandare ogni α_i , che è una radice di f in E , in un'altra radice α_j . Dunque $L\varphi \subseteq L$. Ora però il grado $|L : F|$ è finito, e dunque per l'argomento su grado/dimensione del risultato appena visto deve essere $L\varphi = L$. In particolare α sta nell'immagine di φ . Dato che α era arbitrario, abbiamo che φ è suriettiva. \square

Supponiamo ora di avere una estensione di grado finito E/F , e di voler ampliare E a un campo di spezzamento su F . Il risultato appena visto non ci lascia scelta. Scriviamo $E = F(\alpha_1, \dots, \alpha_n)$, e sia f_i il polinomio minimo di α_i su F . Allora un campo di spezzamento che contenga E deve contenere tutte le radici degli f_i , per il risultato appena visto. Dunque il più piccolo campo di spezzamento che contenga E deve essere il campo di spezzamento M su F se $f = f_1 \cdot \dots \cdot f_n$. Se E/F è separabile, allora il polinomio f è separabile, e otteniamo che M/F è normale.

M si dice la chiusura spezzante di E/F . Qualora E/F sia separabile, M si dice chiusura normale di E/F .

E' utile per il seguito vedere come M si possa costruire a partire da E . Cercando di evitare notazioni troppo pesanti, M è generata su F da tutte le radici dei vari polinomi f_i . Sia β una di queste radici. Per argomenti familiari, c'è un isomorfismo su F fra $F(\alpha_i)$ e $F(\beta)$ che manda α_i in β . Dato che M è un campo di spezzamento, in particolare sia su $F(\alpha_i)$ che su $F(\beta)$, questo isomorfismo si estende a un elemento $\varphi \in \text{Gal}(M/F)$. Dunque $\beta = \alpha_i\varphi \in E\varphi$. Ne segue che M è generati da tutti i sottocampi $E\varphi$, al variare di $\varphi \in \text{Gal}(M/F)$, cioè che M è il più piccolo campo che li contiene tutti. (Si usa dire che M è il *compositum*, o composto, degli $E\varphi$.)

5.2. Osservazioni

Come già osservato altrove, la seconda condizione del Lemma 5.1.1 è ciò che in altri testi è la definizione di normalità di E/F (quindi più debole, ovvero meno restrittiva, della nostra). Notate che del Lemma 5.1.1 già conosciamo la versione per estensioni separabili, che possiamo formulare come segue.

LEMMA 5.2.1. *Sia E/F una estensione di grado finito. Sono equivalenti*

1. *E è separabile su F ed è un campo di spezzamento su F (vale a dire, E è normale, grazie alla caratterizzazione data dal Teorema 4.2.1).*
2. *Se un polinomio monico e irriducibile $f \in F[x]$ ha una radice in E , allora le ha tutte e sono distinte (cioè f si spezza in $E[x]$ nel prodotto di fattori lineari distinti).*

Infatti, la seconda condizione di questo Lemma è semplicemente la tesi del Teorema 4.1.1, che quindi mostra (assieme al Teorema 4.2.1) l'implicazione $1 \Rightarrow 2$.

L'implicazione $2 \Rightarrow 1$ si dimostra invece esattamente come abbiamo dimostrato l'implicazione $1 \Rightarrow 3$ del Teorema 4.2.1.

Quindi l'implicazione $2 \Rightarrow 1$ del Lemma 5.1.1 si dimostra nello stesso modo (anzi, tralasciando la parte che riguarda la separabilità). Invece per l'implicazione $1 \Rightarrow 2$ ci manca il Teorema 4.1.1 (l'estensione non ha sufficienti automorfismi per decidere mediante essi se un elemento di E sta in F), e per questo facciamo la dimostrazione descritta nelle Note, ricorrendo al Teorema di unicità del campo di spezzamento.

In realtà non c'è bisogno di fare quella dimostrazione per assurdo, si può fare anche in forma diretta.

Un'osservazione riguardo alla costruzione della chiusura normale di un'estensione E/F : come si deduce dal ragionamento fatto nelle Note, che tale chiusura spezzante sia un'estensione separabile, e che quindi si possa chiamare la chiusura normale di E/F , dipende solamente dal fatto che l'estensione di partenza E/F sia separabile (l'una è separabile se e solo se l'altra lo è).

Estensioni normali e sottogruppi normali

6.1. Campi intermedi stabili

Nella corrispondenza di Galois, ad *estensioni normali* corrispondono proprio quelli che si dicono *sottogruppi normali*. In realtà la normalità di un sottogruppo corrisponde a una proprietà che si dice *stabilità*; nel caso algebrico questa corrisponde alla normalità di una estensione.

Sia E/F una estensione. Un campo intermedio L si dice *stabile* rispetto a E/F se per ogni $g \in \text{Gal}(E/F)$ si ha $Lg = L$. Notate che non si chiede che L sia fissato elemento per elemento, ma solo che sia mandato in sé.

TEOREMA 6.1.1. *Sia E/F una estensione, $G = \text{Gal}(E/F)$.*

1. *Se L è un campo intermedio stabile, allora L' è un sottogruppo normale di G .*
2. *Se H è un sottogruppo normale di G , allora H' è un campo intermedio stabile.*

DIMOSTRAZIONE. Sia L un campo intermedio stabile. Dobbiamo far vedere che L' è un sottogruppo normale di G , e cioè che per ogni $g \in G$ e ogni $h \in L'$ si ha $g^{-1}hg \in L'$. Dunque dobbiamo vedere che per ogni $a \in L$ si ha $ag^{-1}hg = a$. Ora per la stabilità si ha $ag^{-1} \in L$, dunque $ag^{-1}h = ag^{-1}$, e $ag^{-1}hg = ag^{-1}g = a$ come richiesto.

Viceversa, sia H normale in G , sia $a \in H'$, $g \in G$. Dobbiamo vedere che $ag \in H'$, cioè che per ogni $h \in H$ valga $(ag)h = ag$. Ma poiché H è normale si ha $gh = kg$ per qualche $k \in H$, e dunque $agh = akh = ag$ come richiesto, dato che $a \in H'$ e $k \in H$. \square

6.2. Stabilità e normalità

COROLLARIO 6.2.1. *Siano $F \subseteq K \subseteq E$ campi.*

1. *Se E/F è normale, e K è stabile in E/F , allora K/F è normale.*
2. *Se K/F è normale e algebrica, allora K è stabile in E/F .*

Questi risultati mostrano che nel caso algebrico dire che K/F è normale è la stessa cosa che dire che K è stabile in E/F , e quindi che K è un sottogruppo normale di $\text{Gal}(E/F)$.

Notiamo già che ci siamo che invece E/K è sempre una estensione normale, se E/F è normale di grado finito. Infatti per il Teorema 3.13.3 K è chiuso nella corrispondenza di Galois, e dunque $K = K'' = \text{Gal}(E/K)'$. Questa è proprio la definizione di normalità per E/K .

Vedremo più avanti un fatto più generale in questa direzione.

DIMOSTRAZIONE. Sia $a \in K \setminus F$. Per la normalità di E/F esiste un $g \in G = \text{Gal}(E/F)$ tale che $ag \neq a$. Dato che K è stabile, la restrizione $h = g|_K$ manda K in K , ed è quindi un elemento di $\text{Gal}(K/F)$. Dato che $ah = ag \neq a$, ne segue che K/F è normale.

Per la seconda parte, dobbiamo dimostrare che se $a \in K$, e $g \in G = \text{Gal}(E/F)$, allora $ag \in K$. Sia f il polinomio minimo di a su K . Per il Teorema 4.1.1, f ha tutte le sue radici in K . Ora g deve mandare a in un'altra radice di f , e quindi comunque in un altro elemento di K . Ne segue che K è stabile.

Oppure, almeno per il caso di grado finito, si può usare direttamente il Teorema 4.2.1, conseguenza del Teorema 4.1.1: K è un campo di spezzamento di F , dunque chiaramente stabile. \square

Sia adesso E/F una estensione normale di grado finito, e sia K un campo intermedio, con K/F normale, e dunque $K' = \text{Gal}(E/K)$ normale in $G = \text{Gal}(E/F)$. Dato che K è stabile, la restrizione a K degli elementi di G è ben definita, e manda gli elementi di G in elementi di $\text{Gal}(K/F)$; il nucleo di tale mappa

$$\begin{aligned} \text{Gal}(E/F) &\rightarrow \text{Gal}(K/F) \\ g &\mapsto g|_K \end{aligned}$$

è subito visto essere $\text{Gal}(E/K)$. D'altra parte

$$\frac{|\text{Gal}(E/F)|}{|\text{Gal}(E/K)|} = \frac{|\text{Gal}(E/F)|}{|\text{Gal}(E/K)|} = \frac{|E:F|}{|E:K|} = |K:F| = |\text{Gal}(K/F)|,$$

ove abbiamo usato formula dei gradi, Lagrange, e l'identità $|\text{Gal}(M/L)| = |M:L|$ per una estensione normale M/L . Per questioni di ordine, otteniamo l'importante isomorfismo

$$\frac{\text{Gal}(E/F)}{\text{Gal}(E/K)} \cong \text{Gal}(K/F).$$

Una dimostrazione alternativa si basa sul fatto che E è un campo di spezzamento su F di un polinomio separabile $f \in F[x]$. Dunque E è campo di spezzamento dello stesso polinomio anche su L . (Questo fornisce una dimostrazione alternativa, grazie al Teorema 4.2.1, del fatto che allora E/L è normale.) Dunque per il teorema di unicità posso estendere un elemento di $\text{Gal}(L/F)$ a un elemento di $\text{Gal}(E/F)$. Questo argomento ci permetterà di estendere il risultato precedente al caso di estensioni algebriche anche di dimensione infinita.

6.3. Una situazione più generale

Abbiamo visto che se E/F è un'estensione normale di grado finito con un campo intermedio K normale su F vale l'isomorfismo

$$\text{Gal}(E/F)/\text{Gal}(E/K) \cong \text{Gal}(K/F).$$

Ecco ciò che rimane vero nel caso di un'estensione E/F arbitraria con campo intermedio K stabile: $\text{Gal}(E/F)/\text{Gal}(E/K)$ è isomorfo al sottogruppo di $\text{Gal}(K/F)$ che consiste degli automorfismi che estendono ad automorfismi di E . La dimostrazione è analoga, l'isomorfismo è dato dalla restrizione, salvo il fatto che qui

non tutti gli automorfismi di K/F estendono necessariamente ad automorfismi di E/F .

ESEMPIO. Prendendo $F = \mathbf{Q}$, $K = \mathbf{Q}(\sqrt{2})$, $E = \mathbf{Q}(\sqrt[4]{2})$, abbiamo che K/F è normale (e quindi stabile, per quanto visto, essendo un'estensione algebrica), ed anche E/K (è campo di spezzamento del polinomio $x^2 - \sqrt{2}$), mentre E/F non lo è (il polinomio irriducibile $x^4 - 2$ ha solo due radici in E). Il gruppo $\text{Gal}(E/F)$ è composto dall'identità e dall'automorfismo individuato da $\sqrt[4]{2} \mapsto -\sqrt[4]{2}$, che sono le due possibili estensioni dell'automorfismo identità di K/F . (In effetti si vede anche direttamente che l'automorfismo non banale di K/F , che manda $\sqrt{2} \mapsto -\sqrt{2}$, non si può estendere ad un automorfismo di E/F , perché tale estensione dovrebbe mandare $\sqrt[4]{2}$ in una delle radici quadrate di $-\sqrt{2}$, che non sono reali e quindi non appartengono ad E ; naturalmente il detto automorfismo di K/F estende, come sempre, ad un automorfismo dell'intero campo di spezzamento di $x^4 - 2$ su F , solo che tali estensioni non mandano E in E .) La mappa restrizione $\text{Gal}(E/F) \rightarrow \text{Gal}(K/F)$ è l'omomorfismo banale, e quindi il suo nucleo $\text{Gal}(E/K)$ coincide con $\text{Gal}(E/F)$.

L'esempio mostra anche che componendo due estensioni normali non si ottiene necessariamente un'estensione normale. (Analogamente nei gruppi, la relazione "essere sottogruppo normale di" non è transitiva.)

6.4. Altri esercizi

ESERCIZIO 20. (UN PO' LABORIOSO) Determinate il campo di spezzamento di $x^4 - 2$ su \mathbf{Q} , costruite i campi ed i sottogruppi intermedi, determinando quelli normali (su \mathbf{Q} , e rispettivamente nel gruppo di Galois), e determinate esplicitamente la corrispondenza di Galois.

(*Suggerimento:* L'esercizio è simile agli esercizi sul campo di spezzamento di $x^3 - 2$ e di $x^5 - 2$ su \mathbf{Q} . Il gruppo di Galois G è un gruppo diedrale di ordine 8 (il gruppo delle simmetrie di un quadrato). La struttura dei sottogruppi è un po' più complicata dei casi già visti: ci sono tre sottogruppi (necessariamente normali) di ordine 4, uno dei quali è ciclico (le rotazioni del quadrato) e quindi contiene un unico sottogruppo di ordine 2, che poi risulta essere normale in G ; G ha inoltre altri quattro sottogruppi di ordine 2, (nessuno normale).)

ESERCIZIO 21. Questo è un po' difficile, ma uno studente coraggioso può provarlo. Calcolare campo di spezzamento e relativo gruppo di Galois su \mathbf{Q} di $x^8 - 2$, $x^8 + 2$ e di $x^8 - 3$. C'è una differenza ...

Equazioni risolubili per radicali

7.1. Caratteristica zero

In questo capitolo supporremo (quando non affermato esplicitamente il contrario) che la caratteristica sia zero. Dunque tutte le estensioni sono separabili, e normale equivale a campo di spezzamento. Si può fare di meglio, vedi ad esempio [Kap95] o [vdW71, vdW91].

Vogliamo caratterizzare quelle equazioni

$$(7.1.1) \quad x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$$

le cui soluzioni si possano ottenere a partire dai coefficienti a_i mediante formule in cui compaiano le *quattro operazioni* (cioè somma, prodotto, sottrazione e divisione un elemento $\neq 0$, che si possono fare in un campo), più *estrazioni di radice*.

7.2. L'equazione di secondo grado

Per esempio sappiamo che l'equazione di secondo grado $x^2 + a_1x + a_0 = 0$ ha soluzioni

$$(7.2.1) \quad x = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_0}}{2},$$

ove occorre solo notare che la formula non ha senso se la caratteristica è 2. Vale la pena di ricordare la dimostrazione, che si fa “completando il quadrato”. L'idea è di cercare di completare i termini $x^2 + a_1x$ al quadrato di qualcosa della forma $(x + b)^2 = x^2 + 2bx + b^2$. Dovremo quindi scegliere $2b = a_1$, o $b = a_1/2$. Dunque

$$x^2 + a_1x + a_0 = x^2 + 2\frac{a_1}{2}x + \left(\frac{a_1}{2}\right)^2 - \left(\frac{a_1}{2}\right)^2 + a_0,$$

dove abbiamo “aggiunto e tolto” il quadrato $b^2 = (a_1/2)^2$. Otteniamo

$$0 = x^2 + a_1x + a_0 = \left(x + \frac{a_1}{2}\right)^2 - \frac{a_1^2}{4} + a_0 = \left(x + \frac{a_1}{2}\right)^2 - \frac{a_1^2 - 4a_0}{4},$$

che ha quindi per soluzione

$$\left(x + \frac{a_1}{2}\right)^2 = \frac{a_1^2 - 4a_0}{4}, \quad \text{ovvero} \quad x = -\frac{a_1}{2} \pm \sqrt{\frac{a_1^2 - 4a_0}{4}},$$

che si riduce subito a (7.2.1).

7.3. Eliminare un coefficiente

In realtà questo ragionamento ha una portata più generale. Supponiamo di voler trovare una formula per le soluzioni dell'equazione (7.1.1) in termini dei coefficienti, sul modello di quella (7.2.1) per l'equazione di secondo grado. Sia F il campo da cui partiamo, sia E/F il campo di spezzamento, e siano $\alpha_1, \alpha_2, \dots, \alpha_n \in E$ le radici. Come abbiamo visto nella dimostrazione del Teorema 4.1.1, abbiamo

$$-a_{n-1} = \alpha_1 + \alpha_2 + \dots + \alpha_n.$$

Facciamo la sostituzione

$$(7.3.1) \quad x = y - \frac{a_{n-1}}{n}, \quad \text{ovvero,} \quad y = x + \frac{a_{n-1}}{n},$$

in (7.1.1). Otteniamo un'equazione

$$y^n + b_{n-1}y^{n-1} + \dots + b_1y + b_0 = 0,$$

le cui soluzioni sono, tenendo conto di (7.3.1), i numeri

$$\beta_i = \alpha_i + \frac{a_{n-1}}{n}.$$

Ne segue che

$$\begin{aligned} -b_{n-1} &= -\beta_1 - \beta_2 - \dots - \beta_n \\ &= \alpha_1 - \frac{a_{n-1}}{n} + \dots + \alpha_n - \frac{a_{n-1}}{n} \\ &= a_{n-1} - n \cdot \frac{a_{n-1}}{n} = 0. \end{aligned}$$

Dunque con la sostituzione (7.3.1) si può sempre supporre che in un'equazione di grado n il coefficiente di x^{n-1} sia zero.

7.4. Estensioni radicali e gruppi risolubili

Appare sensata la seguente definizione. Una estensione E/F si dice *radicale* se esistono $\alpha_1, \dots, \alpha_n \in E$ tali che $E = F(\alpha_1, \dots, \alpha_k)$, ed interi $n_i \geq 1$ tali che per ogni i

$$\alpha_i^{n_i} \in F(\alpha_1, \dots, \alpha_{i-1}).$$

Qui se $i = 1$ si intende che il termine di destra è semplicemente F . Dunque α_i è algebrico su $F(\alpha_1, \dots, \alpha_{i-1})$, dato che è radice del polinomio

$$f_i(x) = x^{n_i} - \alpha_i^{n_i} \in F(\alpha_1, \dots, \alpha_{i-1})[x].$$

Quindi l'estensione E/F è di grado finito.

Vale la pena notare che inserendo ulteriori elementi si può sempre supporre che gli n_i siano numeri primi. Ad esempio, se ho che $\alpha_1^6 \in F$, posso inserire $\beta = \alpha_1^2$, in modo che $\alpha_1^2 \in F(\beta)$, e $\beta^3 = \alpha_1^6 \in F$.

Come è fatto il gruppo di Galois di una estensione radicale e *normale*? (Vedremo tra poco perché quest'ultima affermazione non è restrittiva.) Supponiamo per ora per semplicità che tutte le radici $(n_1 \cdot n_2 \cdot \dots \cdot n_k)$ -sime dell'unità siano in F . Ora le radici del polinomio $f_1(x)$ sono $\alpha_1\omega$, al variare di ω nell'insieme delle radici n_1 -sime dell'unità. Tutte queste radici sono quindi in $F(\alpha_1)$. Ne segue che

$F(\alpha_1)$ è il campo di spezzamento su F del polinomio f_1 . Come è fatto il gruppo di Galois $\text{Gal}(F(\alpha_1)/F)$?

LEMMA 7.4.1. *Sia $L = F(\alpha)$ un'estensione di F , con $\alpha^n \in F$. Supponiamo che F contenga le radici n -sime dell'unità. Allora $\text{Gal}(L/F)$ è abeliano.*

DIMOSTRAZIONE. Come sopra α è radice di $x^n - \alpha^n \in F[x]$, e le radici di questo polinomio sono della forma $\alpha\omega$, con $\omega \in F$ una radice n -sima dell'unità. Un elemento $g \in G = \text{Gal}(L/F)$ è completamente determinato da αg , che per le solite ragioni è della forma $\alpha\omega$, e quindi è determinato da ω . Siano $g_1, g_2 \in G$, con $\alpha g_i = \alpha\omega_i$. Abbiamo

$$\alpha(g_1g_2) = (\alpha g_1)g_2 = (\alpha\omega_1)g_2 = (\alpha g_2)\omega_1 = \alpha\omega_2\omega_1 = \alpha\omega_1\omega_2 = \cdots = \alpha(g_2g_1),$$

e quindi $g_1g_2 = g_2g_1$, e G è abeliano. \square

Tornando alla nostra discussione, abbiamo scoperto che $\text{Gal}(F(\alpha_1)/F)$ è abeliano. D'altra parte $F(\alpha_1)/F$ è normale, dunque $F(\alpha_1)' = \text{Gal}(E/F(\alpha_1))$ è un sottogruppo normale di $\text{Gal}(E/F)$, e

$$\frac{\text{Gal}(E/F)}{\text{Gal}(E/F(\alpha_1))} = \text{Gal}(F(\alpha_1)/F).$$

Quindi $G = \text{Gal}(E/F)$ ha un sottogruppo normale $N = \text{Gal}(E/F(\alpha_1))$ tale che il quoziente G/N è abeliano. ora l'estensione $E/F(\alpha_1)$ è ancora radicale, per cui $N = \text{Gal}(E/F(\alpha_1))$ gode della stessa proprietà. Abbiamo ottenuto il seguente risultato provvisorio.

LEMMA 7.4.2. *Sia E/F un'estensione normale e radicale. Supponiamo che F contenga le radici dell'unità necessarie, come descritto sopra, e sia $G = \text{Gal}(E/F)$.*

Allora esistono sottogruppi $G = N_0 \geq N_1 \geq N_2 \geq \cdots \geq N_{k-1} \geq N_k = \{1\}$ tali che ogni N_{i+1} è normale in N_i , e il quoziente N_i/N_{i+1} è abeliano.

Dato il contesto, un gruppo con questa proprietà si dice *risolubile*.

Occorre sottolineare il fatto che se M/F è una estensione radicale, allora la sua chiusura normale L/F è ancora una estensione radicale. (Ricordiamo che siamo in caratteristica zero, e dunque ogni estensione è automaticamente separabile). Questo segue dall'argomento in coda alla sezione 5.1 – dovrei espanderlo un tantino.

Dato un polinomio monico non costante $f \in F[x]$, l'equazione corrispondente è $f(x) = 0$. Sia E/F un campo di spezzamento di f su F . Il gruppo di Galois di f su F (o dell'equazione corrispondente) è $\text{Gal}(E/F)$. L'equazione si dice risolubile per radicali se $E \subseteq M$, ove M/F è una estensione radicale. Vale allora

TEOREMA 7.4.3. *Sia $f \in F[x]$ monico non costante, E/F il suo campo di spezzamento. Se $f = 0$ è risolubile per radicali, allora $\text{Gal}(E/F)$ è risolubile.*

Occorre prima notare il seguente Lemma, senza dimostrazione

LEMMA 7.4.4 (Proprietà dei gruppi risolubili). 1. *Se un gruppo è risolubile, allora lo sono anche i suoi sottogruppi e i suoi gruppi quoziente.*

2. Se un gruppo G ha un sottogruppo normale N tale che N e G/N sono risolubili, allora G è risolubile.

Cominciamo per il momento a supporre che F contenga le radici dell'unità che ci servono per poter applicare il Lemma 7.4.1.

Allora, per dimostrare il Teorema 7.4.3 basta passare da M alla sua chiusura normale N su F . Ora E/F è normale, come campo di spezzamento (in caratteristica zero), dunque E è stabile rispetto a N/F , e il gruppo $\text{Gal}(E/F)$ è un quoziente di $\text{Gal}(N/F)$. Quest'ultimo è risolubile, e quindi lo è anche il primo, per il Lemma appena visto.

7.5. Un commento

Quando diciamo di supporre che F contenga tutte le radici n -esime dell'unità, dove $n = n_1 n_2 \cdots n_k$, intendiamo in generale che $x^n - 1$ si spezza in un prodotto di fattori lineari in $F[x]$; poi, avendo supposto di essere in caratteristica zero, $x^n - 1$ ha radici distinte per il criterio della derivata, e quindi le radici n -esime dell'unità in F sono in numero di n . D'altra parte, non è difficile vedere che in caratteristica $p > 0$ il numero di radici n -esime dell'unità distinte in un campo "che le contenga tutte", cioè in un campo di spezzamento per $x^n - 1$, è il più grande divisore m di n che non sia multiplo di p (cioè $n = m \cdot p^a$ con $p \nmid m$); infatti $x^n - 1 = (x^m - 1)^{p^a}$, e $x^m - 1$ ha radici distinte.

Nelle ipotesi del Lemma 7.4.1, ci vuol poco a concludere che $\text{Gal}(L/F)$ è addirittura ciclico, di ordine un divisore di n . Per vederlo, consideriamo l'insieme U delle radici n -esime dell'unità in F , che è un gruppo ciclico rispetto alla moltiplicazione, ed ha ordine n , avendo supposto di essere in caratteristica zero (ma in ogni caso ha ordine un divisore di N , come visto). Abbiamo visto che (supponendo di non essere nel caso banale $\alpha = 0$), ad ogni $g \in \text{Gal}(L/F)$ possiamo associare una radice dell'unità $\omega \in U$ (individuata in modo unico come $\alpha g/\alpha$): essendo $\alpha g_1 g_2 = \alpha \omega_1 \omega_2$, la mappa $g \mapsto \omega$ è un omomorfismo, ovviamente iniettivo, e quindi un isomorfismo, di $\text{Gal}(L/F)$ in U .

Di conseguenza, Nel Lemma 7.4.2 possiamo addirittura concludere che G ha una serie di sottogruppi N_i come descritta, con ciascun N_{i+1} normale in N_i , ed a quozienti N_i/N_{i+1} ciclici; anzi, grazie ad un'osservazione precedente, possiamo assumerli ciclici di ordine primo. Comunque, l'esistenza di una tale serie di sottogruppi a quozienti di ordine primo equivale ancora all'essere G risolubile (cioè all'esistenza di una serie a quozienti abeliani). (L'unico suo vantaggio è che la verifica che un gruppo G sia risolubile si può fare evitando di considerare i gruppi quoziente N_i/N_{i+1} , basta trovare una serie N_i con ciascun N_{i+1} normale in N_i e con indici $|N_i : N_{i+1}|$ primi.)

ESERCIZIO 22. Verificate che i gruppi simmetrici S_3 ed S_4 sono risolubili, trovando per ciascuno di essi:

1. una serie a quozienti abeliani;
2. una serie a quozienti ciclici di ordine primo.

Ancora riguardo al Lemma 7.4.1, l'ipotesi che E/F sia normale è superflua. Infatti se non lo è, E/K è comunque normale, dove $K = F'' = \mathbf{Inv}(\text{Gal}(E/F)) \supseteq$

F , rimane ovviamente radicale, e quindi $\text{Gal}(E/K)$ è risolubile grazie al Lemma; ma $\text{Gal}(E/F) = \text{Gal}(E/K)$.

Ecco, in breve, come mostrare che la chiusura normale N/F di un'estensione radicale M/F è anch'essa radicale. Sappiamo dalla fine del Capitolo 5 che N è generato su F dai vari *coniugati* Mg di M , al variare di $g \in \text{Gal}(N/F)$. Quindi se $M = F(\alpha_1, \dots, \alpha_k)$ con $\alpha_i^{n_i} \in F(\alpha_1, \dots, \alpha_{i-1})$ per ogni i , e $\text{Gal}(N/F) = \{g_1, \dots, g_n\}$ avremo che $N = F(\alpha_1 g_1, \dots, \alpha_k g_1; \dots; \alpha_1 g_n, \dots, \alpha_k g_n)$ è chiaramente anch'essa un'estensione radicale di F . Notiamo anche che gli interi n_i che servono per esibirla come estensione radicale di F sono gli stessi che servivano per esibire M come estensione radicale di F . (La rilevanza di quest'ultimo punto è che se F contiene le radici dell'unità che conviene avere per trattare l'estensione radicale M/F , queste bastano anche per trattare la sua chiusura normale N/F .)

7.6. E se non ci sono le radici dell'unità?

Se invece in F non ci sono le radici dell'unità, per poter dimostrare il Teorema 7.4.3 occorre appena un po' più lavoro. Intanto l'argomento appena visto ci riduce a dimostrare che il gruppo di Galois di una estensione radicale e normale N/F sia risolubile. Sia

$$N = F(\alpha_1, \dots, \alpha_k),$$

con $\alpha_i^{p_i} \in F(\alpha_1, \dots, \alpha_{i-1})$, per opportuni primi p_i , e supponiamo che k sia il numero più piccolo per cui possiamo fare una cosa del genere. Procederemo per induzione su k .

Consideriamo una radice p_1 -sima primitiva ω dell'unità. Scriviamo $p = p_1$, e $\alpha = \alpha_1$. Consideriamo i campi della Figura 1.

Se facciamo vedere che $\text{Gal}(N(\omega)/F)$ è risolubile, lo sarà anche $\text{Gal}(N/F)$, che ne è immagine omomorfa.

Ora l'estensione $F(\omega)/F$ è normale. Se facciamo vedere che il suo gruppo di Galois è abeliano, allora basta vedere che $\text{Gal}(N(\omega)/F(\omega))$ è risolubile, perché allora lo sarà anche $\text{Gal}(N(\omega)/F)$, per il Lemma 7.4.4, dato che

$$\frac{\text{Gal}(N(\omega)/F)}{\text{Gal}(N(\omega)/F(\omega))} \cong \text{Gal}(F(\omega)/F).$$

Serve il

LEMMA 7.6.1. *Sia ω è un radice primitiva n -sima dell'unità su F . Allora $\text{Gal}(F(\omega)/F)$ è abeliano.*

DIMOSTRAZIONE. Un elemento $g \in \text{Gal}(F(\omega)/F)$ manda ω in un'altra radice n -sima dell'unità, dunque in un ω^i . Un altro $h \in \text{Gal}(F(\omega)/F)$ manda ω in ω^j . Dunque

$$\omega gh = (\omega^i)h = (\omega h)^i = \omega^{ji},$$

e naturalmente $\omega hg = \omega^{ij} = \omega gh$, per cui $gh = hg$. \square

Finalmente dobbiamo mostrare che $\text{Gal}(N(\omega)/F(\omega))$ è risolubile. Notiamo che $F(\omega, \alpha)/F(\omega)$ è una estensione normale, come campo di spezzamento di $x^n - \alpha^n$,

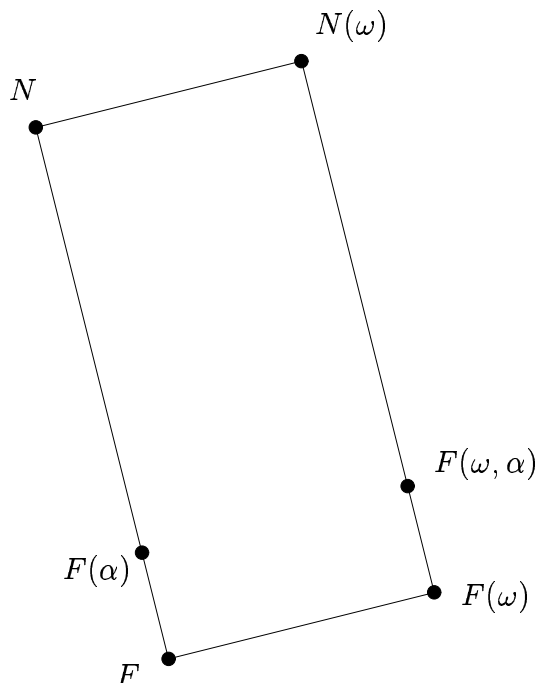


FIGURA 1. Aggiungere le radici

che ha lí tutte le sue radici $\alpha\omega^i$. Ma ora $\text{Gal}(F(\omega, \alpha)/F(\omega))$ è abeliano per 7.4.1. Quindi il problema è spostato sull'estensione normale e radicale $N(\omega)/F(\omega, \alpha)$, ma dato che

$$N(\omega) = F(\omega, \alpha)(\alpha_2, \dots, \alpha_k),$$

questa adesso ha $k - 1$ al posto di k , e quindi per l'induzione su k che avevamo preso all'inizio ha gruppo di Galois risolubile.

7.7. Un commento

Un po' piú di attenzione nella dimostrazione del Lemma 7.6.1 mostra che $\text{Gal}(F(\omega)/F)$ (dove ω è una radice n -esima primitiva dell'unità su F , cioè in un'opportuna estensione di F) è isomorfo ad un sottogruppo del gruppo $\text{Aut}(U)$ degli automorfismi del gruppo (ciclico) U delle radici n -esime dell'unità, infatti la mappa $g \mapsto g|_U$ (la restrizione ad U di un automorfismo di $F(\omega)/F$) è un omomorfismo di gruppi $\text{Gal}(F(\omega)/F) \rightarrow \text{Aut}(U)$, iniettivo perché ciascun $g \in \text{Gal}(F(\omega)/F)$ è determinato da come agisce su ω (o, in altre parole, perché U genera $F(\omega)$ su F).

Sappiamo inoltre che $\text{Aut}(U)$ è abeliano, essendo isomorfo al gruppo $U(\mathbf{Z}/n\mathbf{Z})$ degli elementi invertibili di $\mathbf{Z}/n\mathbf{Z}$. Un omomorfismo iniettivo di $\text{Gal}(F(\omega)/F)$ in $U(\mathbf{Z}/n\mathbf{Z})$ si può ottenere direttamente mandando g in $i + n\mathbf{Z}$, se $\omega g = \omega^i$.

Un fatto che non dimostreremo (e che non serve qui, ma gioca un ruolo nella teoria delle costruzioni dei poligoni regolari mediante riga e compasso) è che tale omomorfismo è un isomorfismo nel caso $F = \mathbf{Q}$. Il motivo è che $|\mathbf{Q}(\omega) : \mathbf{Q}| = \varphi(n)$, e quindi $|\text{Gal}(F(\omega)/F)| = \varphi(n) = |U(\mathbf{Z}/n\mathbf{Z})|$.

ESERCIZIO 23. Il *polinomio ciclotomico* $\lambda_n(x)$ è definito come

$$\lambda_n(x) = \prod_{0 \leq i < n, (i,n)=1} (x - \omega^i),$$

quindi è il polinomio monico che ha per radici le radici primitive n -esime (complesse) dell'unità. Mostrate che $\lambda_n(x)$ ha coefficienti razionali, e quindi il polinomio minimo di ω su \mathbf{Q} divide $\lambda_n(x)$.

In realtà si dimostra che il *polinomio ciclotomico* $\lambda_n(x)$ è irriducibile su \mathbf{Q} (cosa che già sapevamo nel caso in cui p è primo, avendola vista nel Capitolo 1 come applicazione del Criterio di Eisenstein), e quindi è il polinomio minimo di ω su \mathbf{Q} , da cui segue che $|\mathbf{Q}(\omega) : \mathbf{Q}| = \varphi(n)$, come affermato prima.

7.8. Un'equazione non risolubile per radicali

Possiamo ora esibire una equazione non risolubile per radicali.

Notiamo innanzitutto una cosa importante, che per la verità avevamo sostanzialmente già visto nel Capitolo 3. Sia $f \in F[x]$ un polinomio monico di grado $n > 0$. Sia E/F il campo di spezzamento, e $\alpha_1, \dots, \alpha_n \in E$ le radici di f . Allora, per argomenti già visti, gli elementi di $G = \text{Gal}(E/F)$ mandano ogni α_i in un α_j . Dunque G agisce sull'insieme $\Omega = \{\alpha_1, \dots, \alpha_n\}$. Dato che $E = F(\alpha_1, \dots, \alpha_n)$, l'azione di G su E è determinata dall'azione di G su Ω . Cioè la restrizione

$$G \rightarrow S_\Omega \cong S_n$$

è iniettiva. Ne segue che G è (isomorfo a) un sottogruppo di S_n .

Consideriamo ora il polinomio

$$f(x) = x^5 - 6x + 3 \in \mathbf{Q}[x],$$

e sia E/\mathbf{Q} il suo campo di spezzamento. Si vede subito, con un buon vecchio studio di funzioni, che f ha tre radici reali e due complesse, dunque coniugate fra loro. Ne segue che il coniugio sui complessi induce un 2-ciclo sull'insieme Ω delle radici di f . Il criterio di Eisenstein ci dice subito che f è irriducibile su F , dunque 5 divide $|E : \mathbf{Q}| = |\text{Gal}(E/\mathbf{Q})|$. Ora si ha il

LEMMA 7.8.1 (comunemente detto di Cauchy). *Se un gruppo finito ha ordine divisibile per un primo p , allora contiene un elemento di ordine p .*

DIMOSTRAZIONE. Sia G il gruppo in questione. Consideriamo l'insieme

$$B = A^p = \{ (a_0, a_1, \dots, a_{p-1}) : a_i \in G \}.$$

Sia S_p il gruppo delle permutazioni sull'insieme $\{0, 1, \dots, p-1\}$. Allora S_p agisce su B permutando gli indici. Consideriamo il p -ciclo $\sigma = (0, 1, 2, \dots, p-1)$, e il sottogruppo $H = \langle \sigma \rangle$ di S_p di ordine p da lui generato. Anche H dunque agisce su B .

Consideriamo ora il sottoinsieme di B dato da

$$A = \{ (a_0, a_1, \dots, a_{p-1}) : a_i \in G, a_0 \cdot a_1 \cdots a_{p-1} = 1 \}.$$

Se $(a_0, a_1, \dots, a_{p-1}) \in A$ si ha chiaramente $a_{p-1} = (a_0 \cdot a_1 \cdots a_{p-2})^{-1}$. Viceversa, scelti elementi arbitrari $a_0, a_1, \dots, a_{p-2} \in G$, si ha $(a_0, a_1, \dots, a_{p-2}, a_{p-1}) \in A$ per

$a_{p-1} = (a_0 \cdot a_1 \cdots a_{p-2})^{-1}$. Ne segue che A ha $|G|^{p-1}$ elementi, un numero divisibile per p .

Affermiamo che H continua ad agire su A . E' sufficiente vedere che σ mandi un elemento di A in un altro elemento di A . Abbiamo

$$(a_0, a_1, \dots, a_{p-1})\sigma = (a_1, a_2, \dots, a_{p-1}, a_0),$$

e in effetti se $(a_0, a_1, \dots, a_{p-1}) \in A$ abbiamo

$$a_1 \cdot a_2 \cdots a_{p-1} \cdot a_0 = a_0^{-1} \cdot (a_0 \cdot a_1 \cdot a_2 \cdots a_{p-1}) \cdot a_0 = a_0^{-1} \cdot 1 \cdot a_0 = 1,$$

e quindi anche $(a_1, a_2, \dots, a_{p-1}, a_0) \in A$.

Il teorema orbita-stabilizzatore ci dice che la lunghezza di ogni orbita di H su A divide l'ordine di H . Dato che H ha ordine p , un'orbita può essere lunga p o 1 . In quest'ultimo caso si deve avere in particolare

$$(a_0, a_1, \dots, a_{p-1}) = (a_0, a_1, \dots, a_{p-1})\sigma = (a_1, a_2, \dots, a_{p-1}, a_0),$$

e quindi $a_0 = a_1 = \cdots = a_{p-1} = a$ per un certo a . Dato che $(a, a, \dots, a) \in A$, dobbiamo avere $a^p = 1$, e quindi o $a = 1$, o a ha ordine p .

Sia n_1 il numero di orbite lunghe 1 , e n_p il numero di orbite lunghe p . Contando gli elementi di A si ha

$$|A| = n_1 + p \cdot n_p.$$

Abbiamo visto che $|A|$ è divisibile per p , e lo stesso vale per $p \cdot n_p$. Dunque anche n_1 è divisibile per p . Ora $n_1 \geq 1$, dato che $(1, 1, \dots, 1) \in A$. Dunque $n_1 \geq p$, e ogni elemento $a \neq 1$ tale che $(a, a, \dots, a) \in A$ è un elemento di ordine p . \square

Dunque $\text{Gal}(E/\mathbf{Q})$ contiene un 2-ciclo e un elemento di ordine 5 . Ma si ha

LEMMA 7.8.2. *Se un sottogruppo di S_p , p un primo, contiene un elemento di ordine p e un 2-ciclo, allora è tutto S_p .*

DIMOSTRAZIONE. Il 2-ciclo possiamo supporre sia $\tau = (1, 2)$. Il p -ciclo sarà della forma

$$\sigma = (1, a_2, a_3, \dots, a_p).$$

Supponiamo sia $a_{k+1} = 2$. Allora si ha $\sigma^k = (1, 2, \dots)$, e σ^k è ancora un p -ciclo. Si può dunque supporre

$$\sigma = (1, 2, 3, \dots, p).$$

Ora $\tau^\sigma = (2, 3)$, e continuando si ottengono tutti i 2-cicli $(i, i+1)$. (Quando si trova $p+1$ si intende 1 .) A questo punto si vede che $(1, 2)^{(2,3)} = (1, 3)$, e poi $(1, 3)^{(3,4)} = (1, 4)$. Continuando si ottengono tutti i 2-cicli $(1, i)$, e quindi il generico 2-ciclo $(i, j) = (1, j)^{(1,i)}$. Poi si sa che ogni permutazione è prodotto di 2-cicli. \square

7.9. Un commento

Chiaramente la nostra discussione dipende solo da una proprietà specifica del polinomio irriducibile $x^5 - 6x + 3$: qualsiasi polinomio di quinto grado irriducibile su \mathbf{Q} e *con esattamente due radici reali* ha S_5 come gruppo di Galois.

ESERCIZIO 24. Supponete per semplicità che il polinomio $f(x) = x^5 + ax + b \in \mathbf{R}[x]$ abbia radici distinte. Usando strumenti tipici degli “studi di funzioni” (massimi e minimi, usando f') mostrate che

1. il polinomio f non può avere cinque radici reali;
2. se $f(x)$ ha tre radici reali, allora $a < 0$ (il che sarà conseguenza del punto successivo, ma fate anche questo come passo intermedio);
3. f ha esattamente tre radici reali se e solo se $4^4 a^5 + 5^5 b^4 < 0$.

La quantità $4^4 a^5 + 5^5 b^4$ è il *discriminante* del polinomio f (o dell'equazione $f(x) = 0$), che sarà discusso nel prossimo Capitolo.

ESERCIZIO 25. Utilizzando il risultato dell'esercizio precedente, costruite almeno un paio di altri esempi (ancor meglio infiniti) di polinomi della forma $f(x) = x^5 + ax + b \in \mathbf{Q}[x]$ che abbiano S_5 come gruppo di Galois, e la cui irriducibilità su \mathbf{Q} si possa mostrare mediante il Criterio di Eisenstein.

C'è una dimostrazione del Piccolo Teorema di Fermat $a^p \equiv a \pmod{p}$ (per p primo ed a intero, che possiamo tranquillamente assumere positivo) simile alla dimostrazione del Lemma di Cauchy (anzi, leggermente più semplice). Se Ω un insieme di n oggetti, allora il gruppo ciclico H di ordine p agisce su $B = \Omega^p = \{(\omega_0, \dots, \omega_{p-1}) : \omega_i \in \Omega\}$ come descritto nella dimostrazione del Lemma, permutando le componenti. In questo caso ci sono esattamente a punti fissi (cioè orbite di lunghezza p), mentre $|B| = a^p$. Poiché ogni altra orbita ha ordine un multiplo di p , segue la tesi.

La parte di dimostrazione dopo il primo paragrafo mostra il seguente fatto più generale.

LEMMA 7.9.1. *Se un sottogruppo i S_n contiene $(1, 2)$ e $(1, 2, \dots, n)$, allora è tutto S_n . (In altre parole, S_n è generato da questi due elementi.)*

Notate che il 2-ciclo e l' n -ciclo nelle ipotesi del Lemma non si possono scegliere liberamente, infatti ad esempio $(1, 2, 3, 4)$ e $(1, 3)$ non generano tutto S_4 , bensì un sottogruppo di ordine 8 (un gruppo *diedrale*, il gruppo delle simmetrie di un quadrato, se ne numerate i vertici diciamo in senso antiorario).

7.10. Permutazioni pari e dispari, e gruppo alterno

Abbiamo già ricordato che ogni permutazione di S_n si può scrivere come prodotto di 2-cicli. Una stessa permutazione si può scrivere in più modi diversi come prodotto di 2-cicli, e da un modo all'altro anche il *numero* dei 2-cicli può cambiare. per esempio $(2, 3) = (1, 2)(1, 3)(1, 2)$. Si potrebbe però vedere che da un modo all'altro non cambia la *parità* del numero di 2-cicli che compaiono. In altre parole, se una permutazione si può scrivere come prodotto di un numero pari di

2-cicli, allora non si può scrivere come prodotto di un numero dispari di 2-cicli, e viceversa.

Diciamo che una permutazione è *pari* o *dispari* a seconda che il numero di 2-cicli che occorrono per scriverla sia pari o dispari. Si vede subito che il prodotto di due permutazioni pari, o di due dispari, è una permutazione pari, mentre il prodotto di una permutazione pari e di una dispari è una permutazione dispari. Dunque le permutazioni pari di S_n formano un sottogruppo, detto *gruppo alterno*, e denotato con A_n . Se poi $\sigma \in S_n \setminus A_n$, ovvero σ è una permutazione dispari, allora $(1, 2) \cdot \sigma$ è pari, dunque $(1, 2) \cdot \sigma \in A_n$, e $\sigma \in (1, 2)A_n$. Ne segue che $S_n \setminus A_n = (1, 2)A_n$. Quindi A_n ha indice 2 in S_n , e in particolare è un sottogruppo normale.

7.11. Il gruppo simmetrico su cinque elementi non è risolubile

A questo punto resta solo da vedere che S_5 non è risolubile. Ne seguirà che l'equazione

$$x^5 - 6x + 3 = 0$$

non è risolubile per radicali.

Faremo vedere che il gruppo alterno A_5 è semplice, cioè non ha altri sottogruppi normali che $\{1\}$ e tutto A_5 . Inoltre A_5 non è abeliano, dato che $(12)(45) \cdot (13)(45) = (123) \neq (132) = (13)(45) \cdot (12)(45)$. Adesso se S_5 fosse risolubile, anche A_5 dovrebbe esserlo, per il Lemma 7.4.4. Ma allora A_5 dovrebbe avere un sottogruppo normale abeliano diverso da $\{1\}$, il che non è.

Vediamo adesso che A_5 è semplice. Studieremo le sue classi di coniugio, e poi faremo vedere che i soli sottogruppi normali sono $\langle 1 \rangle$ e A_5 stesso.

Abbiamo forse già notato il seguente lemma, che descrive il coniugio in S_n :

LEMMA 7.11.1. *Sia $(i_1 i_2 \dots i_k)$ un ciclo in S_n , e $\sigma \in S_n$.*

Allora

$$(i_1 i_2 \dots i_k)^\sigma = \sigma^{-1}(i_1 i_2 \dots i_k)\sigma = (i_1^\sigma i_2^\sigma \dots i_k^\sigma).$$

Dunque due permutazioni in S_n sono coniugate in S_n se e solo se hanno la stessa *struttura ciclica*: ovvero lo stesso numero di cicli di una data lunghezza k , per ogni k . Ad esempio $(123)(45)$ e $(253)(14)$ sono coniugate sotto la permutazione che manda 1 in 2, 2 in 5, 3 in 3, 4 in 1 e 5 in 4, cioè sotto $\sigma = (1254)$.

Dunque è facile vedere le classi di coniugio in S_5 :

x	Num. con. x	$ C_{S_5}(x) $
1	1	120
(1 2)	10	12
(1 2 3)	20	6
(1 2 3 4)	30	4
(1 2 3 4 5)	24	5
(1 2) (3 4)	15	8
(1 2 3) (4 5)	20	6

Qui la prima colonna indica un elemento rappresentativo x per ogni possibile struttura ciclica. La seconda indica il numero di elementi con quella struttura

ciclica, e quindi il numero di elementi della classe di coniugio x^{S_5} di x in S_5 . Nella terza colonna c'è l'ordine del centralizzante di x in S_5 , che per il teorema orbita stabilizzatore deve soddisfare

$$|S_5| = |x^G| \cdot |C_{S_5}(x)|.$$

Il numero di elementi di x^G si calcola come negli esempi che seguono. Per calcolare il numero dei coniugati di (12), cioè dei 2-cicli (ij) , con $i \neq j$, si nota che ci sono 5 possibilità per i e 4 per j . Dato che $(ij) = (ji)$, il totale è $5 \cdot 4/2 = 10$. Invece coi 3-cicli si calcola $5 \cdot 4 \cdot 3/3$, dato che $(ijk) = (jki) = (kij)$. Nel caso del prodotto di due 2-cicli disgiunti, si nota che $(ij)(kl) = (kl)(ij)$, per cui il calcolo è

$$\frac{5 \cdot 4}{2} \cdot \frac{3 \cdot 2}{2} = 15.$$

Quando vado a vedere le classi di coniugio di A_5 , devo incominciare a guardare solo le permutazioni pari, cioè 1, (123), (12345), (12)(34).

Premettiamo il seguente Lemma

LEMMA 7.11.2. *Sia G un gruppo finito, $H, K \leq G$. Consideriamo l'insieme HK . Sia ha*

$$|HK| = \frac{|H| |K|}{|H \cap K|}.$$

In particolare, se HK è un sottogruppo, allora

$$|HK : K| = |H : H \cap K|.$$

DIMOSTRAZIONE. L'insieme HK è unione di classi laterali di K rispetto a H :

$$HK = \bigcup_{h \in H} hK.$$

Si tratta di vedere quando sono eguali due classi. Si ha $h_1K = h_2K$ se e solo se $h_1^{-1}h_2 \in K$, e dunque $h_1^{-1}h_2 \in H \cap K$. Questa è la stessa relazione che da le classi laterali di $H \cap K$ in H , dunque

$$\frac{|HK|}{|K|} = |H : H \cap K| = \frac{|H|}{|H \cap K|}.$$

□

Ora dimostriamo

LEMMA 7.11.3. *Il gruppo finito G agisca sull'insieme finito Ω . Sia H un sottogruppo di G di indice 2.*

Sia $\alpha \in \Omega$. Si ha

$$|\alpha^H| = \begin{cases} \frac{1}{2} \cdot |\alpha^G| & \text{se } \text{Stab}_G(\alpha) \leq H, \\ |\alpha^G| & \text{altrimenti.} \end{cases}$$

DIMOSTRAZIONE. Abbiamo

$$\begin{aligned} |\alpha^H| &= |H : \text{Stab}_H(\alpha)| \\ &= |H : H \cap \text{Stab}_G(\alpha)| \\ &= \frac{|H|}{|H \cap \text{Stab}_G(\alpha)|} \\ &= \frac{|H \text{Stab}_G(\alpha)|}{|\text{Stab}_G(\alpha)|}. \end{aligned}$$

Ora se $\text{Stab}_G(\alpha) \leq H$ questo ordine è

$$|H : \text{Stab}_G(\alpha)| = \frac{|G : \text{Stab}_G(\alpha)|}{|G : H|} = \frac{1}{2} \cdot |\alpha^G|,$$

mentre se $\text{Stab}_G(\alpha) \not\leq H$, allora $H \text{Stab}_G(\alpha) = G$, dato che H ha indice 2 in G , e quindi $|\alpha^H| = |G : \text{Stab}_G(\alpha)| = |\alpha^G|$. \square

Dunque le classi di coniugio di elementi x di A_5 sono le stesse che in S_5 , tranne quando $C_{S_5}(x) \leq A_5$. Ora sapere l'ordine di questi centralizzanti ci aiuta a sapere chi sono. E in effetti (123) è centralizzato dalla permutazione dispari (45), mentre (12)(34) è centralizzato dalla permutazione dispari (1324) (basta notare che $(1324)^2 = (12)(34)$). Invece il centralizzante di (12345) ha ordine 5, e dunque

$$C_{S_5}((12345)) = \langle (12345) \rangle \leq A_5.$$

Dunque la classe di coniugio di (12345) in S_5 si spezza in due in A_5 , e abbiamo la tabella delle classi di coniugio di A_5

x	Num. con. x	$ C_{A_5}(x) $
1	1	60
(1 2 3)	20	3
(1 2 3 4 5)	12	5
(1 3 5 2 4)	12	5
(1 2) (3 4)	15	4

Si noti che in effetti $x = (12345)$ e (13524) non sono coniugati in A_5 , perché sono coniugati sotto la permutazione dispari (2354), e ogni altra permutazione che li coniughi è nella classe laterale $C_{S_5}(x) \cdot (2354)$, che è fatta tutta di permutazioni dispari, dato che tutti gli elementi di $C_{S_5}(x)$ sono permutazioni pari.

Adesso se N è un sottogruppo normale di A_5 diverso da $\langle 1 \rangle$, dovrà essere unione disgiunta di alcune delle classi di coniugio, inclusa $\langle 1 \rangle$. Ma si vede facilmente che non si possono raggruppare i numeri di elementi delle classi per formare un divisore di 60 diverso da 60 stesso. Dunque A_5 è semplice.

7.12. Un commento

Nella dimostrazione del Lemma 7.11.3 è possibile evitare il ricorso al Lemma 7.11.2, per quanto esso sia fondamentale, nel modo seguente.

Se $\text{Stab}_G(\alpha) \leq H$, allora $\text{Stab}_H(\alpha) = \text{Stab}_G(\alpha)$, da cui $|\alpha^G| = |G : \text{Stab}_G(\alpha)| = |G : H| |H : \text{Stab}_H(\alpha)| = 2|\alpha^H|$.

Se invece $\text{Stab}_G(\alpha) \not\leq H$, allora $\text{Stab}_H(\alpha) = H \cap \text{Stab}_G(\alpha) < \text{Stab}_G(\alpha)$, e quindi $\text{Stab}_H(\alpha)$ ha indice almeno 2 in $\text{Stab}_G(\alpha)$. (A questo punto il Lemma 7.11.2 permetterebbe di concludere che è *esattamente* 2.) Dunque $2|\text{Stab}_H(\alpha)| \leq |\text{Stab}_G(\alpha)|$, da cui $|\alpha^H| = |H : \text{Stab}_H(\alpha)| = |G : \text{Stab}_H(\alpha)|/2 \geq |G : \text{Stab}_G(\alpha)| \geq |\alpha^G|$, e quindi $|\alpha^H| = |\alpha^G|$.

ESERCIZIO 26. Determinate le lunghezze delle classi di coniugio di S_4 e concludete, in modo analogo al ragionamento fatto per A_5 , che i soli sottogruppi normali di S_4 sono 1 , $V_4 = \{1, (12)(34), (13)(24), (14)(23)\}$, A_4 e S_4 .

Ora fate lo stesso per A_4 . (Notate che non si riduce a quanto già fatto per S_4 , perché a priori non è detto che un sottogruppo normale di A_4 sia normale in S_4 . Ad esempio, quali sono i sottogruppi normali di V_4 ?)

Per concludere: trovate *tutte* le serie $S_4 = N_0 > N_1 > \dots > N_k = 1$ (con ogni N_i normale nel precedente e) a quozienti di ordine primo; trovate *tutte* le serie $S_4 = N_0 > N_1 > \dots > N_k = 1$ a quozienti abeliani e con ogni N_i normale in S_4 .

7.13. L'equazione generale di n -simo grado

Cominciamo col seguente

LEMMA 7.13.1. *Sia E un campo. Sia G un gruppo finito di automorfismi di E . Sia F il sottocampo di E degli elementi fissati da G . Allora E/F è una estensione normale, e $\text{Gal}(E/F) = G$.*

DIMOSTRAZIONE. Intanto notiamo che G si può considerare come un sottogruppo di $\text{Gal}(E/K)$, dove K è il campo primo.

E' chiaro che $\text{Gal}(E/F) \geq G$. Per i soliti lemmi, abbiamo $|G| \geq |E : F| \geq |\text{Gal}(E/F)| \geq |G|$, e dunque si ottiene che tutti i numeri sono eguali. In particolare $|E : F| = |\text{Gal}(E/F)|$, e quindi E/F è normale. \square

Consideriamo adesso un campo K , e il campo $E = K(t_1, t_2, \dots, t_n)$ delle funzioni razionali. Su E agisce in modo naturale come gruppo di automorfismo il gruppo simmetrico $G = S_n$, permutando gli indici. Il campo F degli elementi fissati da S_n è detto il campo delle funzioni razionali simmetriche, dato che non cambiano se permuti fra loro le variabili t_1, t_2, \dots, t_n . Si ha quindi $|E : F| = |S_n| = n!$.

Consideriamo adesso il polinomio

$$\begin{aligned} f(x) &= (x - t_1) \cdot (x - t_2) \cdot \dots \cdot (x - t_n) \\ &= x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} + (-1)^{n-1} \sigma_{n-1} x + (-1)^n \sigma_n. \end{aligned}$$

Qui σ_i è la i -sima funzione simmetrica elementare nei t_1, t_2, \dots, t_n , ovvero la somma di tutti i prodotti di i elementi distinti fra essi. Ad esempio

$$\sigma_1 = t_1 + t_2 + \dots + t_n, \quad \sigma_n = t_1 t_2 \dots t_n.$$

Dunque $f(x) \in L[x]$, ove $L = K(\sigma_1, \sigma_2, \dots, \sigma_n) \subseteq F$, ed E è il campo di spezzamento di f su L . Per l'Esercizio 10, si ha $n! = |E : F| \leq |E : L| \leq n!$, e dunque $F = L$. Ne segue l'importante

TEOREMA 7.13.2. *Ogni funzione razionale simmetrica è una funzione razionale delle funzioni simmetriche elementari.*

Un risultato analogo varrebbe per i polinomi: si veda ad esempio [Jac85].

L'equazione $f(x) = 0$ viene detta *equazione generale di n -simo grado*, dato che ogni equazione di n -simo grado si ottiene attribuendo valori particolari ai t_i . (Qui ci sarebbe da fare un discorso *molto* più preciso sul concetto di *specializzazione*, ma preferisco ometterlo completamente.) Abbiamo visto che il suo gruppo di Galois è S_n . Per $n \geq 5$, abbiamo $S_5 \leq S_n$. Abbiamo visto che S_5 non è risolubile, per cui neanche S_n lo è. Ne segue che l'equazione generale di n -simo grado non è risolubile per radicali, per $n \geq 5$.

Vedremo invece che le equazioni di grado tre e quattro sono risolubili per radicali, dato che S_3 e S_4 sono gruppi risolubili. Per la verità per ora garantisco solo la dimostrazione per quanto riguarda l'equazione di terzo grado, anche se poi il più è fatto anche per quella di quarto.

7.14. Un commento

Un commento al senso dell'*equazione generale di grado n* . L'esempio esplicito di $x^5 - 6x + 3 = 0$ mostra che non può esistere una *formula risolutiva generale* in termini di operazioni razionali e radicali per l'equazione generica di grado 5 a coefficienti razionali. In realtà esso mostra che non può esistere una tale formula per alcuna equazione di grado $n \geq 5$ a coefficienti razionali: infatti se esistesse si dovrebbe poter applicare all'equazione $x^{n+5} - 6x^{n+1} + 3x^n = 0$.

Ma nulla ci dice riguardo all'esistenza o meno di una formula risolutiva generale per equazioni su campi diversi da \mathbf{Q} . Ad esempio, qualsiasi equazione a coefficienti *reali* (fissati!) è certamente risolubile per radicali nel senso della nostra definizione, in quanto un campo di spezzamento è contenuto in \mathbf{C} (sarà \mathbf{R} o \mathbf{C}), e l'estensione \mathbf{C}/\mathbf{R} è certamente radicale! Ciò significa soltanto che ogni numero complesso si può esprimere a partire da opportuni numeri reali usando solo operazioni razionali ed estrazioni di radici, una banalità, visto che basta un'unica radice, ad esempio $i = \sqrt{-1}$. Questo ci mostra che la nostra definizione di risolubilità per radicali è quanto meno ingannevole.

L'esistenza o meno di una formula risolutiva generale nel senso comune dell'espressione, in termini di operazioni razionali e radicali, equivale invece al fatto che un'equazione a *coefficienti indeterminati* sia risolubile per radicali nel senso della nostra definizione.

ESERCIZIO 27. Mostrate che ogni estensione E/F con E un campo finito è radicale. Significa che esiste una formula generale per l'equazione di grado n a coefficienti in un campo finito, ad esempio in \mathbb{F}_p ?

7.15. Determinante di Vandermonde

La formula seguente è spesso utile

LEMMA 7.15.1 (Determinante di Vandermonde).

$$(7.15.1) \quad \Delta(t_1, \dots, t_n) = \det \begin{bmatrix} 1 & 1 & \dots & 1 \\ t_1 & t_2 & \dots & t_n \\ t_1^2 & t_2^2 & \dots & t_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ t_1^{n-1} & t_2^{n-1} & \dots & t_n^{n-1} \end{bmatrix} = \prod_{1 \leq i < j \leq n} (t_j - t_i).$$

Qui i t_i possono essere per esempio indeterminate. L'espressione $\Delta(t_1, \dots, t_n)$ si dice *determinante di Vandermonde*.

DIMOSTRAZIONE. Si può fare una dimostrazione per induzione, i casi $n = 1, 2$ essendo ovvi. Consideriamo il polinomio

$$(7.15.2) \quad f(x) = \det \begin{bmatrix} 1 & 1 & \dots & 1 & 1 \\ t_1 & t_2 & \dots & t_{n-1} & x \\ t_1^2 & t_2^2 & \dots & t_{n-1}^2 & x^2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ t_1^{n-2} & t_2^{n-2} & \dots & t_{n-1}^{n-2} & x^{n-2} \\ t_1^{n-1} & t_2^{n-1} & \dots & t_{n-1}^{n-1} & x^{n-1} \end{bmatrix}$$

a coefficienti in $\mathbf{Z}[t_1, t_2, \dots, t_{n-1}]$. E' un polinomio di grado $n - 1$, che ha radici distinte t_1, t_2, \dots, t_{n-1} : infatti sostituendo $x = t_i$, per $1 \leq i < n$, si ottiene il determinante di una matrice con due colonne eguali, che è zero. Per la regola di Ruffini si ha

$$f(x) = C(x - t_1)(x - t_2) \dots (x - t_{n-1}).$$

Il coefficiente C si ricava facilmente da (7.15.2), dato che è il coefficiente di x^{n-1} , dunque il minore che si ottiene eliminando l'ultima riga e l'ultima colonna, che si vede subito essere un determinante di Vandermonde su una matrice $(n - 1) \times (n - 1)$. Ora $f(t_n)$ è proprio il determinante di Vandermonde, per cui si ottiene il risultato. \square

7.16. Un commento

Un altro modo di dimostrare il Lemma 7.15.1 sull'espressione del determinante di Vandermonde è il seguente: iniziando da $i = n$ e scendendo fino a $i = 2$, si sottrae alla i -esima riga della matrice la $(i - 1)$ -esima moltiplicata per t_1 ; raccogliendo da ciascuna colonna un opportuno fattore comune ai suoi elementi e sviluppando il determinante rispetto alla prima colonna si trova che $\Delta(t_1, \dots, t_n) = (t_n - t_1)(t_{n-1} - t_1) \dots (t_2 - t_1) \cdot \Delta(t_1, \dots, t_{n-1})$, da cui si conclude per induzione.

ESERCIZIO 28. Completate i dettagli della dimostrazione appena accennata.

7.17. Da gruppi risolubili a estensioni radicali

Vogliamo ora vedere che se il campo di spezzamento E su F di un polinomio $f(x) \in F[x]$ ha gruppo di Galois risolubile, allora E è contenuto in una estensione radicale di F .

Anche qui semplificheremo le cose supponendo che F contenga le radici dell'unità che ci serviranno lungo la strada. Questo farà sì che ci venga fuori addirittura che E/F è una estensione radicale, cosa che non è vera però quando le radici dell'unità non ci sono.

Se $G = \text{Gal}(E/F)$ è risolubile, avrà un sottogruppo normale $N < G$ tale che il quoziente G/N sia abeliano. Non sarebbe difficile convincersi che esiste un sottogruppo $M \leq N$ che è ancora normale, ed ha quoziente G/M di ordine un numero primo p . A questo punto, procedendo per induzione, basta dimostrare il seguente

LEMMA 7.17.1 (Risolvendi di Lagrange). *Sia K/F una estensione normale tale che il gruppo di Galois $\text{Gal}(K/F)$ sia ciclico di ordine p primo.*

Supponiamo che F contenga le radici p -sime dell'unità, e che esse siano distinte. (Quest'ultimo fatto è automatico sotto la nostra condizione generale che la caratteristica sia zero.)

Allora esiste $\alpha \in K$ tale che $K = F(\alpha)$ e $\alpha^p \in F$.

Per un tale α vale $F(\alpha) \neq F$, e dunque $F(\alpha) = K$, dato che $|K : F| = p$, e quindi non ci sono campi intermedi. Dunque K/F è una estensione radicale.

Applichiamo il Lemma per $K = M'$. Dato che M è un sottogruppo normale di $G = \text{Gal}(E/F)$, ne segue che K/F è normale, e $\text{Gal}(K/F) \cong G/M$ ha ordine p . Dunque da F a K si va con una estensione radicale, e poi si va avanti per induzione.

DIMOSTRAZIONE. Nella dimostrazione si introducono i cosiddetti *risolvendi di Lagrange*, che saranno essenziali anche per trovare le formule risolutive per l'equazione di terzo grado.

Siano $1, \omega, \omega^2, \dots, \omega^{p-1}$ le radici p -sime dell'unità in F . Sia $\beta \in K \setminus F$, per cui $K = F(\beta)$. Sia $\text{Gal}(K/F) = \langle g \rangle$. Dato che l'estensione K/F è normale, si ha $\beta g \neq \beta$, e dunque per il teorema orbita-stabilizzatore gli elementi $\beta, \beta g, \dots, \beta g^{p-1}$ sono distinti.

Consideriamo i risolvendi di Lagrange

$$\left\{ \begin{array}{l} (1, \beta) = \beta + \beta g + \beta g^2 + \dots + \beta g^{p-1} \\ (\omega, \beta) = \beta + \omega \cdot \beta g + \omega^2 \cdot \beta g^2 + \dots + \omega^{p-1} \cdot \beta g^{p-1} \\ \dots \\ (\omega^i, \beta) = \beta + \omega^i \cdot \beta g + \omega^{2i} \cdot \beta g^2 + \dots + \omega^{(p-1)i} \cdot \beta g^{p-1} \\ \dots \\ (\omega^{p-1}, \beta) = \beta + \omega^{p-1} \beta g + \omega^{2(p-1)} \beta g^2 + \dots + \omega^{(p-1)(p-1)} \cdot \beta g^{p-1} \end{array} \right.$$

Abbiamo per ogni i

$$(\omega^i, \beta)g = \beta g + \omega^i \beta g^2 + \omega^{2i} \cdot \beta g^3 + \dots + \omega^{i(p-1)} \cdot \beta = \omega^{-i}(\omega^i, \beta),$$

dato che $g^p = 1$. Dunque

$$(\omega^i, \beta)^p g = ((\omega^i, \beta)g)^p = (\omega^{-i}(\omega^i, \beta))^p = (\omega^i, \beta)^p.$$

Dunque per ogni i si ha $(\omega^i, \beta)^p \in \text{Gal}(K/F)' = F$.

Ora $(1, \beta), (\omega, \beta), \dots, (\omega^{p-1}, \beta)$ si esprimono come combinazioni lineari degli $\beta, \beta g, \dots, \beta g^{p-1}$ mediante una matrice

$$\begin{bmatrix} 1 & 1 & \dots & 1 & \dots & 1 \\ \omega & \omega^2 & \dots & \omega^j & \dots & \omega^{p-1} \\ \omega^i & \omega^{2i} & \dots & \omega^{ji} & \dots & \omega^{(p-1)i} \\ \omega^{p-1} & \omega^{2(p-1)} & \dots & \omega^{j(p-1)} & \dots & \omega^{(p-1)(p-1)} \end{bmatrix}$$

che ha determinante di Vandermonde $\Delta(1, \omega, \dots, \omega^{p-1})$. Dato che per ipotesi le p radici p -sime dell'unità $1, \omega, \dots, \omega^{p-1}$ sono distinte, segue dalla formula (7.15.1) che $\Delta(1, \omega, \dots, \omega^{p-1}) \neq 0$.

Dunque la matrice in questione è invertibile, e si possono scrivere anche i $\beta, \beta g, \dots, \beta g^{p-1}$ come combinazioni lineari di $(1, \beta), (\omega, \beta), \dots, (\omega^{p-1}, \beta)$. Abbiamo naturalmente $K = F(\beta) = F(\beta, \beta g, \dots, \beta g^{p-1})$. Dunque almeno uno degli (ω^i, β) non sta in F , e si ha quindi $K = F(\omega^i, \beta)$. Il risultato si ottiene ponendo $\alpha = (\omega^i, \beta)$. \square

Un'applicazione banale dei risolvanti di Lagrange si ha con l'equazione di secondo grado $f(x) = x^2 + a_1x + a_0 = 0$, con $f \in F[x]$. Sia K il campo di spezzamento di f su F . Se supponiamo f irriducibile in $F[x]$, allora $|K : F| = 2$. Stiamo supponendo che la caratteristica sia zero, o almeno diversa da 2, per cui f è separabile, il gruppo di Galois $\text{Gal}(K/F)$ è ciclico di ordine 2, e se β è una radice di f , l'altra è βg , per $1 \neq g \in \text{Gal}(K/F)$. Qui $\omega = -1$, e abbiamo

$$(7.17.1) \quad \begin{aligned} (1, \beta) &= \beta + \beta g = -a_1 \in F, \\ (-1, \beta) &= \beta - \beta g. \end{aligned}$$

Dato che uno di questi due elementi deve stare fuori da F , si ha $(-1, \beta) \notin F$, e dunque $K = F(-1, \beta)$. Inoltre

$$\begin{aligned} (-1, \beta)^2 &= (\beta - \beta g)^2 \\ &= \beta^2 + (\beta g)^2 - 2\beta \cdot (\beta g) \\ &= (\beta + \beta g)^2 - 4\beta \cdot (\beta g) \\ &= a_1^2 - 4a_0. \end{aligned}$$

Dunque $(-1, \beta) = \sqrt{a_1^2 - 4a_0}$. A questo punto si risolve il sistema (7.17.1) di due equazioni lineari nelle due incognite $\beta, \beta g$, e si ritrova la solita formula.

7.18. Un commento

Notate che il Lemma 7.17.1 è un inverso parziale del Lemma 7.4.1 nella nostra versione migliorata, in cui mostriamo che se F contiene n radici distinte dell'unità, allora un'estensione E/F generata da una radice n -esima di un elemento di F è ciclica (cioè normale con gruppo di Galois ciclico). Infatti il Lemma 7.17.1 afferma che se F contiene p radici distinte dell'unità, e p è primo, allora un'estensione ciclica E/F è generata da una radice p -esima di un elemento di F .

In realtà l'ipotesi che p sia primo nel Lemma 7.17.1 è superflua, il Lemma vale per qualsiasi estensione E/F ciclica (sempre con F contenente n radici distinte dell'unità), e quindi esso è un vero inverso del Lemma 7.4.1, ma la dimostrazione in tal caso è più complicata (conseguenza della Satz 90 di Hilbert, vedi [Jac85]).

7.19. Un'altra dimostrazione

Del Lemma 7.17.1 possiamo anche dare una dimostrazione forse meno costruttiva, ma molto istruttiva, nel modo seguente. Fissiamo un elemento non banale g del gruppo di Galois. Possiamo pensare g come una trasformazione lineare dello spazio vettoriale E sul campo F . Essendo $g^p = \text{id}$, il polinomio minimo di g (che divide sempre il polinomio caratteristico) divide $\lambda^p - 1$. Avendo supposto che F contenga tutte le radici di $\lambda^p - 1$, concludiamo g ha almeno un autovalore (in F), diciamo ω ; sia $\gamma \in E$ un corrispondente autovettore (inteso non nullo). (A meno di multipli, γ sarà il risolvente di Lagrange (ω^{-1}, β) costruito nella dimostrazione data nelle Note.) Dunque $\gamma g = \omega \gamma$, da cui $\gamma^p g = \gamma^p$. Poiché g genera il gruppo di Galois, concludiamo che $\gamma^p \in F$; d'altra parte $F(\gamma)$ contiene F propriamente, e quindi coincide con E , come si voleva.

Nella precedente dimostrazione ce la siamo cavata con meno conti, usando solo un po' di algebra lineare. Non abbiamo però costruito esplicitamente un tale autovettore γ per g . Naturalmente saremmo in grado di farlo con i metodi dell'algebra lineare, ad esempio scegliendo una base per E/F , e quindi trovando (risolvendo un sistema di equazioni) una combinazione lineare della base che sia un autovettore per g relativo all'autovalore ω , ma a questo punto i calcoli necessari diventerebbero più complicati che la dimostrazione data nelle Note.

Ci sarebbe una scelta giusta di una base per semplificare i calcoli, e sarebbe scegliere una base cosiddetta *normale*, cioè del tipo $\{\beta, \beta g, \dots, \beta g^{p-1}\}$ per qualche β . Un teorema, il *Teorema della base normale* (vedi [Jac85]) afferma che una tale base esiste sempre, per ogni estensione normale: se E/F è un'estensione normale, allora esiste $\beta \in E$ tale che $\{\beta g : g \in \text{Gal}(E/F)\}$ siano indipendenti su F , e quindi formino una base di E/F . (Nel linguaggio della Teoria delle rappresentazioni, questo dice che E è isomorfo al modulo regolare per l'algebra gruppale FG . Nel caso della nostra estensione ciclica E/F , ne seguirebbe che un generatore g del gruppo di Galois ha p autovalori distinti su E , e quindi è in effetti diagonalizzabile; a noi era bastato mostrare che ne avesse uno.)

ESERCIZIO 29. Supponendo di avere a disposizione una base normale di E/F , cioè della forma $\{\beta, \beta g, \dots, \beta g^{p-1}\}$, trovatene una combinazione lineare non nulla che sia un autovettore per g con autovalore ω , dove ω è una *qualsiasi* radice p -esima dell'unità in F . (Usate i metodi dell'algebra lineare, cioè scrivete una combinazione lineare generica, imponete che essa sia un autovettore, e risolvete un sistema di equazioni per i coefficienti).

7.20. Trovare una base normale

Il problema è ora quello di trovare una tale base normale. Purtroppo, fissato $\beta \in E \setminus F$, non è detto che $\{\beta, \beta g, \dots, \beta g^{p-1}\}$ siano linearmente indipendenti

su F . I risolventi di Lagrange aggirano questo problema. Una spiegazione è la seguente, che però riserverei agli studenti che seguono anche il corso di Teoria delle rappresentazioni.

Fissiamo $\beta \in E \setminus F$, e sia L il sottospazio di E (come spazio vettoriale su F) generato da $\{\beta, \beta g, \dots, \beta g^{p-1}\}$. Naturalmente L non coincide necessariamente con E , e (quindi) non è nemmeno un sottocampo, in generale. Non importa, esso viene mandato in se stesso dal gruppo di Galois G , e quindi è un modulo per G sul campo F (un sottomodulo di E). La nostra ipotesi che F contenga p distinte radici p -esime dell'unità garantisce non solo che $|G| = p$ non divida la caratteristica di F (che potete anche supporre 0 per semplicità), ma che la teoria delle rappresentazioni di G su F , per quanto ci servirà qui, sia la stessa che se F fosse un campo algebricamente chiuso (di questo fidatevi). Dunque l' FG -modulo L è completamente riducibile, e possiamo decomporlo nella somma delle sue componenti omogenee, ciascuna corrispondente ad un carattere irriducibile χ_i di G . Ricordiamo infatti che ciascuna componente omogenea di L è composta da autovettori per ogni elemento g di G , e quindi una fra esse che non sia contenuta in F ci fornirà l'elemento γ di cui si parlava in precedenza (tale che $F(\gamma) = E$).

Fissati un generatore g di G , ed una radice p -esima primitiva dell'unità $\omega \in F$, la mappa $\chi_i : G \rightarrow F^\times$ tale che $\chi(g^j) = \omega^{-ij}$ (il segno meno all'esponente è solo per conformarci alla notazione usata nelle Note) è un omomorfismo, quindi un carattere lineare di G ; notate che χ_i è determinato in modo univoco da $\chi(g) = \omega^{-i}$. Come sappiamo dal corso di Teoria delle rappresentazioni, la decomposizione di L nella somma delle sue componenti omogenee è data da $L = L \cdot 1 = L \cdot (\sum_i e_i) = \bigoplus_i L e_i$ (qualcuna delle quali potrebbe ben essere nulla), dove e_i è l'idempotente centrale primitivo dell'algebra grupale di G corrispondente al carattere irriducibile χ_i , che sappiamo essere dato dalla formula

$$e_i = \frac{1}{|G|} \sum_{g \in G} \chi_i(1) \chi_i(g^{-1}) g = \frac{1}{|G|} \sum_j \omega^{ij} g^j.$$

Notate che la matrice dei coefficienti ω^{ij} è essenzialmente la tabella dei caratteri di G ; il suo determinante è il determinante di Vandermonde. (Non ci serve, ma conosciamo già la componente omogenea di L relativa al modulo principale, deve essere F (perché $F = \mathbf{Inv}(G)$). Ora L è generato da β come FG -modulo, cioè $L = \sum_{g \in G} F \cdot \beta g$, avremo $L e_i = \sum_{g \in G} F \cdot (\beta g) e_i = \sum_{g \in G} F \cdot (\beta e_i) g$ (essendo gli idempotenti e_i centrali), e quindi $L e_i$ è generato come FG -modulo da $\beta e_i = \frac{1}{|G|} \sum_j \omega^{ij} (\beta g^j)$. Ma questo, a parte il fattore scalare $1/|G|$, altro non è che il risolvente di Lagrange (ω_i, β) , l'autovettore cercato (o meglio, uno fra essi che sia non nullo).

Naturalmente la giustificazione dei risolventi di Lagrange che vi ho appena dato è più lunga della stessa dimostrazione del Lemma 7.17.1, ma lo scopo era quello di mostrare come essi non siano artifici estratti da un cappello, ma abbiano una chiara interpretazione teorica.

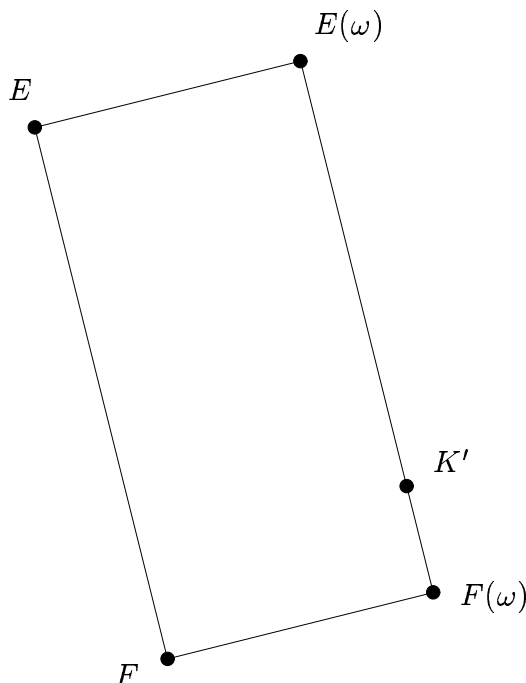


FIGURA 2. Aggiungere le radici

7.21. E se non ci sono le radici dell'unità?

Rivediamo adesso gli ultimi argomenti senza supporre di avere già a disposizione le radici dell'unità. Vogliamo dimostrare

TEOREMA 7.21.1. *Sia E/F il campo di spezzamento su F del polinomio monico non costante $f \in F[x]$. Supponiamo che $\text{Gal}(E/F)$ sia risolubile.*

Allora esiste una estensione radicale M/F tale che $M \supseteq E$.

DIMOSTRAZIONE. Dato che $G = \text{Gal}(E/F)$ è risolubile, avrà un sottogruppo normale H di indice un primo p . Sia ω una radice primitiva p -sima dell'unità, e consideriamo i campi della Figura 2.

Dato che E/F è un campo di spezzamento, e la separabilità è sempre garantita dalla caratteristica zero, E sarà stabile rispetto a $\text{Gal}(E(\omega)/F)$. In particolare possiamo considerare la restrizione

$$\text{Gal}(E(\omega)/F(\omega)) \rightarrow \text{Gal}(E/F).$$

Questa restrizione è iniettiva, perché un isomorfismo di $E(\omega)$ in sé che fissi sia ω che gli elementi di E deve essere l'identità. Dunque $\text{Gal}(E(\omega)/F(\omega))$ è isomorfo a un sottogruppo di $\text{Gal}(E/F)$. Procediamo per induzione sull'ordine del gruppo di Galois. Se $\text{Gal}(E(\omega)/F(\omega))$ ha ordine più piccolo di quello di $\text{Gal}(E/F)$, allora per induzione c'è una estensione radicale $M/F(\omega)$, con $M \supseteq E(\omega)$. Allora anche M/F è una estensione radicale, e $M \supseteq E$, come richiesto.

Se invece gli ordini sono gli stessi, allora $\text{Gal}(E(\omega)/F(\omega))$ e $\text{Gal}(E/F)$ sono gruppi isomorfi. Dunque anche $\text{Gal}(E(\omega)/F(\omega))$ ha un sottogruppo K , normale, di indice p . Consideriamo K' come in figura. Allora $|K' : F(\omega)| = p$, e l'estensione

$K'/F(\omega)$ è normale, perché K è un sottogruppo normale di $\text{Gal}(E(\omega)/F(\omega))$. A questo punto posso applicare il Lemma 7.17.1, e ottenere che $K' = F(\omega, \alpha)$, con $\alpha^p \in F(\omega)$. Quindi da F a K' siamo andati con una estensione radicale, e ora possiamo applicare l'ipotesi induttiva a $E(\omega)/K'$. \square

7.22. Un esempio: L'equazione biquadratica generale

Sezione in costruzione!

Trovarne il gruppo di Galois (D_8). Trovare campi e gruppi intermedi. Risolverla.

Il discorso è del tutto analogo per l'equazione reciproca di quarto grado.

CAPITOLO 8

L'equazione di terzo grado

Questa parte è ispirata da [vdW71], e supponiamo sempre di essere in caratteristica zero.

8.1. Discriminante

Denotiamo con $\Delta(t_1, t_2, \dots, t_n) \in \mathbf{Z}[t_1, t_2, \dots, t_n]$ l'elemento di (7.15.1). Il gruppo simmetrico S_n agisce su $\mathbf{Z}[t_1, t_2, \dots, t_n]$ permutando gli indici. Un 2-ciclo ha l'effetto di scambiare due colonne della matrice di (7.15.1), e quindi di cambiare il segno di $\Delta(t_1, t_2, \dots, t_n)$. Ne segue che

$$(8.1.1) \quad \Delta(t_1, t_2, \dots, t_n)\sigma = \begin{cases} \Delta(t_1, t_2, \dots, t_n) & \text{se } \sigma \text{ è pari,} \\ -\Delta(t_1, t_2, \dots, t_n) & \text{se } \sigma \text{ è dispari,} \end{cases}$$

Prendiamo adesso un'equazione di grado n su un campo F ,

$$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0,$$

e siano $\alpha_1, \dots, \alpha_n$ le sue radici nel campo di spezzamento E . Sia $G = \text{Gal}(E/F)$. Allora $D = \Delta(\alpha_1, \dots, \alpha_n)^2$ è fissato da G , e quindi sta in F . D viene detto *discriminante* del polinomio o dell'equazione. Per esempio, per l'equazione di secondo grado

$$x^2 + a_1x + a_0 = 0$$

viene proprio il discriminante noto. Infatti

$$(\alpha_1 - \alpha_2)^2 = \alpha_1^2 + \alpha_2^2 - 2\alpha_1\alpha_2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = a_1^2 - 4a_0.$$

In generale, dato che $\Delta(\alpha_1, \dots, \alpha_n)^2$ è una funzione simmetrica degli α_i , si deve scrivere come un polinomio nelle funzioni simmetriche elementari negli α_i , cioè nei coefficienti a_j . Sia $\Omega = \{\alpha_1, \dots, \alpha_n\}$. Abbiamo già notato in 3.3 che la restrizione

$$\text{Gal}(E/F) \rightarrow S_\Omega$$

è un morfismo (ben definito e) iniettivo, per cui gli elementi del gruppo di Galois possono essere visti come permutazioni su Ω , ovvero come elementi di S_n .

LEMMA 8.1.1. *Sia $f(x) \in F[x]$ un polinomio, E il campo di spezzamento di f su F . Sia D il discriminante di f .*

Supponiamo che f abbia radici distinte in E . (Dunque $D \neq 0$.)

Sono equivalenti

1. *Tutti gli elementi di $\text{Gal}(E/F)$ danno luogo a permutazioni pari.*
2. $\Delta = \sqrt{D} \in F$.

DIMOSTRAZIONE. Se tutte le permutazioni sono pari, allora per (8.1.1) $\Delta = \sqrt{D}$ è fissato da ogni elemento di $\text{Gal}(E/F)$, e dunque è in F .

Viceversa se $\Delta \in F$, allora Δ è fissato da ogni elemento di $\text{Gal}(E/F)$, e dunque per (8.1.1) ogni tale elemento rappresenta una permutazione pari. \square

8.2. Un commento

Possiamo enunciare il Lemma 8.1.1 nella seguente forma leggermente piú generale (che si dimostra nello stesso modo).

LEMMA 8.2.1. *Nella corrispondenza di Galois per l'estensione E/F , al sottocampo $F(\Delta)$ corrisponde il sottogruppo di $\text{Gal}(E/F)$ costituito dagli automorfismi che realizzano permutazioni pari di Ω (cioè $\text{Gal}(E/F) \cap A_\Omega$, se A_Ω denota il gruppo alterno su Ω).*

Vediamo dal Lemma che per risolvere per radicali un'equazione di grado n , un primo passo (eventualmente banale) si può sempre fare, ed è estendere il campo F con una radice quadrata del discriminante dell'equazione; fatto questo, il gruppo di Galois dell'equazione, che in generale è un sottogruppo di S_n , si riduce ad un sottogruppo di A_n (che naturalmente potrà essere risolubile o non). Questo sarà comunque il primo passo da fare per risolvere le equazioni di secondo, terzo e quarto grado (e sarà l'unico passo nel caso di secondo grado).

Applicando il Lemma alla situazione dell'equazione generale di grado n , otteniamo immediatamente una caratterizzazione delle funzioni razionali *alternanti* in n indeterminate, cioè di quelle funzioni (o meglio *espressioni*) razionali in n indeterminate che cambiano segno scambiando due delle indeterminate. (Supponiamo per il momento di essere in caratteristica diversa da 2, altrimenti $1 = -1$.) Infatti, ricordando la definizione di permutazioni pari e dispari, si vede subito che una condizione equivalente ad essere alternante, per una funzione razionale, è di rimanere invariata per ogni permutazione *pari* delle indeterminate, ma non per quelle *dispari* (almeno una, e quindi tutte). Grazie al Lemma, ed usando la notazione della Sezione 7.13, le funzioni razionali simmetriche o alternanti saranno gli elementi del sottocampo di $K(t_1, \dots, t_n)$ corrispondente al gruppo alterno A_n , cioè $K(\sigma_1, \dots, \sigma_n, \Delta)$.

TEOREMA 8.2.2. *Ogni funzione razionale simmetrica o alternante nelle indeterminate t_1, \dots, t_n , è una funzione razionale delle funzioni simmetriche elementari e del determinante di Vandermonde in t_1, \dots, t_n .*

Notate che nel teorema non serve supporre di essere su un campo K di caratteristica diversa da 2; infatti in quel caso le funzioni alternanti sono la stessa cosa di quelle simmetriche, e in particolare il determinante di Vandermonde è anch'esso una funzione simmetrica!

Ci sono vari modi per calcolare il discriminante di un polinomio. Il modo piú diretto, descritto ad esempio in [Jac85], è quello di cercare di esprimere il discriminante $\prod_{i < j} (\alpha_j - \alpha_i)^2$ in termini delle espressioni simmetriche elementari nelle radici $\alpha_1, \dots, \alpha_n$ del polinomio, e quindi in termini dei coefficienti del polinomio. Infatti il discriminante come funzione delle radici è un "polinomio" simmetrico

omogeneo di grado $n(n-1)$, e sappiamo dalla teoria (l'analogo per i polinomi, che non abbiamo dimostrato, del Teorema 7.13.2) che ogni polinomio simmetrico in $\alpha_1, \dots, \alpha_n$ si deve poter scrivere come un'espressione polinomiale (piuttosto che solo *espressione razionale*, come ci dice il Teorema 7.13.2) nelle espressioni simmetriche elementari in $\alpha_1, \dots, \alpha_n$.

ESERCIZIO 30. Calcolate il discriminante del polinomio biquadratico $x^4 + bx^2 + c$, a partire dalla definizione.

(*Suggerimento:* Se le radici sono $\pm\alpha$ e $\pm\beta$, notate che $b = -\alpha^2 - \beta^2$ e $c = \alpha^2\beta^2$. Dovreste trovare che il discriminante è $16c(b^2 - 4c)^2$.)

Talvolta ci può essere qualche scorciatoia per il calcolo del discriminante, come nell'Esercizio seguente.

ESERCIZIO 31. Vogliamo calcolare il discriminante del polinomio

$$f(x) = x^3 + px + q.$$

Sappiamo che deve essere un "polinomio" simmetrico nelle radici $\alpha_1, \dots, \alpha_n$, e quindi un polinomio nelle espressioni simmetriche elementari $\alpha_1 + \alpha_2 + \alpha_3 = 0$, $\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = p$, $\alpha_1\alpha_2\alpha_3 = -q$. Ma il discriminante è anche omogeneo di grado 6 come polinomio nelle radici, quindi per una questione di gradi deve essere una combinazione lineare di p^3 e q^2 . Determinatene i coefficienti calcolando esplicitamente (a partire dalla definizione) il discriminante dei polinomi $x^3 - x$ e $x^3 - 1$.

Un altro modo per calcolare il discriminante di un polinomio f è basato sull'osservazione che esso è nullo se e solo se f ha radici multiple, cioè se e solo se f ed f' hanno almeno una radice in comune (in un campo di spezzamento). Dunque, pensando i coefficienti di f come indeterminate, l'equazione ottenuta eguagliando a zero il suo discriminante è equivalente (cioè ha le stesse soluzioni) all'equazione ottenuta eliminando la x dal sistema $\{f(x) = 0, f'(x) = 0\}$. Ad esempio, nel caso del polinomio $ax^2 + bx + c$, eliminando la x dal sistema $\{ax^2 + bx + c = 0, 2ax + b = 0\}$ si ottiene $b^2 - 4ac = 0$, o un'equazione ad essa equivalente; poiché questo il grado giusto per essere il discriminante e non ha fattori irriducibili multipli (importante!), possiamo concludere che esso è il discriminante, a meno di un coefficiente. Come vedrete nell'Esercizio seguente, in vari casi questo ci permette di calcolare il discriminante di un polinomio f (a coefficienti indeterminati, diciamo almeno uno), ma comunque a meno di un coefficiente moltiplicativo; quest'ultimo si potrà sempre calcolare calcolando direttamente il discriminante dell'equazione ottenuta dando dei valori particolari ai coefficienti indeterminati, come nell'Esercizio precedente.

ESERCIZIO 32.

1. Mostrate che $x^3 + px + q$ ha radici multiple se e solo se $-4p^3 - 27q^2 = 0$; concludete che $-4p^3 - 27q^2$ è il discriminante, a parte un coefficiente. (In effetti esso è il discriminante, come sappiamo).

2. Mostrate che $x^4 + px + q$ ha discriminante proporzionale a $-3^3p^4 + 4^4q^3$. (In effetti questo è il discriminante.)
3. Mostrate che $x^5 + px + q$ ha discriminante proporzionale a $4^4p^5 + 5^5q^4$. (In effetti questo è il discriminante. Ricordate l'Esercizio della Sezione 7.6. Troverete una generalizzazione in un esercizio successivo.)
4. Mostrate che il polinomio biquadratico $x^4 + bx^2 + c$ ha radici multiple se e solo se $c(b^2 - 4c) = 0$. (Qui il polinomio $c(b^2 - 4c)$ ha grado 8 come polinomio nelle radici, quindi non ha il grado giusto per essere il discriminante, che sarebbe 12. Inoltre, vediamo dalla parte 2. dell'esercizio che nel discriminante dovrebbe comparire il monomio 4^4c^3 . In effetti il discriminante è $16c(b^2 - 4c)^2$, come trovato in un esercizio precedente. Più in generale, l'equazione trinomia $x^{2n} + bx^2 + c$ ha discriminante $n^{2n}c^{n-1}(b^2 - 4c)^n$.)

Ecco altri esercizi (meno fondamentali) sul discriminante.

ESERCIZIO 33. (FACOLTATIVO)

Sia $f(x) = (x - t_1) \cdots (x - t_n) \in F(t_1, \dots, t_n)[x]$. (Qui t_1, \dots, t_n sono indeterminate su F , ma non è indispensabile: possiamo anche supporre semplicemente $f(x) \in F[x]$, e t_1, \dots, t_n sono le sue radici in un campo di spezzamento su F .) Mostrate che il discriminante di f è uguale a $(-1)^{n(n-1)/2} \prod_{i=1}^n f'(t_i)$.

(Suggerimento: Notate che $\prod_{i < j} (t_j - t_i)^2 = (-1)^{n(n-1)/2} \prod_{i \neq j} (t_j - t_i)$.)

ESERCIZIO 34. (FACOLTATIVO) Utilizzando il risultato dell'esercizio precedente, mostrate che il polinomio $x^n - 1$ ha discriminante $(-1)^{(n-1)(n-2)/2} \cdot n^n$.

ESERCIZIO 35. (FACOLTATIVO, E UN PO' PIÙ COMPLICATO DEI PRECEDENTI) Mostrate che il polinomio $f(x) = x^n + px + q$ ha discriminante

$$(-1)^{n(n-1)/2} (n-1)^{n-1} p^n + (-1)^{(n-1)(n-2)/2} n^n q^{n-1}.$$

(Suggerimento: Il discriminante è determinato a meno di multipli eliminando la x dal sistema $\{x^n + px + q = 0, nx^{n-1} + p = 0\}$, dopodiché per calcolare il coefficiente basta considerare il caso $p = 0, q = -1$ ed usare l'esercizio precedente.)

8.3. Il gruppo di Galois dell'equazione di terzo grado

Veniamo adesso all'equazione di terzo grado

$$f(x) = x^3 + px + q = 0$$

(le notazioni p e q sono tradizionali), a cui supponiamo di aver già rimosso col solito trucco il coefficiente di x^2 , e prendiamola su un campo F che contenga una radice terza dell'unità

$$\omega = -\frac{1}{2} + \frac{\sqrt{-3}}{2}.$$

Ricordiamo che

$$\omega^2 = -\frac{1}{2} - \frac{\sqrt{-3}}{2}.$$

Tanto vale supporre f irriducibile su F , altrimenti abbiamo equazioni di grado uno o due, non tre. Dunque il gruppo di Galois $G = \text{Gal}(E/F)$ sarà S_3 o A_3 .

Infatti sappiamo che il gruppo di Galois è in grado di mandare ciascuna delle tre radici del polinomio irriducibile f in ciascun'altra, ovvero come gruppo di permutazioni deve essere transitivo sulle tre radici. Che i sottogruppi transitivi di S_3 siano solo S_3 e A_3 è ora facile, dato che gli altri hanno ordine due, e scambiano fra loro due radici, fissando la terza. In ogni caso alla catena di sottogruppi

$$G \cap S_3 \supseteq G \cap A_3 \supseteq \{1\}$$

corrispondono i campi fissati

$$F \subseteq F(\sqrt{D}) \subseteq E.$$

Quindi la prima estensione radicale è $F(\sqrt{D})/F$ (di grado uno o due), e si tratta di esprimere in forma radicale l'estensione di grado tre $E/F(\sqrt{D})$. Notate che questa è una estensione normale, ed ha gruppo di Galois A_3 , quindi soddisfa le ipotesi di 7.17.1.

Il discriminante è $D = -4p^3 - 27q^2$; questo è ottenuto in [Jac85] con alcuni calcoli, ma si può fare più semplicemente e concettualmente, come abbiamo visto nell'Esercizio 31 a p. 77. Siano $\alpha_1, \alpha_2, \alpha_3$ le tre radici. Formiamo i risolventi di Lagrange

$$(8.3.1) \quad \begin{cases} (1, \alpha_1) = \alpha_1 + \alpha_2 + \alpha_3 = 0, \\ (\omega, \alpha_1) = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3, \\ (\omega^2, \alpha_1) = \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3. \end{cases}$$

Sappiamo che $(\omega, \alpha_1)^3 \in F(\sqrt{D})$. A questo proposito, vale la pena di notare che il più piccolo campo su cui f è definito è $\mathbf{Q}(p, q)$, per cui non si perde niente a supporre $F = \mathbf{Q}(p, q, \omega)$. Dunque $(\omega, \alpha_1)^3$ deve essere esprimibile in termini di p, q, ω, \sqrt{D} .

8.4. Espressione esplicita per le radici cubiche

Per trovare questa espressione in forma esplicita, calcoliamo

$$(8.4.1) \quad \begin{aligned} (\omega, \alpha_1)^3 &= \alpha_1^3 + \alpha_2^3 + \alpha_3^3 \\ &\quad + 3\omega(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1) \\ &\quad + 3\omega^2(\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2) \\ &\quad + 6\alpha_1\alpha_2\alpha_3. \end{aligned}$$

La formula per $(\omega^2, \alpha_1)^3$ è del tutto analoga, dato che basta (ovviamente!) scambiare ω e ω^2 .

Ora

$$\begin{aligned} \sqrt{D} &= (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) \\ &= \alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1 - (\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2). \end{aligned}$$

Se scriviamo temporaneamente

$$u = \alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1 + \alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2,$$

possiamo risolvere il sistema dato dalle ultime due equazioni, ed ottenere

$$\begin{cases} \alpha_1^2 \alpha_2 + \alpha_2^2 \alpha_3 + \alpha_3^2 \alpha_1 &= \frac{1}{2}(u + \sqrt{D}), \\ \alpha_1 \alpha_2^2 + \alpha_2 \alpha_3^2 + \alpha_3 \alpha_1^2 &= \frac{1}{2}(u - \sqrt{D}). \end{cases}$$

Ora possiamo riscrivere (8.4.1), tenendo conto che $\omega + \omega^2 = -1$ e $\omega - \omega^2 = \sqrt{-3}$ (un modo intellettuale di vederlo è notando che $(\omega - \omega^2)^2 = (\omega + \omega^2)^2 - 4\omega\omega^2$), come

$$\begin{aligned} (\omega, \alpha_1)^3 &= \alpha_1^3 + \alpha_2^3 + \alpha_3^3 \\ &\quad + \frac{3}{2}\omega(u + \sqrt{D}) + \frac{3}{2}\omega^2(u - \sqrt{D}) \\ &\quad + 6\alpha_1\alpha_2\alpha_3 \\ (8.4.2) \quad &= \alpha_1^3 + \alpha_2^3 + \alpha_3^3 \\ &\quad - \frac{3}{2}u + \frac{3}{2}\sqrt{-3D} \\ &\quad + 6\alpha_1\alpha_2\alpha_3. \end{aligned}$$

Notate che in (ω^2, α_1) avrò il segno cambiato davanti a $\frac{3}{2}\sqrt{-3D}$, dato che qui il coefficiente sarà $\omega^2 - \omega = -\sqrt{-3}$.

Ora, sommando per $i = 1, 2, 3$ le formule

$$\alpha_i^3 + p\alpha_i + q = 0$$

otteniamo (formula di Newton, che potrei scrivere, uno di questi giorni)

$$\alpha_1^3 + \alpha_2^3 + \alpha_3^3 + 3q = 0.$$

Dopodiché

$$0 = (\alpha_1 + \alpha_2 + \alpha_3)^3 = \alpha_1^3 + \alpha_2^3 + \alpha_3^3 + 3u + 6\alpha_1\alpha_2\alpha_3 = -3q + 3u - 6q,$$

ovvero $u = 3q$. Sostituendo in (8.4.2) otteniamo

$$(\omega, \alpha_1)^3 = -3q - \frac{9}{2}q + \frac{3}{2}\sqrt{-3D} - 6q = -\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}.$$

Quello che abbiamo fatto è un caso particolare di un algoritmo più generale per esprimere una funzione polinomiale simmetrica in termini di funzioni simmetriche elementari: vedi [vdW71].

La morale è che

$$(\omega, \alpha_1)^3 = -\frac{27}{2}q + \frac{3}{2}\sqrt{-3D},$$

e similmente

$$(\omega^2, \alpha_1)^3 = -\frac{27}{2}q - \frac{3}{2}\sqrt{-3D}.$$

Prima di estrarre allegramente le radici cubiche, occorre notare che bisogna farlo in modo coerente – una volta scelta la prima, la seconda si determina tenendo

presente che

$$\begin{aligned}
 (\omega, \alpha_1) \cdot (\omega^2, \alpha_1) &= \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + (\omega + \omega^2) \cdot (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) \\
 &= \alpha_1^2 + \alpha_2^2 + \alpha_3^2 - (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) \\
 (8.4.3) \quad &= (\alpha_1 + \alpha_2 + \alpha_3)^2 - 3(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) \\
 &= -3p.
 \end{aligned}$$

8.5. Le formule di Cardano

Finalmente possiamo risolvere il sistema (8.3.1), dato che conosciamo i termini di sinistra, e otteniamo

$$\begin{cases}
 3\alpha_1 = \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}} + \sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{-3D}} \\
 3\alpha_2 = \omega^2 \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}} + \omega \sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{-3D}} \\
 3\alpha_3 = \omega \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}} + \omega^2 \sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{-3D}}
 \end{cases}$$

dove una volta scelta una delle tre radici cubiche possibili di $-\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}$, dobbiamo quindi calcolare la radice cubica di $-\frac{27}{2}q - \frac{3}{2}\sqrt{-3D}$ usando (8.4.3).

ESERCIZIO 36 (Facoltativo, ma divertente da provare). Sia F un campo di caratteristica diversa da 2 e 3. Si mostri che sono equivalenti le seguenti due affermazioni:

1. la somma di due quadrati in F è ancora un quadrato in F ;
2. se un polinomio di terzo grado in $F[x]$ ha tutte le sue radici in F , allora anche la sua derivata (che sarà un polinomio di secondo grado) ha le sue due radici in $F[x]$.

8.6. Un altro modo di trovare le formule di Cardano

Ecco un artificio per risolvere l'equazione di terzo grado. Si tratta di un trucco, senza usare la Teoria di Galois (anche se a posteriori la vi si può ritrovare): potrebbe essere il modo in cui Cardano scoprì le sue formule.

Vogliamo risolvere l'equazione $x^3 + px + q = 0$, cioè $x^3 = -px - q$. Confrontiamola con la formula del cubo di un binomio, nella forma $(u + v)^3 = 3uv(u + v) + u^3 + v^3$. Se esprimiamo x come $u + v$, euristicamente possiamo usare il grado di libertà nella scelta di u e v per imporre che $3uv = -p$ e $u^3 + v^3 = -q$; ora basta risolvere il sistema costituito da queste due equazioni. Come è noto, avendo u^3 e v^3 somma $-q$ e prodotto $-p^3/27$, essi saranno le due radici dell'equazione $y^2 + qy - p^3/27 = 0$ che sono $-q/2 \pm \sqrt{q^2/4 + p^3/27}$. Concludiamo che le radici di $x^3 + px + q = 0$ sono date dalla formula

$$\sqrt[3]{-q/2 + \sqrt{q^2/4 + p^3/27}} + \sqrt[3]{-q/2 - \sqrt{q^2/4 + p^3/27}},$$

dove le due radici cubiche sono scelte in modo che il loro prodotto sia $-p/3$.

CAPITOLO 9

Casus Irreducibilis

9.1. La teoria

Da un esercizio di Jacobson, ma i dettagli sono quelli di [vdW71, § 64].

Sia $F \subseteq \mathbf{R}$ un campo, $f(x) = x^3 + bx + c \in F[x]$ irriducibile in $F[x]$, con tre radici reali che sono quindi ovviamente distinte. Il discriminante D è dunque positivo, in quanto è il quadrato di un numero reale. Il polinomio f resta irriducibile in $F(\sqrt{D})$, dato che altrimenti quest'ultima estensione, che ha al più grado due su F , conterrebbe una radice di f , che ha grado tre su F . Possiamo quindi rimpiazzare F con $F(\sqrt{D})$, ovvero supporre che F contenga \sqrt{D} . Con questa ridefinizione, otteniamo che il campo di spezzamento E ha grado 3 su F . Vogliamo far vedere che non esiste alcuna estensione radicale M/F , con $E \subseteq M \subseteq \mathbf{R}$. In altre parole, i numeri complessi non reali che compaiono nelle formule di Cardano sono inevitabili.

Esplicitamente

TEOREMA 9.1.1. *Sia $F \subseteq \mathbf{R}$ un campo.*

Sia $f(x) = x^3 + bx + c \in F[x]$ un polinomio irriducibile, con tre radici reali. Sia E/F il suo campo di spezzamento.

Allora non esiste alcuna estensione radicale M/F tale che

$$E \subseteq M \subseteq \mathbf{R}.$$

Una semplice riduzione ci porta a considerare il caso in cui $M = F(\alpha)$, con $\beta = \alpha^p \in F$, per qualche numero primo $p \geq 3$. Ora qualunque sia il campo F (anche di caratteristica positiva), vale il seguente semplice fatto

LEMMA 9.1.2. *Sia p un numero primo. Se il polinomio $g(x) = x^p - \beta \in F[x]$ è riducibile in $F[x]$, allora ha una radice in F , ovvero esiste $\gamma \in F$ tale che $\gamma^p = \beta$.*

Si può dire di più se il campo contiene le radici dell'unità (vedi [vdW71]): non sarebbe difficile completare la dimostrazione per vedere che allora f si riduce completamente.

DIMOSTRAZIONE. Se $\beta = 0$ c'è poco da dire, per cui sia $\beta \neq 0$.

Sia α una fissata radice di g nel suo campo di spezzamento, sicché $\alpha^p = \beta$. Nel suo campo di spezzamento, g si fattorizza dunque come

$$x^p - \beta = x^p - \alpha^p = \prod_{i=0}^{p-1} (x - \alpha\omega_i),$$

ove gli ω_i sono le radici p -sime di 1. Supponiamo quindi che questo polinomio si fattorizzi propriamente in F come

$$x^p - \beta = \varphi(x)\psi(x),$$

con $\varphi, \psi \in F[x]$, e $\text{grado}(\varphi) = \mu$, con $0 < \mu < p$. Allora (a meno di segni) il coefficiente costante di φ , che è un certo $\delta \in F$, è della forma $\delta = \alpha^\mu \omega \in F$, per una appropriata radice p -sima ω dell'unità, e si ha $\delta^p = (\alpha^\mu \omega)^p = \beta^\mu$. Dato che μ è coprimo con p , esistono c, d tali che $1 = \mu c + p d$. Si ha

$$\beta = \beta^1 = \beta^{\mu c} \beta^{p d} = (\delta^c \beta^d)^p.$$

Basta ora prendere $\gamma = \delta^c \beta^d \in F$. □

Nel nostro caso le radici di $x^p - \beta = x^p - \alpha^p$ sono

$$\alpha, \alpha\vartheta, \alpha\vartheta^2, \dots, \alpha\vartheta^{p-1},$$

ove ϑ è una radice primitiva p -sima di 1. Di queste, solo α è reale (dato che $p > 2$), e quindi se $x^p - \beta$ fosse riducibile su $F \subseteq \mathbf{R}$, dovrebbe essere $\alpha \in F$, e dunque $M = F(\alpha) = F$, e dato che $F \subseteq E \subseteq M$, anche $E = F$, una contraddizione.

Dunque $x^p - \beta$ è irriducibile su F , e per ragioni di grado $p = 3$, e $M = E$. Ma allora nell'estensione normale M/F ci dovrebbero essere le altri radici di $x^p - \alpha^p = x^3 - \alpha^3$. Di nuovo, queste sono $\alpha, \alpha\omega, \alpha\omega^2$, ove ω è una radice terza primitiva dell'unità, e quindi le altre due radici non sono reali, una contraddizione finale.

9.2. Un esempio

Un polinomio f che dà luogo al *casus irreducibilis* è per esempio $f(x) = x^3 - 6x + 2$, con $F = \mathbf{Q}$. È irriducibile in $\mathbf{Q}[x]$, per il criterio di Eisenstein (Proposizione 1.1.2). Si ha

$$\lim_{x \rightarrow -\infty} f(x) = -\infty, \quad \lim_{x \rightarrow \infty} f(x) = \infty,$$

$f(-1) = 7 > 0$ e $f(1) = -3 < 0$. Dunque f ha tre radici reali.

L'equazione di quarto grado

Supponiamo di avere un polinomio monico e irriducibile f di quarto grado sul campo F . Come al solito supporremo F di caratteristica zero, o almeno diversa da 2 e da 3. Supporremo che F contenga le radici terze e quarte dell'unità e, per semplicità che il gruppo di Galois del campo di spezzamento di f sia tutto S_4 .

Con un semplice trucco, ci si può ridurre al caso di una equazione di terzo grado, detta *cubica risolvente*.

Se $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ sono le quattro radici distinte di f nel suo campo di spezzamento E , consideriamo gli elementi

$$(10.0.1) \quad \beta_1 = \alpha_1\alpha_4 + \alpha_2\alpha_3, \quad \beta_2 = \alpha_2\alpha_4 + \alpha_1\alpha_3, \quad \beta_3 = \alpha_3\alpha_4 + \alpha_1\alpha_2.$$

Consideriamo il polinomio di terzo grado

$$g(x) = (x - \beta_1)(x - \beta_2)(x - \beta_3).$$

Sia $V = \{1, (12)(34), (13)(24), (14)(23)\}$, un sottogruppo normale di S_4 . E' facile vedere che $\beta_i \in K = V'$ per ogni i . Dunque $F(\beta_1, \beta_2, \beta_3) \subseteq K$. Si ha $|K : F| = 6$. Se mostriamo che $|\text{Gal}(F(\beta_1, \beta_2, \beta_3)/F)| \geq 6$, avremo $K = F(\beta_1, \beta_2, \beta_3)$.

Ora notiamo che $S_3 \leq S_4$. Gli elementi di S_3 sono nient'altro che le permutazioni di S_4 che fissano 4. Abbiamo $S_4 = S_3 \cdot V = V \cdot S_3$. Infatti se $\sigma \in S_4$ porta ad esempio 4 in 1, allora $g = \sigma \cdot (14)(23)$ fissa 4, e dunque $g \in S_3$, e $\sigma = g \cdot (14)(23) = ((14)(23))^{g^{-1}} \cdot g$.

Dato che $\beta_i \in V'$, per vedere l'azione di S_4 sui β_i basta dunque limitarsi a S_3 . E qui si vede direttamente che

$$\begin{aligned} \beta_1(123) &= \beta_2, & \beta_2(123) &= \beta_3, & \beta_3(123) &= \beta_1; \\ \beta_1(12) &= \beta_2, & \beta_2(12) &= \beta_1, & \beta_3(12) &= \beta_3. \end{aligned}$$

Dunque S_3 permuta i β_i , e li permuta come permuta gli indici. Dunque il gruppo di Galois $\text{Gal}(F(\beta_1, \beta_2, \beta_3)/F)$ ha almeno 6 elementi, ed abbiamo

$$K = V' = F(\beta_1, \beta_2, \beta_3).$$

Abbiamo mostrato in particolare che il gruppo di Galois $\text{Gal}(E/F)$ permuta fra loro i β_i . Dunque $g \in F[x]$. Un calcolo esplicito mostra che se

$$f(x) = x^4 + bx^3 + cx^2 + dx + e,$$

allora

$$g(x) = x^3 - cx^2 + (bd - 4e)x - b^2e + 4ce - d^2.$$

Vediamo i dettagli. E' chiaro che la somma dei β_i è proprio c .

Per il prodotto, si ha

$$\begin{aligned}\beta_1 \cdot \beta_2 \cdot \beta_3 &= (\alpha_1\alpha_2 + \alpha_3\alpha_4) \cdot (\alpha_1\alpha_3 + \alpha_2\alpha_4) \cdot (\alpha_1\alpha_4 + \alpha_2\alpha_3) \\ &= (\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2) \cdot \alpha_1\alpha_2\alpha_3\alpha_4 \\ &\quad + \alpha_1^2\alpha_2^2\alpha_3^2 + \alpha_1^2\alpha_2^2\alpha_4^2 + \alpha_1^2\alpha_3^2\alpha_4^2 + \alpha_2^2\alpha_3^2\alpha_4^2.\end{aligned}$$

Ora

$$(\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2) \cdot \alpha_1\alpha_2\alpha_3\alpha_4 = (b^2 - 2c)e.$$

Inoltre

$$d^2 = \alpha_1^2\alpha_2^2\alpha_3^2 + \alpha_1^2\alpha_2^2\alpha_4^2 + \alpha_1^2\alpha_3^2\alpha_4^2 + \alpha_2^2\alpha_3^2\alpha_4^2 + 2ce.$$

Infine

$$\begin{aligned}\beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3 &= \alpha_1 \cdot (\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4) \\ &\quad + \text{termini simili per gli altri } \alpha_i \\ &= \alpha_1 \cdot (-d - \alpha_2\alpha_3\alpha_4) \\ &\quad + \text{termini simili per gli altri } \alpha_i \\ &= bd - 4e.\end{aligned}$$

Dunque per risolvere f è sufficiente prima trovare le soluzioni β_i di $g(x) = 0$ con le formule di Cardano, e poi usare (10.0.1) per ricostruire gli α_i . Quest'ultimo passaggio si può fare così. Si comincia con l'eliminare α_4 :

$$\begin{aligned}\beta_1 &= \alpha_1\alpha_4 + \alpha_2\alpha_3 \\ &= \alpha_1(-b - \alpha_1 - \alpha_2 - \alpha_3) + \alpha_2\alpha_3 \\ &= -b\alpha_1 - \alpha_1^2 - \alpha_1\alpha_2 - \alpha_1\alpha_3 + \alpha_2\alpha_3, \\ \beta_2 &= \alpha_2\alpha_4 + \alpha_1\alpha_3 \\ &= \alpha_2(-b - \alpha_1 - \alpha_2 - \alpha_3) + \alpha_1\alpha_3 \\ &= -b\alpha_2 - \alpha_1\alpha_2 - \alpha_2^2 - \alpha_2\alpha_3 + \alpha_1\alpha_3\end{aligned}$$

Ora

$$\beta_1 + \beta_2 = -b(\alpha_1 + \alpha_2) - (\alpha_1 + \alpha_2)^2.$$

Per semplificare, supponiamo di aver ridotto l'equazione di quarto grado col solito sistema in modo che sia $b = 0$. Abbiamo allora

$$\alpha_1 + \alpha_2 = \sqrt{-(\beta_1 + \beta_2)}$$

Con procedure simili si ottengono formule per tutte le somme $\alpha_i + \alpha_j$, con $i \neq j$. Abbiamo allora

$$(10.0.2) \quad \left\{ \begin{array}{llll} \alpha_1 + \alpha_2 & & & = \sqrt{-(\beta_1 + \beta_2)} \\ & \alpha_3 + \alpha_4 & = & -\sqrt{-(\beta_1 + \beta_2)} \\ \alpha_1 + & & \alpha_4 & = -\sqrt{-(\beta_2 + \beta_3)} \\ & \alpha_2 + \alpha_3 & = & \sqrt{-(\beta_2 + \beta_3)} \\ \alpha_1 + & & \alpha_3 & = \sqrt{-(\beta_1 + \beta_3)} \\ & \alpha_2 + & \alpha_4 & = -\sqrt{-(\beta_1 + \beta_3)} \end{array} \right.$$

Come per l'equazione di terzo grado, bisogna scegliere le radici quadrate "positive" in modo da rispettare

$$\begin{aligned} & \sqrt{-(\beta_2 + \beta_3)} \cdot \sqrt{-(\beta_1 + \beta_2)} \cdot \sqrt{-(\beta_1 + \beta_3)} = \\ & = \sqrt{-(\beta_1(\beta_1\beta_2 + \beta_1\beta_3) + \beta_2(\beta_2\beta_1 + \beta_2\beta_3) + \beta_3(\beta_3\beta_1 + \beta_3\beta_2) + 2\beta_1\beta_2\beta_3)} = \\ & = \sqrt{c \cdot (4e) - 4ce + d^2} = d. \end{aligned}$$

Ora la somma delle quattro radici α_i è zero, per cui per risolvere (10.0.2) basta sommare per ogni α_i le tre righe in cui compare. Si ottiene:

$$\begin{cases} 2\alpha_1 = +\sqrt{-(\beta_1 + \beta_2)} - \sqrt{-(\beta_1 + \beta_3)} + \sqrt{-(\beta_1 + \beta_3)} \\ 2\alpha_2 = +\sqrt{-(\beta_1 + \beta_2)} + \sqrt{-(\beta_1 + \beta_3)} - \sqrt{-(\beta_1 + \beta_3)} \\ 2\alpha_3 = -\sqrt{-(\beta_1 + \beta_2)} + \sqrt{-(\beta_1 + \beta_3)} + \sqrt{-(\beta_1 + \beta_3)} \\ 2\alpha_4 = -\sqrt{-(\beta_1 + \beta_2)} - \sqrt{-(\beta_2 + \beta_3)} - \sqrt{-(\beta_1 + \beta_3)} \end{cases}$$

10.1. Cosa dice MAPLE

Secondo MAPLE (ed un po' di lavoro manuale), le quattro radici del polinomio $x^4 + px^3 + qx + r$ sono

$$\begin{aligned} & \frac{1}{12}\sqrt{6B} \pm \frac{1}{12}\sqrt{-6} \sqrt{8p + \sqrt[3]{A} + \frac{48r + 4p^2}{\sqrt[3]{A}} + \frac{12q\sqrt{6}}{\sqrt{B}}}, \\ & \frac{1}{12}\sqrt{6B} \pm \frac{1}{12}\sqrt{-6} \sqrt{8p + \sqrt[3]{A} + \frac{48r + 4p^2}{\sqrt[3]{A}} - \frac{12q\sqrt{6}}{\sqrt{B}}}, \end{aligned}$$

dove

$$\begin{aligned} D &= 256r^3 - 128r^2p^2 + 16rp^4 + 144prq^2 - 27q^4 - 4q^2p^3 \quad (\text{il discriminante}), \\ A &= -288pr + 108q^2 + 8p^3 + 12\sqrt{3}\sqrt{-D}, \\ B &= -4p + \sqrt[3]{A} + \frac{48r + 4p^2}{\sqrt[3]{A}}. \end{aligned}$$

Infatti MAPLE conosce le formule risolutive delle equazioni di terzo e quarto grado (perché qualcuno si è preso la briga di programmarle), ma naturalmente non compaiono in una forma particolarmente piacevole a vedersi. Comunque offrono uno spunto per il seguente

ESERCIZIO 37. Riconoscere nei vari passaggi delle formule viste la strategia risolutiva di scendere dal gruppo di Galois S_4 fino al sottogruppo identità lungo una serie a quozienti abeliani. In particolare, nominare i campi intermedi che si incontrano man mano.

Teoria di Galois delle estensioni di dimensione infinita

Questo capitolo trae origine da alcune note che avevo scritto per me stesso, e che ho rielaborato un po' per la prima versione (1997/98) di queste note. Nel 1998/99 non ho trattato questa parte, per cui non ho avuto occasione di rimetterci le mani, cosa che sarebbe ben necessaria. Mi riprometto di sistemarle decentemente la prossima volta.

Prendo sostanzialmente da [Lan84] l'estensione della teoria di [Kap95] dal caso delle estensioni di grado finito a quella delle estensioni algebriche, e svolgo l'esercizio [Lan84, n 19, p 233] indicatomi da Edoardo Ballico. Si può usare [Hig74] per i gruppi topologici, ma vedendo solo il minimo essenziale per capire ciò di cui si parla.

11.1. Campi di spezzamento di famiglie di polinomi

Si comincia definendo il campo di spezzamento di una famiglia qualsiasi di polinomi. L'esistenza deriva da fatti generali di teoria degli insiemi, che ometterei. Se si prendono in particolare *tutti* i polinomi (monici e) non costanti, si ottiene la *chiusura algebrica* come caso particolare.

Vale anche qui l'unicità, cioè è possibile estendere gli isomorfismi. Qui può valere la pena fare un argomento "alla Zorn", a scopo illustrativo. Per vedere che l'estensione è un isomorfismo, si ricorda il Lemma [Lan84, Lemma 1, p. 167], già visto a lezione, che dice che un isomorfismo di E/F in sé stesso, con E estensione algebrica di F , è anche suriettivo. Si fa prendendo $\alpha \in E$, e riducendosi a

$$F(\alpha_1, \dots, \alpha_n),$$

ove gli α_i sono le radici in E del polinomio minimo di α su F .

Ancora mediante il Lemma si estende al caso algebrico di grado arbitrario la caratterizzazione dei campi di spezzamento mediante il fatto che ogni polinomio irriducibile che vi ha una radice vi si spezza completamente.

Poi mostro l'equivalenza anche per un'estensione algebrica E/F delle condizioni:

- essere normale;
- essere separabile e un campo di spezzamento di una famiglia di polinomi;
- essere un campo di spezzamento di una famiglia di polinomi separabili.

(1) \Rightarrow (2) è come nel caso finito. (2) \Rightarrow (3) è ovvio, naturalmente. Si prova agevolmente anche (3) \Rightarrow (2), ricordando che E è l'unione insiemistica delle estensioni mediante le radici dei particolari polinomi di cui in (3), quindi tutte "piccole" estensioni normali, e pertanto separabili, per il solito Lemma.

Infine da (2) a (1) si passa mediante l'estendibilità degli automorfismi: tanto vale allora far vedere che ogni campo intermedio è chiuso.

Definizione di gruppo topologico, ed esempio dei numeri reali rispetto all'addizione. Topologia prodotto.

Comincio con il Lemma sul fatto che $(x, y) \mapsto x \cdot y^{-1}$ è continua, e sul fatto che se V è aperto allora c'è un aperto U tale che $U \cdot U^{-1} \subseteq V$. Ne deduco che se è T_1 (i punti sono chiusi) allora è anche T_2 .

ESERCIZIO 38. Si mostri che se G è un gruppo, e anche uno spazio topologico, e la mappa

$$\begin{aligned} G \times G &\rightarrow G \\ (x, y) &\mapsto x \cdot y^{-1} \end{aligned}$$

è continua allora G è un gruppo topologico.

Le traslazioni sono continue, dunque un gruppo topologico è uno spazio omogeneo, e per conoscerne la topologia basta conoscere gli aperti contenenti 1, e anzi basta un sistema fondamentale, cioè gli elementi di una base che contengano 1.

Ora prendo un'estensione algebrica e normale E/F . Definisco la *topologia di Krull* sull'insieme $E^E = \prod_{x \in E} E_x$ delle mappe da E a E . (Qui ogni E_x è una copia di E , e la mappa $f : E \rightarrow E$ corrisponde alla E -pla $(f(x))_{x \in E}$.) Questa è la topologia prodotto, ove E ha la topologia discreta.

La topologia di Krull ha dunque per base gli insiemi del tipo

$$\prod_{x \in E} U_x,$$

dove tutti gli U_x tranne un numero finito coincidono con E , mentre quelli rimanenti sono aperti di E , o anche basta aperti di base, e quindi sono della forma $U_x = \{y\}$, per qualche $y \in E$.

Fissiamo un $n \geq 1$, poi n punti distinti $x_1, \dots, x_n \in E$, e n punti arbitrari $y_1, \dots, y_n \in E$. Allora un aperto di base generico è dato da

$$\{f \in E^E : x_i f = y_i, i = 1, \dots, n\}.$$

(Perché basta prendere aperti di base, come detto.) Se prendo solo $n = 1$ ottengo una sottobase. Istruttivo vedere chi sono gli aperti di base che contengono una funzione data: serve fra un attimo.

Questa topologia induce una struttura di gruppo topologico sull'insieme delle mappe biettive da E a E , cioè rende continue le mappe prodotto e inversa. Questo si vede bene prendendo la sottobase della topologia prodotto su E^E , dato che le immagini inverse conservano sia unione che intersezione. Si ha:

$$\{(g, h) : \alpha gh = \beta\} = \bigcup_{\gamma \in E} \{g : \alpha g = \gamma\} \times \{h : \gamma h = \beta\},$$

mentre per l'inversa ho

$$\{g : \alpha g^{-1} = \beta\} = \{g : \beta g = \alpha\}$$

Notare chi sono gli aperti contenenti l'unità, avendo visto la cosa già per un elemento qualsiasi: ripetuto subito sotto.

11.2. Topologia di Krull sul gruppo di Galois

Ora, su $G = \text{Gal}(E/F)$ definisco la *topologia di Krull* come ereditata dal gruppo delle mappe biettive da E a E .

(Dubbio su quanto segue: Definire uno SFIA, le sue connessioni con la topologia, e vedere che il caso particolare di un insieme di sottogruppi (normali) a intersezione 1 definisce una topologia che è Hausdorff, e totalmente sconnessa.)

Si vede subito che uno SFIA (sistema fondamentale di intorni aperti, vedi [Hig74]: basta dire che sono aperti di base contenenti 1, e che determinano tutta la topologia, per la solita faccenda delle traslazioni) di 1 è dato dalla famiglia dei sottogruppi K' , ove K è un'estensione di dimensione finita di F in E . Infatti un intorno di definizione è della forma

$$\{g \in G : \alpha_i g = \alpha_i, i = 1, \dots, n\} = F(\alpha_1, \dots, \alpha_n)'.$$

Va anche bene prendere come SFIA di 1 la famiglia di sottogruppi *normali*

$$\mathcal{U} = \{U = N' : N \text{ estensione normale di dimensione finita di } F\}.$$

Infatti se $K = F(\alpha_1, \dots, \alpha_n)$ come sopra, prendo la sua chiusura normale N , che è ancora in E per quanto visto sopra. Dunque $N' \leq K'$, e quindi se è aperto il primo lo è anche il secondo, che ne è unione di classi laterali. (Un sottogruppo aperto è anche chiuso. Un sottogruppo che contenga un sottogruppo aperto è aperto.)

11.3. Chiusure

Ora dico che $H \leq G$ è Krull-chiuso sse $H = H''$, cioè H è Galois-chiuso. Infatti, se $H = L'$, allora

$$H = L' = \left(\bigcup_{\alpha \in L} F(\alpha) \right)' = \bigcap_{\alpha \in L} F(\alpha)',$$

e quindi è Krull-chiuso.

Nota che ho usato il Lemma immediato, in esercizio sul Kaplansky, che dice $(L \cup M)' = (L \vee M)' = L' \cap M'$, valido anche nel caso di un numero arbitrario di termini. $L \vee M$ sta per il *compositum*, cioè il sottocampo generato. Vale la pena di dire due parole sul caso algebrico, che è appena un po' più semplice, anche se a lezione ho fatto del tutto a meno del compositum.

Adesso mostro che Krull-chiuso implica Galois-chiuso. Noto prima la formula $\overline{H} = \bigcap \{HU : U \in \mathcal{U}\}$. Questa vale facilmente nel nostro contesto, dato che $U = U^{-1}$ per i nostri sottogruppi U . Nel caso di un gruppo topologico qualsiasi, basta notare che se uno ha uno SFIA, si possono rimpiazzare i suoi elementi V con quelli $U = V \cap V^{-1}$, e ora la formula vale rispetto a questi ultimi. Dunque $aU^{-1} \cap H \neq \emptyset$ per ogni $U \in \mathcal{U}$ sse $a \in HU$ per ogni $U \in \mathcal{U}$.

Ora se $H = \overline{H}$ ho

$$H = \overline{H} = \bigcap \{HU : U \in \mathcal{U}\} = \bigcap \{F'_U : U \in \mathcal{U}\} = (\vee \{F_U : U \in \mathcal{U}\})',$$

ove \vee indica il *compositum* degli F_U . (E' veramente necessario?) Qui si ha facilmente che $HU = F_U$ per qualche campo intermedio F_U , dato che $U \leq HU \leq G$,

U è Galois-chiuso, e l'indice $|G : U|$ è finito, per cui anche quello $|HU : U|$ lo è. Dunque, per il Lemma 3.13.2, anche HU è chiuso.

Cosa voglio fare adesso? Mostrare, credo, che il gruppo di Galois è compatto. Noto, se non l'ho fatto prima, che è T_2 , e totalmente sconnesso. Basta far vedere questa seconda cosa, dato che essa implica che i punti sono chiusi, dunque il gruppo è T_1 , e quindi T_2 per fatti generali. Ora si fa vedere che $\cap \mathcal{U} = \{1\}$. Sia C è un insieme qualsiasi contenente 1. Se C contiene propriamente $\{1\}$, diciamo esista $a \in C \setminus \{1\}$ allora scelgo $U \in \mathcal{U}$ che non contenga a , e allora $U \cap C$ sconnette C , perché U è un sottogruppo aperto, dunque il suo complementare è ancora aperto.

Immergo G nel suo completamento \mathcal{U} -adico. Qui prendo \mathcal{U} una famiglia di sottogruppi normali con le proprietà:

- per ogni $U \in \mathcal{U}$, il quoziente G/U è finito;
- \mathcal{U} è chiusa rispetto alle intersezioni finite;
- $\cap \mathcal{U} = \{1\}$.

Cominciamo col considerare il gruppo

$$X = \prod_{U \in \mathcal{U}} G/U,$$

con la topologia prodotto, ove ogni G/U è (finito e) discreto. Nel nostro caso particolare $\mathcal{U} = \{U = N' : N \text{ estensione normale di dimensione finita di } F\}$. Adesso consideriamo il sottogruppo di X

$$\widehat{G} = \{(g_U U)_{U \in \mathcal{U}} : \text{per } U \geq V \text{ si ha } g_U V = g_V V\}.$$

In altre parole, un elemento di X è una famiglia di automorfismi $g_L \in \text{Gal}(L/F)$, uno per ogni estensione normale L di F di grado finito. Una collezione di questo genere sta in \widehat{G} se vale che se $L \supseteq M$, con L e M estensioni normali di F di grado finito, allora $g_L|_M = g_M$. Una famiglia (g_L) di questo tipo si dice compatibile.

Per vedere che sia isomorfo, è sufficiente vedere che l'immersione canonica

$$\begin{aligned} \varphi : G &\rightarrow \widehat{G} \\ g &\mapsto (g_U)_{U \in \mathcal{U}} \end{aligned}$$

sia suriettiva. In altre parole φ manda un elemento di $\text{Gal}(E/F)$ nell'insieme delle sue restrizioni alle estensioni normali di grado finito.

La suriettività segue dal fatto, veramente elementare, che una famiglia compatibile di automorfismi sulle estensioni normali, di dimensione finita, definisce un automorfismo di tutta l'estensione. Cioè che per ogni estensione normale di dimensione finita N/F ho un elemento $g_N \in \text{Gal}(N/F) \cong G/U$ tale che se $N \supseteq M$ sono due estensioni di questo tipo allora

$$g_N|_M = g_M,$$

allora esiste $g \in \text{Gal}(E/F)$ tale che

$$g|_N = g_N$$

per ogni estensione normale di dimensione finita N/F . Infatti per $\alpha \in E$ definisco αg come αg_N , ove N è la chiusura normale di $F(\alpha)$. Si tratta di vedere che sia un automorfismo di E .

Siano allora $\alpha, \beta \in E$, e siano N la chiusura normale di $F(\alpha)$, M la chiusura normale di $F(\beta)$, e $P \supseteq N \cup M$ la chiusura normale di $F(\alpha, \beta)$. Per la condizione di compatibilità

$$\alpha g = \alpha g_N = \alpha g_P \mid_N = \alpha g_P,$$

e similmente $\beta g = \beta g_P$. Dunque

$$(\alpha + \beta)g = (\alpha + \beta)g_P = \alpha g_P + \beta g_P = \alpha g + \beta g,$$

e similmente per il prodotto.

Occorre poi vedere anche che φ sia un omeomorfismo, ma questo è abbastanza facile a partire dalle definizioni. La continuità è immediata, basta comporre con le proiezioni, e vedere che le controimmagini dei punti sono le classi laterali di uno dei sottogruppi di \mathcal{U} . Vediamo ora che l'immagine di un aperto $U \in \mathcal{U}$ è aperta in \widehat{G} . Infatti l'immagine di U in \widehat{G} coincide con l'intersezione con \widehat{G} dell'aperto di sottobase che ha 1 sulla componente U -sima, e le altre componenti libere. Notate che non è detto che l'immagine in X di U sia aperta, dato che potrei star toccando infinite componenti contemporaneamente. (Espandere ancora un po'.)

Dovrei commentare che questo mostra la compattezza del gruppo di Galois, ma per questo devo notare che il sottogruppo di X è chiuso, cosa che non mi sembra abbia scritto finora. Questo deriva dal fatto che l'insieme delle famiglie compatibili è l'intersezione dei sottoinsiemi

$$C = \{(g_L) : g_N \mid_M = g_M\}$$

per fissati $N \supseteq M$. Se mostriamo che ognuno di questi è chiuso siamo a posto, dato che ogni intersezione di chiusi è chiusa. Ora notiamo che C è un insieme riconducibile alla forma

$$C = \{x \in X : f(x) = g(x)\},$$

ove $f, g : X \rightarrow Y$ sono mappe continue fra gli spazi topologici X e Y . Qui X è il prodotto, e Y è $\text{Gal}(M/F)$. Le due mappe sono la proiezione su Y , continua per definizione, e la composizione della proiezione su $\text{Gal}(N/F)$ (ancora continua) con la restrizione $\text{Gal}(M/F) \rightarrow \text{Gal}(N/F)$, pure continua perché sono entrambi spazi discreti. Ora vale il Lemma, facile da dimostrare:

LEMMA 11.3.1. *Y è T_2 se e solo se la diagonale*

$$\Delta = \{(y, y) : y \in Y\} \subseteq Y \times Y$$

è chiusa in $Y \times Y$.

Si conclude con l'osservazione che C è la controimmagine della diagonale $\Delta \subseteq Y \times Y$ sotto la mappa

$$\begin{aligned} X &\rightarrow Y \times Y \\ x &\mapsto (f(x), g(x)). \end{aligned}$$

Quest'ultima mappa è continua perché le componenti lo sono per ipotesi. Dunque C è chiuso.

11.4. Un'osservazione finale

Ho da dimostrare il piccolo Lemma che se N , M sono estensioni normali di F , anche $N \cap M$ lo è, ma questo mi pare sia chiaro attraverso i sottogruppi associati (prodotto di normali aperti), o anche mediante il Lemma che caratterizza le estensioni normali in base alle radici dei polinomi irriducibili (se ce n'è una ci sono tutte).

CAPITOLO 12

Numeri trascendenti

In questo capitolo vorrei fare due cose:

1. La dimostrazione di Cantor dell'*esistenza* di numeri trascendenti. Questa si fa semplicemente facendo vedere che i numeri algebrici sono numerabili, mentre i reali sono più che numerabili. Lo svantaggio è che non è costruttiva, dato che alla fine non ci rimane in mano neanche un esempio di numero trascendente.
2. La dimostrazione di Liouville che un numero algebrico non si può approssimare meglio di tanto con un numero razionale. Questa ha il vantaggio di permetterci di costruire esplicitamente dei numeri trascendenti, ma non ci fornisce nessuna informazione sulla trascendenza di numeri che a noi potrebbero interessare.

In un primo momento avevo in mente di fare anche la dimostrazione della trascendenza di e e π , ma poi mi sono reso conto che questa parte è forse tecnicamente troppo complicata, e alla fine ho lasciato perdere.

12.1. Cantor

Un insieme A si dice *numerabile* quando esiste una mappa suriettiva $\mathbf{N} \rightarrow A$. Se A è infinito, non sarebbe difficile vedere che allora esiste una mappa biiettiva di questo tipo. Dunque A è numerabile se i suoi elementi possono essere messi in una successione, eventualmente con ripetizioni.

Un insieme finito è naturalmente numerabile, ma \mathbf{N} è ovviamente numerabile (e infinito), dato che basta prendere l'identità come mappa $\mathbf{N} \rightarrow \mathbf{N}$. Anche \mathbf{Z} è numerabile, come mostra la successione

$$0, 1, -1, 2, -2, 3, -3, \dots$$

Si può considerare questo esempio come un caso molto semplice del seguente criterio.

LEMMA 12.1.1 (Zeresimo procedimento diagonale di Cantor).

Sia $A = \bigcup_{i=1}^{\infty} A_i$, con ogni A_i finito. Allora A è numerabile.

DIMOSTRAZIONE. Mettiamo gli elementi di ogni A_i in una successione (finita) a nostro piacimento. Poi mettiamo tutti gli elementi di A in una successione, nel modo seguente: prima gli elementi di A_1 , nell'ordine scelto, poi gli elementi di A_2 , nell'ordine scelto, e così via. \square

In effetti, si può considerare $\mathbf{Z} = \bigcup_{i=0}^{\infty} A_i$, dove $A_i = \{+i, -i\}$.

ESERCIZIO 39 (Primo procedimento diagonale di Cantor).

Si mostri che la tesi del lemma vale anche se si suppone che ogni A_i sia numerabile.

Ora possiamo vedere che anche l'insieme \mathbf{Q} dei numeri razionali è numerabile. Basta provarlo per i numeri razionali positivi \mathbf{Q}^+ , e poi applicare lo stesso trucco di \mathbf{Z} . Definiamo

$$A_i = \left\{ \frac{p}{q} : p, q \geq 1, p + q \leq i \right\}.$$

Chiaramente l'unione degli A_i è tutto \mathbf{Q}^+ , e ogni A_i ha al più i elementi.

Consideriamo adesso l'insieme

$$A = \{ z \in \mathbf{C} : z \text{ è algebrico su } \mathbf{Q} \}.$$

Anche questo insieme è numerabile. Infatti ogni elemento di A è radice di un polinomio a coefficienti razionali di grado n , per qualche n . Se moltiplichiamo uno di questi polinomi per tutti i denominatori dei coefficienti, otteniamo un polinomio

$$f(x) = a_0 + a_1x + \cdots + a_nx^n,$$

ove gli a_i sono ora interi, e $a_n \neq 0$. Definiamo l'altezza $h(f)$ di tale polinomio come il numero

$$h(f) = |a_0| + |a_1| + \cdots + |a_n|.$$

Di polinomi $f \in \mathbf{Z}[x]$ di grado n e altezza h ce ne sono dunque al più $(2h+1)^n$, e ognuno ha al più n radici. In particolare è finito ogni insieme

$$A_i = \{ z \in \mathbf{C} : z \text{ è radice di un polinomio } f \in \mathbf{Z}[x] \\ \text{di grado } n \text{ e altezza } h, \text{ con } h + n = i \}.$$

Dato che l'unione degli A_i è tutto A , ne risulta che A è numerabile.

Ora resta da vedere che già \mathbf{R} non è numerabile, col secondo procedimento diagonale di Cantor. Faremo vedere che sono già non numerabili i numeri reali compresi fra 0 e 1. Se lo fossero, potrei scriverli tutti in una successione

$$\begin{array}{rcccccccc} a_1 & = & 0. & b_{11} & b_{12} & b_{13} & \cdots & b_{1n} & \cdots \\ a_2 & = & 0. & b_{21} & b_{22} & b_{23} & \cdots & b_{2n} & \cdots \\ a_3 & = & 0. & b_{31} & b_{32} & b_{33} & \cdots & b_{3n} & \cdots \\ \cdots & & & & & & & & \\ a_m & = & 0. & b_{m1} & b_{m2} & b_{m3} & \cdots & b_{mn} & \cdots \\ \cdots & & & & & & & & \end{array}$$

dove b_{ij} è la j -sima cifra decimale di a_i . Ora le frazioni che hanno denominatore divisibile solo per i primi 2 e 5 (e quindi danno luogo a uno sviluppo decimale finito) possono essere scritte in due modi come numeri decimali. Risolviamo questa ambiguità scegliendo la scrittura infinita, cioè scrivendo ad esempio

$$1 = 0,99999\dots \quad \frac{1}{4} = 0.25 = 0.24999\dots$$

In altre parole, nessun numero nella nostra successione ha tutte le cifre decimali eguali a zero da un certo punto in poi. Ora tutto quello che facciamo è di considerare il numero reale c , compreso fra 0 e 1 così ottenuto. Se $b_{ii} = 1$, scegliamo 2 come i -sima cifra decimale di c . Se invece $b_{ii} \neq 1$, scegliamo 1 come i -sima cifra decimale di c . Viene fuori che c non è nella lista a_1, a_2, \dots , perché differisce da a_i per l' i -sima cifra decimale. Ed è comunque scritto nella forma che abbiamo scelto, perché addirittura non ha alcuno 0 nella scrittura decimale, per cui certamente non può aver tutti zeri da un certo punto in poi.

12.2. Liouville

Sia $\alpha \in \mathbf{C}$ algebrico di grado $n > 1$. In particolare, α non è un numero razionale. Scriviamo

$$f(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbf{Z}[x]$$

per quello che non è proprio il polinomio minimo di α su \mathbf{Q} , ma è invece quel polinomio a coefficienti interi che si ottiene moltiplicando il polinomio minimo per il prodotto dei denominatori di tutti i coefficienti.

Sia $r = p/q \in \mathbf{Q}$, con $p, q \in \mathbf{Z}$. Calcoliamo

$$\begin{aligned} -f(r) &= f(\alpha) - f(r) \\ &= a_0 + a_1\alpha + \dots + a_n\alpha^n - a_0 + a_1r + \dots + a_nr^n \\ &= a_1(\alpha - r) + \dots + a_n(\alpha^n - r^n). \end{aligned}$$

Dunque

$$\frac{-f(r)}{\alpha - r} = a_1 + a_2(\alpha + r) + \dots + a_i(\alpha^{n-1} + \alpha^{n-2}r + \dots + \alpha r^{n-2} + r^{n-1}).$$

Scegliamo r abbastanza vicino a α , in modo che sia $|\alpha - r| < 1$. Abbiamo dunque

$$|r| = |\alpha + r - \alpha| \leq |\alpha| + |r - \alpha| < |\alpha| + 1,$$

e dunque

$$|\alpha^i r^j| \leq |\alpha|^i \cdot (|\alpha| + 1)^j \leq (|\alpha| + 1)^{i+j}.$$

Ne segue

$$\left| \frac{f(r)}{\alpha - r} \right| \leq |a_1| + 2|a_2|(|\alpha| + 1) + \dots + n|a_n|(|\alpha| + 1)^{n-1} = M.$$

Ovviamente la costante M non dipende da r . Prendiamo $q > M$. Otteniamo

$$|\alpha - r| \geq \frac{|f(r)|}{M} \geq \frac{|f(r)|}{q}.$$

Ora ovviamente $f(r) \neq 0$, dato che f è irriducibile in $\mathbf{Q}[x]$. Si ha inoltre

$$f(r) = \frac{a_0q^n + a_1pq^{n-1} + \dots + a_np^n}{q^n}.$$

Il numeratore è un intero non nullo, dunque in modulo almeno 1. Ne segue

$$\left| \alpha - \frac{p}{q} \right| \geq \frac{1}{q^{n+1}},$$

che vale per $q > M$, e per $|\alpha - p/q| < 1$.

Vogliamo ricavare un criterio per la trascendenza di un numero.

PROPOSIZIONE 12.2.1. *Sia $\alpha \in \mathbf{R}$, con $0 < \alpha < 1$.*

Siano $p_i, q_i \in \mathbf{Z}$ interi positivi, tali che

$$0 < \frac{p_i}{q_i} < 1 \quad \text{per ogni } i,$$

$$\lim_{i \rightarrow \infty} \frac{p_i}{q_i} = \alpha,$$

$$\lim_{i \rightarrow \infty} q_i = \infty,$$

$$\left| \alpha - \frac{p_i}{q_i} \right| < \frac{1}{q_i^i} \quad \text{per ogni } i.$$

Allora α è trascendente.

DIMOSTRAZIONE. Facciamo vedere che non esiste il numero M sopra citato. Per qualsiasi M , fissiamo n , e scegliamo $i > n + 1$ tale che $q_i > \max\{M, 1\}$.

Abbiamo quindi

$$\left| \alpha - \frac{p_i}{q_i} \right| < \frac{1}{q_i^i} < \frac{1}{q_i^{n+1}}.$$

Ne segue che α non può essere algebrico di grado n . Dato che n era arbitrario, vuol dire che α è trascendente. \square

Ora si può fare la costruzione di Liouville, o qualcosa di simile. Consideriamo la successione

$$q_1 = 10, \quad q_{i+1} = q_i^{i+1}, \quad \text{per } i \geq 1.$$

In altre parole $q_i = 10^{i!}$. Definiamo (questo andrebbe spiegato un attimo meglio, anche se dovrebbe essere corretto)

$$\frac{p_i}{q_i} = \sum_{k=1}^i \frac{1}{q_k},$$

e

$$\alpha = \lim_{i \rightarrow \infty} \frac{p_i}{q_i} = \sum_{k=1}^{\infty} \frac{1}{q_k}.$$

Abbiamo quindi

$$0 < \alpha - \frac{p_i}{q_i} = \sum_{k=i+1}^{\infty} \frac{1}{q_k} < \frac{2}{q_{i+1}} = \frac{2}{q_i^{i+1}} < \frac{1}{q_i^i}.$$

In pratica, il numero α che abbiamo costruito è (controllare)

$$\alpha = 0.110001000000000000000001 \dots$$

Bibliografia

- [AM69] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.
- [CR71] R. Courant and H. Robbins, *Che cos'è la matematica?*, Universale Scientifica, vol. 65/66/67, Paolo Boringhieri, Torino, 1971, Sesta impressione, ottobre 1985.
- [Gar01] Simon & Garfunkel, *Bridge over Troubled Water*, Columbia, Audio CD, 2001, original recording remastered.
- [Hig74] P. J. Higgins, *Introduction to topological groups*, Cambridge University Press, London, 1974, London Mathematical Society Lecture Note Series, No. 15.
- [Jac85] Nathan Jacobson, *Basic algebra. I*, second ed., W. H. Freeman and Company, New York, 1985.
- [Kap95] Irving Kaplansky, *Fields and rings*, Chicago Lectures in Mathematics, University of Chicago Press, Chicago, IL, 1995, Reprint of the second (1972) edition.
- [Lan84] Serge Lang, *Algebra*, second ed., Addison-Wesley Publishing Co., Reading, Mass., 1984.
- [Ric74] Ian Richards, *An application of Galois theory to elementary arithmetic*, *Advances in Math.* **13** (1974), 268–273.
- [vdW71] B. L. van der Waerden, *Algebra. Teil I*, Springer-Verlag, Berlin, 1971, Achte Auflage. Heidelberger Taschenbücher, Band 12.
- [vdW91] B. L. van der Waerden, *Algebra. Vol. I*, Springer-Verlag, New York, 1991, Based in part on lectures by E. Artin and E. Noether, Translated from the seventh German edition by Fred Blum and John R. Schulenberg.