Appunti sulla teoria di Galois (2011-2012)

– First draft –

Ph. ELLIA

Upgrade 18/06/2012

29 Dicembre 2010

Indice

Parte I Teoria di Galois.

1 Risoluzione delle equazioni algebriche di grado basso. 3
1.1 L'equazione del secondo grado. 3
1.2 L'equazione del terzo grado. 4
1.3 L'equazione del quarto grado. 7
1.4 Conclusione (provvisoria). 9
1.5 Il teorema delle funzioni simmetriche. 9
1.5.1 La risolvente di Lagrange. 12

2 La corrispondenza di Galois. 19
2.1 Richiami: estensioni finite di campi. 19
2.1.1 Divisibilità in un anello integro. 19
2.1.2 Estensioni, elementi algebrici. 21
Esercizi 24
2.2 Estensioni separabili, teorema dell'elemento primitivo. 27
2.2.1 Separabilità. 27
2.2.2 Teorema dell'elemento primitivo. 28
Esercizi 30
2.3 Estensioni normali. 32
2.3.1 Immersioni nell'universo. 32
2.3.2 Estensioni normali. 33
Esercizi 37
2.4 Il gruppo di Galois. 39
2.4.1 Definizione moderna. 39
2.4.2 Il gruppo di Galois *à la Galois*. 41
Esercizi 45
2.5 La corrispondenza di Galois. 48
Esercizi 52

3 Risolubilità per radicali delle equazioni algebriche. 55
3.1 La strategia di Galois. 55
3.2 Estensioni cicliche, p-pure. 58
Esercizi 60
3.3 Estensioni ciclotomiche. 63
Esercizi 66
3.4 Estensioni radicali. 67
Esercizi 70
3.5 Il teorema di Galois. 71
Esercizi 76

Parte II Il problema inverso

4 Il problema inverso di Galois. 81
4.1 Il problema inverso. 81
4.1.1 Il problema generale. 81
4.1.2 Il problema inverso effettivo. 82
4.1.3 Gradi delle realizzazioni. 83
Esercizi 84
4.2 Un teorema di Dedekind. 86
4.2.1 Richiami sulle risolventi di Galois. 86
4.2.2 La risolvente di Galois generica. 87
4.2.3 Dimostrazione del teorema di Dedekind. 90
Esercizi 92
4.3 Realizzazioni del gruppo simmetrico. 94
4.3.1 Il teorema di irriducibilità di Hilbert. 94
4.3.2 Realizzazioni di S_n con il teorema di Dedekind. 96
Esercizi 97
4.4 Il problema inverso per i gruppi abeliani. 99
Esercizi 102

5 La classificazione dei gruppi finiti non è finita! 105
5.1 Il teorema di Jordan-Hölder. 105
Esercizi 108
5.2 Gruppi semplici. 109
5.2.1 Gruppi semplici abeliani 109
5.2.2 I gruppi alterni $\mathcal{A}_n$. 109
5.2.3 I gruppi di tipo Lie. 111
Esercizi 113
5.3 Il teorema enorme. 117
5.3.1 Rappresentazioni transitive e gruppi di Mathieu. 117
5.3.2 Gruppi sporadici. 118
Esercizi 120

6 Curve ellittiche e rappresentazioni di Galois. 125
6.1 Preliminari. 125
6.2 Legge di gruppo sulle cubiche liscie. 127
6.3 Forma di Weierstrass, rappresentazioni affini. 129
6.4 Punti di ordine n, i vari avatar delle curve ellittiche. 132
6.5 Rappresentazioni di Galois. 135

Bibliografia 141

Parte I

Teoria di Galois.

1

Risoluzione delle equazioni algebriche di grado basso.

1.1 L'equazione del secondo grado.

Conosciamo tutti la formula risolutiva dell'equazione del secondo grado:

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

Le soluzioni (o le radici) sono date dalla formula:

$$r_1, r_2 = \frac{-b \pm \sqrt{\Delta}}{2a} \tag{1.1}$$

dove $\Delta = b^2 - 4ac$.

Per trovare questa formula si può ragionare così: se si riuscisse, ponendo $x = y - \alpha$, a cancellare il termine del primo grado, si arriverebbe ad un'equazione della forma:

$$a'y^2 - c' = 0$$

di facile risoluzione. Abbiamo:

Osservazione 1.1. Consideriamo il caso generale, sia: $ax^n + bx^{n-1} + cx^{n-2} + ...$ un polinomio di grado n ($a \neq 0$). Cerchiamo α tale che ponendo $x = y - \alpha$ si ottenga un polinomio della forma: $a'y^n + c'y^{n-2} + ...$ (ossia senza termine in y^{n-1}).
Facciamo la sostituzione:
$a(y-\alpha)^n + b(y-\alpha)^{n-1} + c(y-\alpha)^{n-2} + ...$
Sviluppando vediamo che y^n si trova solo nel primo termine, con coefficiente a. Invece y^{n-1} compare solo nei primi due termini: nel primo il suo coefficiente è $-\alpha na$ (formula del binomio), nel secondo è: b. In conclusione viene:
$ay^n + (b - \alpha na)y^{n-1} + c'y^{n-2} + ...$ e basta prendere: $\alpha = \frac{b}{na}$.

Detto ciò, si pone $x = y - \frac{b}{2a}$ e la nostra equazione diventa:

$$ay^2 + \frac{b^2}{4a} - \frac{b^2}{2a} + c = 0$$

ossia:

$$y^2 = \frac{b^2 - 4ac}{4a^2}$$

e ritroviamo la formula (1.1). Le radici sono espresse in funzione dei coefficienti usando le quattro operazioni e un radicale (radice quadrata): è la *risoluzione per radicali* dell'equazione del secondo grado. Tutto questo era noto dall'antichità.

1.2 L'equazione del terzo grado.

La risoluzione per radicali dell'equazione del terzo grado è invece nettamente più difficile.

Consideriamo adesso un'equazione del terzo gardo:

$$ax^3 + bx^2 + cx + d = 0$$

Il problema è di trovare una formula analoga a (1.1) che ci dia almeno una soluzione. Infatti se abbiamo una soluzione, r_1, allora:

$$ax^3 + bx^2 + cx + d = (x - r_1)(\alpha x^2 + \beta x + \gamma)$$

e siamo ricondotti a cercare le soluzioni di: $\alpha x^2 + \beta x + \gamma = 0$, cosa che sappiamo fare. L'esperienza precedente suggerisce di eliminare il termine in x^2 usando 1.1. Infatti ponendo $x = y - \frac{b}{3a}$ si ottiene un'espressione della forma:

$$ay^3 + c'y + d' = 0$$

Siccome $a \neq 0$:

$$ay^3 + c'y + d' = 0 \Leftrightarrow a(y^3 + \frac{c'}{a}y + \frac{d'}{a}) = 0 \Leftrightarrow y^3 + \frac{c'}{a}y + \frac{d'}{a} = 0$$

Ci siamo quindi ricondotti a risolvere un'equazione della forma:

$$y^3 + my = n \tag{1.2}$$

Una soluzione, y_0, di questa soluzione fornisce una radice, $x_0 = y_0 - \frac{b}{3a}$, dell'equazione iniziale. Questi fatti, non espressi in questo modo, erano ben noti dagli algebristi italiani del Medioevo. L'idea di Cardano (1501-1576) per risolvere l'equazione (1.2) si basa sull'identità algebrica:

$$(t - u)^3 = t^3 + 3ut(u - t) - u^3$$

Questa identità non è altro che lo sviluppo binomiale ma sembra che Cardano la vedesse diversamente, geometricamente, come la divisione di un cubo in due cubi e quattro parallelepipedi ($t^3 = u^3 + (t-u)^3 + 2tu(u-t) + u^2(u-t) + u(u-t)$). Comunque sia ponendo $y = t - u$:

$$y^3 = t^3 - 3uty - u^3 \tag{1.3}$$

E poi ponendo:

$$(i)\ 3ut = m \quad (ii)\ n = t^3 - u^3 \tag{1.4}$$

si ritrova la nostra equazione $y^3 + my = n$. Il problema adesso è di risolvere (i) e (ii), cioè di calcolare u e t in funzione di m e n.

Da (i): $u = \frac{m}{3t}$, inserendo in (ii): $n = t^3 - \frac{m^3}{27t^3}$, moltiplicando per t^3:

$$t^6 - t^3 n - \frac{m^3}{27} = 0 \tag{1.5}$$

È successo un miracolo! L'equazione è del sesto grado e sembra che abbiamo peggiorato le cose, ma, ponendo $X = t^3$ ci ritroviamo con un'equazione del secondo grado:

$$X^2 - nX - \frac{m^3}{27} = 0 \tag{1.6}$$

Le soluzioni di questa equazione sono:

$$X_{1,2} = \frac{(n \pm \sqrt{n^2 + \frac{4m^3}{27}})}{2} = \frac{n}{2} \pm \sqrt{\frac{n^2}{4} + \frac{m^3}{27}}$$

Considerando solo la soluzione con il $+$:

$$t^3 = \frac{n}{2} + \sqrt{\frac{n^2}{4} + \frac{m^3}{27}} \tag{1.7}$$

e quindi:

$$t = \sqrt[3]{\frac{n}{2} + \sqrt{\frac{n^2}{4} + \frac{m^3}{27}}}$$

Adesso da (ii): $u^3 = t^3 - n = \frac{n}{2} + \sqrt{\frac{n^2}{4} + \frac{m^3}{27}} - n$, e quindi:

$$u = \sqrt[3]{-\frac{n}{2} + \sqrt{\frac{n^2}{4} + \frac{m^3}{27}}}$$

Finalmente siccome $y = t - u$ otteniamo:

$$y = \sqrt[3]{\frac{n}{2} + \sqrt{\frac{n^2}{4} + \frac{m^3}{27}}} - \sqrt[3]{-\frac{n}{2} + \sqrt{\frac{n^2}{4} + \frac{m^3}{27}}} \tag{1.8}$$

La formula (1.8) (*formula di Cardano*) ci dà quindi una soluzione dell'equazione $y^3 + my = n$ e quindi dell'equazione cubica generale.

Ci sono però alcuni problemi con questa formula:

Per esempio, cosa succede se $\frac{n^2}{4} + \frac{m^3}{27} < 0$?

Infatti in questo caso non possiamo prendere la radice quadrata. Questo sembra volere dire, come nel caso del secondo grado, che l'equazione non ha nessuna soluzione reale. Questo però cozza con il seguente fatto:

Lemma 1.2. *Ogni polinomio a coefficienti reali di grado dispari ha una radice reale.*

Dimostrazione (Dimostrazione). Sia $P(x) = a_n x^n + ... + a_0$ con n dispari e $a_n \neq 0$. Moltiplicando per -1 non si cambiano le radici, quindi possiamo assumere $a_n > 0$. Abbiamo: $\lim_{x \to +\infty} P(x) = +\infty$ e $\lim_{x \to -\infty} P(x) = -\infty$. Siccome $P(x)$ è continua, per il teorema del valore medio, esiste $x_o \in \mathbb{R}$ tale che $P(x_0) = 0$.

Quindi *ogni* equazione cubica a coefficienti reali ha sempre almeno una radice reale. Ma in certi casi la formula di Cardano sembra non funzionare. Per esempio consideriamo l'equazione:

$$x^3 - 15x = 4 \quad (m = -15, n = 4)$$

Applicando la formula (1.8) si trova:

$$x = \sqrt[3]{2 + \sqrt{-121}} - \sqrt[3]{-2 + \sqrt{-121}}$$

Questo è un vero peccato perchè la nostra equazione ha, non una, ma ben tre radici reali: $x^3 - 15x - 4 = (x - 4)(x^2 + 4x + 1)$.

Per risolvere questo grattacapo gli algebristi italiani Cardano e soprattutto Bombelli ebbero l'idea geniale di introdurre un artefizio (*un escamotage*) di calcolo, specificatamente una *quantità immaginaria* (non reale), i, radice di -1. Quindi:

$$i^2 = -1$$

Adesso $\sqrt{-121} = \sqrt{i^2.11^2} = \pm i.11$. Come si calcola con questa quantità immaginaria? Esattamente come se i fosse un numero reale qualsiasi, tranne che bisogna tenere conto della relazione $i^2 = -1$. Per esempio:

$(2 + i)^3 = (2 + i)^2.(2 + i) = (3 + 4i).(2 + i) = 2 + 11i$. Quindi possiamo dire che:

$$\sqrt[3]{2 + \sqrt{-121}} = \sqrt[3]{2 + 11i} = 2 + i$$

Nello stesso modo:

$$\sqrt[3]{-2+\sqrt{-121}} = \sqrt[3]{-2+11i} = -2+i$$

Adesso se riscriviamo la soluzione data dalla formula di Cardano:

$$x = \sqrt[3]{2+\sqrt{-121}} - \sqrt[3]{-2+\sqrt{-121}} = (2+i)-(-2+i) = 4$$

Un altro miracolo! La quantità immaginaria i è scomparsa e 4 è ben una radice reale della nostra equazione!

Osserviamo che questo trucco funzionerà sempre: la soluzione di Cardano è della forma: $\sqrt[3]{a+\sqrt{-b}} - \sqrt[3]{-a+\sqrt{-b}}$. Se $b<0$ siamo a posto, possiamo prendere la radice quadrata e poi la radice cubica la quale è sempre definita. Se $b>0$, scriviamo: $a+\sqrt{-b} = a+i\sqrt{b}$ e cerchiamo $z=\alpha+i\beta$ tale che $z^3 = a+ic$ dove $c=\sqrt{b}$. Non è facile trovare z ma supponiamo di averlo, allora:

$$(\alpha+i\beta)^3 = (-\alpha^3+3\alpha\beta^2)+i(3\alpha^2\beta-\beta^3) = a+ic$$

Si verifica facilmente che se $z' = -\alpha+i\beta$, allora $(z')^3 = -a+ic$ e la formula di Cardano diventa: $x = (\alpha+i\beta)-(-\alpha+i\beta) = 2\alpha$, la quantità immaginaria è scomparsa ed abbiamo una radice reale dell'equazione.

Rimane quindi da trovare z tale che $z^3 = a+ic$. Dividendo tutto per $\sqrt{a^2+c^2}$ possiamo assumere: $a^2+c^2 = 1$. Quindi il punto di coordinate (a,c) è sulla circonferenza unitaria. Se guardiamo alla circonferenza come alla circonferenza trigonometrica, vediamo che esiste θ tale che: $a = cos\theta$, $c = sen\theta$. Detto diversamente: da $a^2+c^2=1$, segue che $|a|\leq 1$, quindi esiste θ tale che: $a = cos\theta$, dalla relazione: $a^2+c^2 = 1 = (cos\theta)^2+(sen\theta)^2$ viene $c^2 = (sen\theta)^2$ e possiamo scrivere: $c = sen\theta$. Abbiamo quindi: $a+ic = cos\theta+isen\theta$. Usando le formule di duplicazioni:

$$cos2\alpha = (cos\alpha)^2-(sen\alpha)^2\,,\ sen2\alpha = 2cos\alpha sen\alpha$$

si verifica con un pò di conti che: $z = cos\frac{\theta}{3}+isen\frac{\theta}{3}$ soddisfa: $z^3 = a+ic$ (scrivere $cos\theta = cos(\frac{\theta}{3}+\frac{2\theta}{3})$ ed usare le formule di duplicazione, nell'espressione risultante scrivere: $cos(\frac{2\theta}{3}) = cos(\frac{\theta}{3}+\frac{\theta}{3})$ (idem per sen) e usare ancora una volta le formule di duplicazione).

In conclusione, grazie all'artefizio della *quantità immaginaria* la formula di Cardano fornisce sempre una soluzione reale dell'equazione cubica.

1.3 L'equazione del quarto grado.

Forti di questo successo i nostri si sono lanciati all'attacco dell'equazione del quarto grado. Sembra che sia stato Ferrari ad avere risolto per primo l'equazione del quarto grado (1545 ca). Ci limiteremo (secondo un approccio

dovuto a Descartes (1637)) ad indicare brevemente come sia possibile trovare una soluzione dell'equazione del quarto grado, sempre che questo sia possibile. Infatti contrariamente all'equazione cubica, alcune equazioni quartiche non ammettono nessuna radice reale (per esempio $x^4 + 1 = 0$ non ammette radici reali). Come nel caso della cubica ci riduciamo a studiare equazioni del tipo: $x^4+bx^2+cx+d = 0$ (cf Oss. 1.1). Si cerca di scrivere la nostra equazione come un prodotto di due equazioni del secondo grado:

$$x^4 + bx^2 + cx + d = (x^2 + \alpha x + \beta)\dot{(}x^2 + \gamma x + \delta)$$

Il problema è di determinare $\alpha, \beta, \gamma, \delta$ in funzione di b, c, d.
Uguagliando i coefficienti si ottiene il sistema:

$$\begin{cases} \gamma = -\alpha \\ \delta + \alpha\gamma + \beta = b = \delta - \alpha^2 + \beta \\ \alpha\delta + \beta\gamma = c = \alpha\delta - \alpha\beta \\ \beta\delta = d \end{cases}$$

Consideriamo la seconda e la terza equazione:

$$\begin{cases} \delta = \alpha^2 - \beta + b \quad (i) \\ \delta = \beta + \frac{c}{\alpha} \quad (ii) \end{cases}$$

Facendo $(i) + (ii)$ viene: $2\delta\alpha^2 + b + \frac{c}{\alpha}$ mentre $(ii) - (i)$ fornisce: $2\beta = \alpha^2 + b - \frac{c}{\alpha}$. Dall'ultima equazione del sistema:

$$4d = (\alpha^2 + b + \frac{c}{\alpha})(\alpha^2 + b - \frac{c}{\alpha})$$

cioè:

$$\alpha^4 + 2\alpha^2 b + b^2 - \frac{c^2}{\alpha^2} = 4d$$

Moltiplicando per α^2 e riordinando:

$$\alpha^6 + 2\alpha^4 b + \alpha^2(b^2 - 4d) - c^2 = 0$$

Ponendo $X = \alpha^2$ troviamo un'equazione cubica:

$$X^3 + 2X^2 b + X(b^2 - 4d) - c^2 = 0$$

Usando il metodo di Cardano possiamo calcolare una soluzione reale, x_0, di questa equazione cubica e quindi $\alpha^2 = x_0$ e quindi (se $x_0 \geq 0$): $\alpha = \sqrt{x_0}$. Usando (i) e (ii) ricaviamo: $\delta = \frac{1}{2}(b + x_0 + \frac{c}{\sqrt{x_0}})$ e $\beta = \frac{1}{2}(b + x_0 - \frac{c}{\sqrt{x_0}})$. Abbiamo quindi scritto (se $x_0 \geq 0$) la nostra equazione come un prodotto di due equazioni del secondo grado. Si conclude con la formula (1.1).

1.4 Conclusione (provvisoria).

I risultati delle sezioni precedenti mostrano che le equazioni del secondo, terzo e quarto grado possono essere risolte con formule *per radicali*. Certo rimangono qualche zone d'ombra: abbiamo sorvolato su certi problemi di segni prendendo le radici quadrate, l'uso della *quantità immaginaria i* è un pò disinvolto. Inoltre non abbiamo, nel caso del terzo e del quarto grado, scritto una formula che dia *tutte* le radici dell'equazione. È chiaro tuttavia che una tale formula esiste e anche che è particolarmente orribile e di poco interesse nella pratica! Quello che invece è importante è che esista. Questo comunque era lo stato dell'arte nel Medioevo dopo i lavori degli algebristi italiani.

Come spesso succede in matematica gli sforzi per risolvere un problema importante portano frutti che vanno ben oltre la soluzione ricercata. Il lavoro degli algebristi italiani ha permesso non solo di risolvere l'equazione del terzo grado, ma soprattutto ha introdotto i numeri complessi e il sentimento che questi numeri immaginari potessero dare una qualche armonia alla teoria delle equazioni algebriche. Infatti se si considera l'equazione del secondo grado è chiaro che, anche se $\Delta < 0$, l'equazione ha comunque *due* soluzioni nell'ambito dei numeri immaginari. Segue che un'equazione del terzo grado ha sempre (nell'ambito dei numeri immaginari) tre radici. Visto che possiamo sempre trovare una radice quadrata (nell'ambito dei numeri immaginari) anche l'equazione del quarto grado ha sempre quattro radici (se nella dimostrazione precedente $x_0 < 0$, si prende $\alpha = i\sqrt{-x_0}$). Viene quindi naturale chiedersi se questa situazione si generalizza.

Bisognerà aspettare Gauss (1777-1855) per avere una teoria consistente dei numeri immaginari (o *numeri complessi* come vengono chiamati oggi) e una, anzi tre, dimostrazioni del *teorema fondamentale dell'algebra*.

I risultati delle sezioni precedenti implicano che data una (qualsiasi) equazione di grado ≤ 4, le soluzioni (reali, quando esistono) di questa equazione possono essere espresse come funzioni *radicali* dei coefficienti. È naturale chiedersi se una tale affermazione è ancora valida per equazioni di grado ≥ 5. Bisognerà aspettare Abel (1802-1829) e soprattutto Galois (1811-1832) per avere una risposta esauriente a questo problema. Ma stiamo correndo un pò troppo: la nostra piccola introduzione storica non è ancora finita...

1.5 Il teorema delle funzioni simmetriche.

Nel XVIII° secolo vari matematici tra cui Ruffini, Vandermonde e soprattutto Lagrange hanno ripreso lo studio della risoluzione delle equazioni algebriche da un nuovo punto di vista reso possibile dal teorema (essenzialmente dovuto a Newton) sulle funzioni simmetriche.

L'osservazione di partenza, molto semplice, è la seguente:
sia $P(x) = x^n + a_{n-1}x^{n-1} + ... + a_0$ un polinomio con n radici $r_1, ..., r_n$, allora:

$$P(x) = x^n + a_{n-1}x^{n-1} + ... + a_0 = (x - r_1)(x - r_2)...(x - r_n)$$

Svolgendo ed uguagliando i coefficienti:

$$-a_{n-1} = r_1 + ... + r_n$$

$$a_{n-2} = r_1 r_2 + ... + r_{n-1} r_n = \sum (\Pi_{1 \leq i < j \leq n} r_i r_j)$$

$$.....$$

$$(-1)^i a_{n-i} = \sum (\Pi_{1 \leq t_1 < ... < t_i \leq n} r_{t_1} ... r_{t_i})$$

$$.....$$

$$(-1)^n a_0 = r_1 r_2 ... r_n$$

Per esempio se $n = 2$:

$$x^2 + a_1 x + a_0 = (x - r_1)(x - r_2)$$

$$-a_1 = r_1 + r_2$$

$$a_0 = r_1 r_2$$

Se $n = 3$:

$$x^3 + a_2 x^2 + a_1 x + a_0 = (x - r_1)(x - r_2)(x - r_3)$$

$$-a_2 = r_1 + r_2 + r_3$$

$$a_1 = r_1 r_2 + r_1 r_3 + r_2 r_3$$

$$-a_0 = r_1 r_2 r_3$$

Quindi i coefficienti, a_j, del polinomio si esprimono come dei polinomi nelle radici: $(-1)^i a_{n-i} = e_i(r_1, ..., r_n)$ dove $e_i(X_1, ..., X_n) = \sum (\Pi_{1 \leq t_1 < ... < t_i \leq n} X_{t_1} ... X_{t_i})$.

<u>Ovviamente</u> queste espressioni *non dipendono dall'ordine in cui prendiamo le radici.*

Queste espressioni (cioè i polinomi $e_i(X_1, ..., X_n)$) sono gli stessi per ogni polinomio di grado n con n radici. Dal teorema fondamentale dell'algebra sappiamo che ogni polinomio $P(x) \in \mathbb{R}[X]$, con $grado(P) = n$, ha n radici in $\mathbb{C}$.

Concludiamo pertanto che i polinomi $e_i(X_1, ..., X_n)$ sono *simmetrici* nelle variabili $X_1, ..., X_n$, cioè se ordinamio le variabili in un altro modo, il polinomio non cambia. Per esempio $e_2(X_1, X_2, X_3) = X_1 X_2 + X_1 X_3 + X_2 X_3$. Se scambiamo X_1 e X_2: $e_2(X_2, X_1, X_3) = X_2 X_1 + X_2 X_3 + X_1 X_3$ e quindi $e_2(X_1, X_2, X_3) = e_2(X_2, X_1, X_3)$.

Una permutazione delle variabili $X_1, ..., X_n$ corrisponde ad una biiezione $\sigma : \{1, 2, ..., n\} \to \{1, 2, ..., n\}$, cioè un altro modo di ordinare le variabili:

$$X_{\sigma(1)}, ..., X_{\sigma(n)}.$$

Definizione 1.3. *Un polinomio $P(X_1, ..., X_n)$ è simmetrico se:*

$$P(X_1, ..., X_n) = P(X_{\sigma(1)}, ..., X_{\sigma(n)}) \quad \forall \sigma \in S_n$$

Osservazione 1.4. Ovviamente i polinomi simmetrici elementari $e_i(X_1, ..., X_n)$ sono simmetrici, ma ne esistono altri. Per esempio $X_1^2 + ... + X_n^2$ è simmetrico, non elementare.

Il risultato principale sui polinomi simmetrici è il seguente teorema (essenzialmente noto a Newton (1642-1727)):

Teorema 1.5. (Teorema delle funzioni simmetriche)
Sia $P(X_1, ..., X_n) \in k[X_1, ..., X_n]$ un polinomio simmetrico. Allora esiste un polinomio (non necessariamente simmetrico) $h(X_1, ..., X_n) \in k[X_1, ..., X_n]$ tale che:

$$P(X_1, ..., X_n) = h(e_1(X_1, ..., X_n), ..., e_n(X_1, ..., X_n))$$

dove gli $e_i(X_1, ..., X_n)$ sono i polinomi simmetrici elementari. Inoltre se i coefficienti di P sono interi, anche h può essere preso a coefficienti interi.

Risolvere l'equazione algebrica $f(x) = 0$ dove $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$ significa essenzialmente esprimere le radici r_i in funzione dei coefficienti a_j. Noi invece abbiamo un modo di esprimere i coefficienti a_j in funzione delle radici r_i ($(-1)^i a_{n-i} = e_i(r_1, ..., r_n)$). Per risolvere bisogna invertire questo processo e il Teorema 1.5 può tornare utile:

Lemma 1.6. *Sia $f(x) \in k[x]$ e siano $\alpha_1, \cdots, \alpha_n$ le radici di f.*
Se $P(X_1, \cdots, X_n) \in k[X_1, \cdots, X_n]$ è simmetrico, allora:

$$P(\alpha_1, \cdots, \alpha_n) \in k.$$

Dimostrazione (Dimostrazione). Per il Teorema 1.5 esiste $h(X_1, \cdots, X_n) \in k[X_1, \cdots, X_n]$ tale che $P(X_1, \cdots, X_n) = h(e_1(X_1, \cdots, X_n), \cdots, e_n(X_1, \cdots, X_n))$, quindi:
$P(\alpha_1, \cdots, \alpha_n) = h(e_1(\alpha_1, \cdots, \alpha_n), \cdots, e_n(\alpha_1, \cdots, \alpha_n))$. Si conclude perchè gli $e_i(\alpha_1, \cdots, \alpha_n)$ sono (modulo il segno) i coefficienti di f quindi elementi di k.

Quindi se abbiamo, per esempio, $f(x) \in \mathbb{Q}[x]$ con radici complesse $\alpha_1, ..., \alpha_n$, allora per ogni polinomio simmetrico $P(X_1, ..., X_n)$ a coefficienti <u>razionali</u>,
$P(\alpha_1, ..., \alpha_n)$ è un numero razionale.
In particolare se riusciamo ad esprimere le radici α_i nella forma

$$\alpha_i = \varphi_i(h_1(\alpha_1, ..., \alpha_n), ..., h_t(\alpha_1, ..., \alpha_n))$$

dove h_i è un polinomio simmetrico a coefficienti razionali e dove φ_i è una funzionale costruita con le quattro operazioni e le estrazioni di radici, allora

avremo espresso le radici in funzione dei coefficienti *razionalmente* (su $\mathbb{Q}$), *per radicali*, cioè avremo risolto $f(x) = 0$ per radicali.

Facciamo un esempio:

Consideriamo l'equazione del secondo grado $X^2+bX+c = (X-r_1)(X-r_2)$. Abbiamo:

$$-b = r_1 + r_2 =: e_1, \quad c = r_1 r_2 =: e_2.$$

Possiamo scrivere: $r_1 = \frac{1}{2}[(r_1 + r_2) + (r_1 - r_2)]$, cioè:

$$r_1 = \frac{1}{2}[e_1 + (r_1 - r_2)].$$

Il polinomio $P(r_1, r_2) = r_1 - r_2$ non è simmetrico, ma $(r_1 - r_2)^2$ lo è. Inoltre $\sqrt{(r_1 - r_2)^2} = \pm(r_1 - r_2)$, quindi, prendendo il segno giusto:

$$r_1 = \frac{1}{2}[e_1 + \sqrt{(r_1 - r_2)^2}]$$

Adesso $(r_1 - r_2)^2$ essendo simmetrico dal Teorema 1.5, esiste un polinomio h tale che: $(r_1 - r_2)^2 = h(e_1, e_2)$. Quindi:

$$r_1 = \frac{1}{2}[e_1 + \sqrt{h(e_1, e_2)}] = \frac{1}{2}[-b + \sqrt{h(-b, c)}]$$

e abbiamo espresso r_1 in funzione dei coefficienti b, c!

Per completezza: $(r_1 - r_2)^2 = (r_1 + r_2)^2 - 4r_1 r_2 = e_1^2 - 4e_2$ e ritroviamo la nostra vecchia formula:

$$r_1 = \frac{1}{2}[-b + \sqrt{b^2 - 4c}]$$

(con $\sqrt{(r_1 - r_2)^2} = -(r_1 - r_2)$ si trova l'altra radice r_2).

1.5.1 La risolvente di Lagrange.

Forti di questo successo, riprendiamo, seguendo Lagrange, il caso dell'equazione cubica:

$$X^3 + aX^2 + bX + c = (X - r_1)(X - r_2)(X - r_3)$$

dove:

$$\begin{cases} -a = r_1 + r_2 + r_3 =: e_1 \\ b \quad = r_1 r_2 + r_1 r_3 + r_2 r_3 =: e_2 \\ -c = r_1 r_2 r_3 =: e_3 \end{cases}$$

L'equazione $X^3 = 1$ ha tre radici complesse, siccome $X^3-1 = (X-1)(X^2+X+1)$ queste radici sono $1, \alpha, \overline{\alpha}$, dove $\alpha = \frac{-1+i\sqrt{3}}{2}$ verifica $\alpha^2 + \alpha + 1 = 0$ (α è una *radice cubica primitiva dell'unità*). Detto ciò possiamo scrivere:

$$r_1 = \frac{1}{3}[(r_1 + r_2 + r_3) + (r_1 + \alpha r_2 + \alpha^2 r_3) + (r_1 + \alpha^2 r_2 + \alpha r_3)]$$

Infatti il termine tra le parentesi quadre vale: $3r_1 + r_2(1 + \alpha + \alpha^2) + r_3(1 + \alpha + \alpha^2) = 3r_1$. È la formula analoga a quella usata nel caso dell'equazione del secondo grado (-1 è radice primitiva quadrata dell'unità).

Le espressioni $r_1 + \alpha r_2 + \alpha^2 r_3$, $r_1 + \alpha^2 r_2 + \alpha r_3$ non sono simmetriche negli r_i. Pertanto consideriamo:

$$u = (r_1 + \alpha r_2 + \alpha^2 r_3)^3, \;\; v = (r_1 + \alpha^2 r_2 + \alpha r_3)^3$$

Neanche u, v sono simmetrici negli r_i ma $u + v$ e uv lo sono.

Infatti se scambiamo r_2 con r_3 (cioè applichiamo la trasposizione τ_1), allora $\tau_1(u) = v$ e $\tau_1(v) = u$. Se applichiamo la permutazione circolare γ_2: $r_1 \to r_3 \to r_2 \to r_1$, allora:

$$\gamma_2(u) = (r_3 + \alpha r_1 + \alpha^2 r_2)^3 = (\alpha(r_1 + \alpha r_2 + \alpha^2 r_3))^3 = \alpha^3 u = u$$

Nello stesso modo: $\gamma_2(v) = v$. Pertanto: $\tau_1(u+v) = u+v, \tau_1(uv) = uv, \gamma_2(u+v) = u + v, \gamma_2(uv) = uv$. Adesso basta osservare che ogni elemento di S_3 si ottiene in funzione di τ_1, γ_2: con notazioni che parlano da sé: $\tau_2 = \gamma_2\tau_1$, $\tau_3 = \tau_1\gamma_2$ e $\gamma_1 = \gamma_2^2$. Pertanto se $\sigma \in S_3$, $\sigma(u + v) = u + v$ e $\sigma(uv) = uv$.

Dal Teorema 1.5 esistono dei polinomi h, g (a coefficienti in $\mathbb{Q}(\alpha)$) tali che: $u + v = h(e_1, e_2, e_3)$, $uv = g(e_1, e_2, e_3)$, cioè: $u + v = h(-a, b, -c), uv = g(-a, b, -c)$.

Adesso u e v sono radici dell'equazione:

$$X^2 - (u + v)X + uv = 0$$

Quindi:

$$u, v = \frac{1}{2}[h(-a, b, -c) \pm \sqrt{h(-a, b, -c)^2 - 4g(-a, b, -c)}]$$

Siccome:

$$r_1 = \frac{1}{3}[-a +^3 \sqrt{u} +^3 \sqrt{v}]$$

abbiamo espresso r_1 in funzione dei coefficienti a, b, c *per radicali* cioè con una formula che comprende le quattro operazioni e l'estrazione di radici (quadratiche e cubiche). Inoltre se $a, b, c \in \mathbb{Q}$, allora la formula contiene solo numeri razionali e potenze di α (h, g possono essere presi con coefficienti in $\mathbb{Q}(\alpha)$, cf Teorema 1.5). Abbiamo quindi risolto per radicali l'equazione cubica, non su $\mathbb{Q}$ ma su $\mathbb{Q}(\alpha)$. Il fatto di dovere considerare α alla stregua di un numero razionale (cioè una *quantità nota*) era assolutamente naturale per Lagrange e i suoi contemporanei.

Riprendendo tutto con un pò di ordine vediamo profilarsi un metodo per affrontare il caso generale.

Con le notazioni precedenti poniamo:

$$t := r_1 + \alpha r_2 + \alpha^2 r_3 \quad (\textit{risolvente di Lagrange})$$

Se permutiamo le radici r_i abbiamo $3! = 6$ valori:

$$\begin{array}{l} Id(t) = t_1 = r_1 + \alpha r_2 + \alpha^2 r_3 \\ \gamma_2(t) = t_2 = r_3 + \alpha r_1 + \alpha^2 r_2 = \alpha t_1 \\ \gamma_1(t) = t_3 = r_2 + \alpha r_3 + \alpha^2 r_1 = \alpha^2 t_1 \\ \tau_1(t) = t_4 = r_1 + \alpha r_3 + \alpha^2 r_2 \\ \tau_3(t) = t_5 = r_2 + \alpha r_1 + \alpha^2 r_3 = \alpha t_4 \\ \tau_2(t) = t_6 = r_3 + \alpha r_2 + \alpha^2 r_1 = \alpha^2 t_4 \end{array}$$

Questi sei valori sono ovviamente radici dell'equazione del sesto grado:

$$F(X) = (X - t_1)(X - t_2)...(X - t_6) \quad (\textit{equazione risolvente di Lagrange})$$

I coefficienti, A_k, di F sono (modulo il segno) i polinomi elementari nelle radici: $A_k = e_k(t_1, ..., t_6)$ e ogni t_j è un polinomio nelle radici r_i. Quindi $A_k = e_k(t_1(r_1, r_2, r_3), ..., t_6(r_1, r_2, r_3))$. Se si applica una permutazione, σ delle radici r_i questo torna a permutare i t_j (perchè $t_j = \tau(t)$, quindi $\sigma(t_j) = \sigma(\tau(t))$) e si ottiene $e_k(t_{\sigma(1)}, ..., t_{\sigma(6)})$, siccome gli e_k sono simmetrici: $e_k(t_{\sigma(1)}, ..., t_{\sigma(6)}) = e_k(t_1, ..., t_6) = A_k$. Quindi i coefficienti A_k di $F(X)$ sono polinomi simmetrici nelle radici r_i, pertanto $A_k = h(e_k(r_i)) = h(a_k)$ (a_k sono i coefficienti della nostra cubica).

Siccome la nostra cubica era a coefficienti razionali, concludiamo che:

$$F(X) \in k[X], \ k = \mathbb{Q}(\alpha).$$

Se riusciamo a risolvere per radicali l'equazione $F(X) = 0$ allora avremo le radici di $F(X)$ cioè i t_i espressi per radicali in funzione dei coefficienti A_k di F. Siccome $A_k = h(a_k)$, avremo t_i espresso per radicali in funzione dei coefficienti della nostra cubica iniziale. Rimane solo da recuperare le radici r_i conoscendo i t_i, ma le radici sono $\frac{1}{3}[e_1 + t_1 + t_4]$, $\frac{1}{3}[e_1 + \alpha^2 t_1 + \alpha t_4]$, $\frac{1}{3}[e_1 + \alpha t_1 + \alpha^2 t_4]$. Quindi una volta ottenuti $t_1, ..., t_6$ rimane solo da individuare t_1 e t_4.

Per risolvere $F(X) = 0$, equazione del sesto grado in X, osserviamo che: $(X - t)(X - \alpha t)(X - \alpha^2 t) = X^3 - t^3$ (infatti $t^3(\frac{X}{t} - 1)(\frac{X}{t} - \alpha)(\frac{X}{t} - \alpha^2) = t^3[(\frac{X}{t})^3 - 1]$). Quindi: $(X - t_1)(X - t_2)(X - t_3) = (X - t_1)(X - \alpha t_1)(X - \alpha^2 t_1) = X^3 - t_1^3$. In modo analogo: $(X - t_4)(X - t_5)(X - t_6) = X^3 - t_4^3$. In conclusione:

$$F(X) = (X^3 - t_1^3)(X^3 - t_4^3)$$

è un'equazione di grado *due* in X^3 (con le notazioni precedenti $u = t_1^3$, $v = t_4^3$ e $F(X) = Y^2 - (u + v)Y + uv$, dove $Y = X^3$). Quindi basta risolvere e prendere le radici cubiche delle soluzioni.

Passiamo adesso al caso generale di un'equazione di grado n.

Poniamo: $t = r_1 + \alpha r_2 + ... + \alpha^{n-1} r_n$, dove α è una radice primitiva n-esima dell'unità. Permutando le radici r_i abbiamo $n!$ valori: $\sigma(t) = r_{\sigma(1)} + \alpha r_{\sigma(2)} + ... + \alpha^{n-1} r_{\sigma(n)}$, $\sigma \in S_n$, che sono radici dell'equazione: $F(X) = \prod_{\sigma \in S_n} (X - \sigma(t))$, quest'equazione ha grado $n!$.

Tra i $\sigma(t)$ abbiamo $\alpha t, \alpha^2 t, ..., \alpha^{n-1} t, t = \alpha^n t$. Osserviamo che in $\alpha^i t$ il coefficiente di r_{n+1-i} vale uno e che $\prod_{1 \le i \le n} (X - \alpha^i t) = X^n - t^n$. Quindi per ogni permutazione, τ, di $r_2, ..., r_n$ abbiamo un $\tau(t)$ nel quale il coefficiente di r_1 è uno. Abbiamo $(n-1)!$ tali $\tau(t)$. Poi per ogni $\tau(t)$ abbiamo $\alpha\tau(t), ..., \alpha^n \tau(t)$, e queste sono le nostre $n! = n(n-1)!$ permutazioni. In conclusione: $F(X) = \prod_{\tau \in S_{n-1}} (X^n - \tau(t)^n)$ è un'equazione di grado $(n-1)!$ in $Y = X^n$.

Se riusciamo a risolvere conosciamo i $\tau(t)^n$, prendendo la radice n-esima opportuna abbiamo i $\tau(t)$; a questo punto possiamo recuperare le radici $r_1, ..., r_n$; in realtà bastano n opportuni $\tau(t)$ per recuperare le radici:

Lemma 1.7. *Sia K un'estensione finita di $\mathbb{Q}$ contenente una radice primitiva n-esima dell'unità, α. Siano $b_1, ..., b_n \in K$. Il sistema lineare:*

$$\begin{cases} x_1 + x_2 + x_3 + ... + x_n & = b_1 \\ x_1 + \alpha x_2 + \alpha^2 x_3 + ... + \alpha^{n-1} x_n & = b_2 \\ \vdots & \vdots \quad \vdots \\ x_1 + \alpha^{(i-1)} x_2 + \alpha^{2(i-1)} + ... + \alpha^{(i-1)(n-1)} x_n & = b_i \\ \vdots & \vdots \quad \vdots \\ x_1 + \alpha^{(n-1)} x_2 + \alpha^{2(n-1)} x_3 + ... + \alpha^{(n-1)^2} x_n & = b_n \end{cases}$$

ammette un'unica soluzione $(x_1, ..., x_n)$ dove

$$x_k = \frac{1}{n} \sum_{i=1}^{n} \alpha^{-(i-1)(k-1)} b_i.$$

Dimostrazione. Addizionando tutte le equazioni abbiamo $nx_1 = b_1 + ... + b_n$. Infatti il coefficiente di x_{t+1} è $\sum_{i=1}^{n} \alpha^{it}$ $(1 \le t \le n-1)$. Siccome $\{\alpha^{it}\}_{1 \le i \le n} = \{\alpha^j\}_{1 \le j \le n}$, questo coefficiente vale $\sum_{j=1}^{n} \alpha^j$. Ma $\frac{X^n - 1}{X - 1} = X^{n-1} + ... + X + 1$, quindi $\sum_{j=1}^{n} \alpha^j = 0$. Quindi $x_1 = \frac{1}{n} \sum_{i=1}^{n} b_i$.

In modo analogo per avere x_k basta moltiplicare ogni equazione per la potenza opportuna di α di modo che il coefficiente di x_k sia uno e poi addizionare. Il coefficiente di x_k in $\sum_{j=1}^{n} \alpha^{(i-1)(j-1)} x_j = b_i$ è $\alpha^{(i-1)(k-1)}$, dobbiamo

quindi moltiplicare per $\alpha^{-(i-1)(k-1)}$. Sommando tutte le equazioni troviamo l'asserto. □

Osservazione 1.8. Il determinante di Vandermonde $\begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & \vdots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{vmatrix}$ vale $\prod_{1\le i<j\le n}(x_j - x_i)$. Il determinante del sistema del Lemma 1.7 è il determinante di Vandermonde per $x_1 = 1, x_2 = \alpha$, ..., $x_n = \alpha^{n-1}$, quindi è la radice del discriminante di $X^n - 1$; siccome $X^n - 1$ non ha radici multiple (la derivata è nX^{n-1}), il determinante è non nullo e il sistema è di Cramer.

Tuttavia avremo ancora bisogno del Lemma 1.7 e dell'espressione esplicita della soluzione.

Tornando al discorso precedente, ci siamo ricondotti a risolvere un'equazione di grado $(n-1)!$. Questo permette di risolvere l'equazione del terzo grado. Se $n = 4$, abbiamo un'equazione di grado 6 in X^4: miracolosamente, come abbiamo già visto questa equazione può essere risolta.
Se n è primo Lagrange mostra che è possibile ricondursi ad un'equazione di grado $(n-2)!$, se $n = 5$ viene un'equazione di grado 6 e questa volta non c'è nessun miracolo, l'equazione risolvente del sesto grado è intrattabile e Lagrange comincia a dubitare fortemente che si possa risolvere per radicali l'equazione di grado cinque...

Riassumendo la strategia di Lagrange è la seguente:
(1) si prende una risolvente t cioè una quantità che sia razionalmente esprimibile in funzione delle radici r_i e dei numeri noti (i coefficienti dell'equazione, i numeri razionali, le radici dell'unità).
(2) Viceversa ogni radice è una funzione razionale di t e dei numeri noti.
(3) t è radice di un'equazione ($F(X) = 0$, *equazione risolvente*) <u>risolubile</u>.

In linguaggio moderno le condizioni (1) e (2) significano che: $k(r_1, ..., r_n) = k(t)$.

Prendendo $t = r_1 + \alpha r_2 + ... + \alpha^{n-1} r_n$ (α radice primitiva n-esima dell'unità) si ottiene un metodo per risolvere l'equazione di grado ≤ 4. Il metodo non sembra applicabile se $n = 5$. Forse questo è dovuto alla scelta di t? Nel suo trattato *Mémoire sur la résolution algébrique des équations* (1770) Lagrange cerca di caratterizzare le possibili risolventi e dimostra quello che si chiama oggi il *teorema dell'elemento primitivo.*

Il lavoro di Lagrange, anche se non ha portato nessun risultato nuovo, è fondamentale perchè ha spianato la strada a Galois.

Terminiamo qui la nostra introduzione storica (anche perchè *here enters the hero*) e iniziamo la presentazione moderna della teoria di Galois. In questa presentazione l'algebra lineare (in dimensione finita) ha un ruolo deter-

minante, i polinomi sono (quasi) completamente scomparsi. Questa formalizzazione è senz'altro un progresso, ma lascia in sospeso la domanda naturale: ma come ha fatto Galois, senza sapere cosa fosse uno spazio vettoriale, un campo, un gruppo (li ha introdotti lui!), a fare la teoria di Galois? Torneremo più avanti su questa questione.

2

La corrispondenza di Galois.

2.1 Richiami: estensioni finite di campi.

In questo paragrafo ricordiamo velocemente (e spesso senza dimostrazioni) alcune nozioni di base.

2.1.1 Divisibilità in un anello integro.

Nel seguito indicheremo con A un anello *integro, commutativo*, si dice anche che A è un *dominio*. Se a, b sono due elementi non nulli di A si dice che a divide b (in simboli $a \mid b$) se esiste $c \in A$ tale che $ac = b$. Questo è equivalente a richiedere $(b) \subset (a)$, dove $(x) = \{tx \mid t \in A\}$ è l'ideale principale generato da x.

Definizione 2.1. *In un dominio A:*

1. *un elemento $e \in A$ è un'*unità *se e è invertibile ($\exists e'$ t.c. $ee' = 1$)*
2. *a e b sono* associati *se $a = be$ dove e è un'unità.*
3. *$q \in A$ è* irriducibile *se q non è un'unità e se $q = ab \Rightarrow a$ o b è un'unità.*
4. *$p \in A$ è* primo *se p non è un'unità e se $p \mid ab \Rightarrow p \mid a$ o $p \mid b$.*

Esempio 2.2. Le unità di $\mathbb{Z}$ sono ± 1; le unità di $k[X]$ (k un campo) sono gli elementi di k^*. In $\mathbb{Z}$ 2 e -2 sono associati. In $\mathbb{Z}$ e $k[X]$ un elemento è primo se e solo se è irriducibile, ma non è sempre così in un dominio qualsiasi (cf Esercizi 1, 2).

Definizione 2.3. *Un dominio A è:*

1. principale *(PID* principal ideal domain*) se ogni ideale $I \subset A$ è della forma $I = (a)$ (i.e. generato da un unico elemento).*
2. fattoriale *(UFD* unique factorization domain*) se ogni elemento ammette un'unica (modulo ordine dei fattori ed associati) fattorizzazione in elementi irriducibili.*

In $\mathbb{N}$ abbiamo la *divisione euclidea* (divisione con resto): dati $n \neq 0, m \in \mathbb{N}$ esistono $q, r \in \mathbb{N}$ tali che: $m = qn + r$ con $0 \leq r < n$; q, r sono univocamente determinati. Questa divisione si estende poi a $\mathbb{Z}$: dati $a, b \neq 0 \in \mathbb{Z}$, esistono q, r tali che $a = bq + r$ con $0 \leq r < |b|$.

In modo analogo abbiamo la divisione euclidea in $k[X]$:

dati $P(X), M(X) \neq 0$ esistono $Q(X), R(X)$ tali che: $P(X) = M(X)Q(X) + R(X)$, con $R(X) = 0$ o $\deg(R) < \deg(M)$.

Più generalmente:

Definizione 2.4. *Un dominio A è* euclideo *se esiste: $f : A^* \to \mathbb{Z}^+$ tale che:*

1. *$f(ab) = f(a)f(b)$*
2. *Per ogni $a, b \neq 0$ in A: $a = bq + r$ con $r = 0$ o $f(r) < f(b)$.*

Questa nozione è particolarmente importante perché:

Teorema 2.5. *Sia A un dominio.*

1. *Se A è euclideo, allora A è principale*
2. *Se A è principale, allora A è fattoriale.*

Quindi $\mathbb{Z}$ e $k[X]$ sono euclidei, principali e fattoriali.

Abbiamo inoltre:

Proposizione 2.6. *Se A è principale (PID) e $p \in A$, le seguenti affermazioni sono equivalenti:*

1. *p è primo*
2. *p è irriducibile*
3. *(p) è massimale.*

Quindi per $\mathbb{Z}$ e $k[X]$ i due anelli di maggior interesse per noi adesso, abbiamo:

$\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ è un campo $\Leftrightarrow$ n è primo.

$k[X]/(P(X))$ è un campo $\Leftrightarrow$ $P(X)$ è irriducibile.

Definizione 2.7. *Sia a, b due elementi del dominio A; $c \in A$ è un comune divisore di a e b se $c \mid a$ e $c \mid b$. Un massimo comune divisore (MCD) di a e b è un comune divisore, d, tale che ogni comune divisore c di a, b verifica $c \mid d$.*

Se d e d' sono due MCD di a, b, allora d e d' sono associati, cioè il MCD, se esiste, è univocamente determinato modulo unità e lo si nota $(a, b) = d$.

Lemma 2.8. *In un PID il MCD esiste sempre, più precisamente se $a, b \in A$ allora $(a) + (b) = (d)$ e $(a, b) = d$. In particolare esistono $u, v \in A$ tali che $au + bv = d$.*

Se $(a, b) = 1$ si dice che a e b sono primi tra di loro*, questo equivale a dire che non esiste nessun primo (=irriducibile) che divide sia a che b.*

Osservazione 2.9. La relazione $au + bv = d$ dove $d = (a, b)$ viene spesso chiamata *Lemma di Bezout.*

In un dominio euclideo l'algoritmo di Euclide permette di determinare u, v.

2.1.2 Estensioni, elementi algebrici.

Se L è un campo e se $K \subset L$ è un sotto campo si dice che L è un'estensione di K (in simboli: L/K).

Definizione 2.10. *Sia L/K un'estensione di K. Un elemento $\alpha \in L$ è algebrico su K se α è radice di un polinomio a coefficienti in K.*

L'estensione L/K è algebrica se ogni $\alpha \in L$ è algebrico su K.

Sia L/K un'estensione e $\alpha \in L$. Abbiamo un morfismo di anelli $\varphi : K[X] \to K[\alpha] \subset L : P(X) \to P(\alpha)$. Per definizione α è algebrico su K se e solo se φ non è iniettivo. In questo caso $Ker(\varphi)$ è un ideale $I \subset K[X]$. Siccome $K[X]$ è un PID (Teorema 2.5), $I = (M)$. Il polinomio M è univocamente determinato modulo un elemento non nullo di K (un'unità di $K[X]$). In particolare esiste uno ed un unico polinomio monico, $M_\alpha(X)$ tale che $I = (M_\alpha)$. Il polinomio M_α è irriducibile su K. Infatti sia $M_\alpha(X) = P(X)Q(X)$ con $P(X), Q(X) \in K[X]$, allora $M_\alpha(\alpha) = 0 = P(\alpha)Q(\alpha)$ implica $P(\alpha) = 0$ o $Q(\alpha) = 0$. Se $P(\alpha) = 0$, allora $P \in I = (M_\alpha)$, cioè $M_\alpha \mid P$ e questo implica che P è una costante (cioè un'unità di $K[X]$) e quindi $M_\alpha(X)$ è irriducibile su K.

Definizione 2.11. *Con le notazioni precedenti il polinomio $M_\alpha(X) \in K[X]$ è il* polinomio minimo *dell'elemento algebrico $\alpha \in L$.*

Il polinomio minimo sarà per noi uno strumento fondamentale. Intanto abbiamo:

Lemma 2.12. *Sia L/K un'estensione di campi e sia $\alpha \in L$. Sono equivalenti:*

1. *α è algebrico su K*
2. *$K[\alpha] = K(\alpha)$*
3. *$\dim_K(K[\alpha]) < \infty$ (infatti $\dim_K(K[\alpha]) = \deg(M_\alpha)$).*

Dimostrazione. (1) $\Rightarrow$ (2): Siccome φ è ovviamente suriettiva su $K[\alpha]$, abbiamo $K[X]/(M_\alpha) \simeq K[\alpha]$. Siccome M_α è irriducibile, $K[X]/(M_\alpha) = K[\alpha]$ è un campo (Lemma 2.6). Quindi $K[\alpha]$ è un campo che contiene K e α, quindi $K(\alpha) \subset K[\alpha]$, l'altra inclusione è ovvia quindi $K(\alpha) = K[\alpha]$.

(2) $\Rightarrow$ (1): $\alpha^{-1} \in K(\alpha) = K[\alpha]$, quindi $\alpha^{-1} = a_n\alpha^n + ... + a_1\alpha + a_0$, moltiplicando per α si vede che il polinomio $P(X) = a_nX^{n+1} + ... + a_0X - 1 \in K[X]$ verifica $P(\alpha) = 0$.

(1) $\Rightarrow$ (3): Abbiamo $M_\alpha(\alpha) = 0 = \alpha^n + ... + a_1\alpha + a_0$ $(a_i \in K, \forall i)$. Allora $B = (1, \alpha, ..., \alpha^{n-1})$ è una base del K-spazio vettoriale $K[\alpha]$. Infatti i vettori di B sono linearmente indipendenti: se $\sum_{i=0}^{n-1} \lambda_i\alpha^i = 0$, allora $P(X) = \sum_{i=0}^{n-1} \lambda_iX^i \in K[X]$ verifica $P(\alpha) = 0$, ma questo è impossibile perché $\deg(P) < n = \deg(M_\alpha)$. Siccome $\alpha^n = -a_0 - ... - a_{n-1}\alpha^{n-1}$, per induzione si ha $< 1, \alpha, ..., \alpha^{n-1} >= K[\alpha]$. In particolare $\dim_K(K[\alpha]) = \deg(M_\alpha)$.

(3) $\Rightarrow$ (1): Se $n = \dim_K(K[\alpha])$ allora $1, \alpha, ..., \alpha^n$ sono linearmente dipendenti e esistono $\lambda_i \in K$ non tutti nulli tali che: $\sum_{i=0}^{n} \lambda_i\alpha^i = 0$ e $P(X) = \sum_{i=0}^{n} \lambda_iX^i \in K[X]$ verifica $P(\alpha) = 0$. $\square$

Definizione 2.13. *L'estensione L/K è* finita *se* $[L : K] := \dim_K(L) < \infty$.

Abbiamo:

Lemma 2.14. *Ogni estensione finita è algebrica.*

Sia $K \subset L \subset F$ una torre di estensioni, se due delle tre quantità $[L : K], [F : L], [F : K]$ sono finite allora anche la terza lo è e:

$$[F : K] = [F : L].[L : K]$$

Finalmente:

Proposizione 2.15. *Sia L/K un'estensione e sia*
$F := \{\alpha \in L \mid \alpha$ è algebrico su $K\}$. Allora:

1. *F è un sottocampo di L e si ha $K \subset F \subset L$*
2. *Se $\alpha \in L$ è algebrico su F, allora $\alpha \in F$*
3. *Se L è algebricamente chiuso anche F lo è.*

Dimostrazione. (1) Chiaramente $K \subset F$ perché se $\alpha \in K$, $X - \alpha \in K[X]$. Sia $\alpha \in L$, $\alpha \neq 0$ con

$$a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0,\ a_i \in K, \forall i$$

Dividendo per α^n (cioè moltiplicando per $(\alpha^{-1})^n$):

$$a_n + \cdots + a_1(\frac{1}{\alpha})^{n-1} + a_0(\frac{1}{\alpha})^n = 0$$

e quindi anche $\alpha^{-1} \in F$. Rimane da vedere che se $\alpha, \beta \in F$ allora anche $\alpha + \beta$ e $\alpha\beta$ sono in F. Siccome β è algebrico su $K(\alpha)$ (perché radice di un polinomio a coefficienti in K) $[K(\alpha, \beta) : K(\alpha)] < \infty$ (Lemma 2.12), osservare che $K(\alpha, \beta) = K(\alpha)(\beta)$). Nello stesso modo, siccome α è algebrico su K: $[K(\alpha) : K] < \infty$. Segue dal Lemma 2.14 che: $[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\alpha)][K(\alpha) : K] < \infty$. Pertanto $K(\alpha, \beta)/K$ è algebrica ((1) del Lemma 2.14). Quindi $\alpha + \beta$, $\alpha\beta \in K(\alpha, \beta)$ sono algebrici su K.

(2) Sia α radice di $P(X) = a_nX^n + ... + a_1X + a_0$ con $a_i \in F$. L'estensione $K(a_n, ..., a_0)/K$ è algebrica finita. Infatti ogni a_i è algebrico su K (perché $a_i \in F$), inoltre $K(a_1, a_0) = K(a_0)(a_1)$, quindi $K(a_0, a_1)/K$ è algebrica finita e procedendo per induzione si ottiene il risultato.

Adesso $P(X) \in K'[X]$ ($K' := K(a_n, ..., a_0)$). Quindi α è algebrico su K', cioè $[K'(\alpha) : K'] < \infty$ (Lemma 2.12). Segue che $[K'(\alpha) : K] = [K'(\alpha) : K'][K' : K] < \infty$, quindi α è algebrico su K, cioè $\alpha \in F$.

(3) Sia $P(X) \in F[X]$ con $\deg(P) \geq 1$. Se L è algebricamente chiuso, esiste $\alpha \in L$ tale che $P(\alpha) = 0$. Quindi α è algebrico su F. Per il passo (2), $\alpha \in F$. Quindi ogni polinomio non costante a coefficienti in F ha una radice in F: F è algebricamente chiuso. □

Esempio 2.16 (Esempio base).
Consideriamo l'estensione $\mathbb{Q} \subset \mathbb{C}$. Un numero complesso algebrico su $\mathbb{Q}$ si chiama (più semplicemente) un *numero algebrico* (chi l'avrebbe mai detto ;-). Per esempio i è un numero algebrico. Per la Prop. 2.15 l'insieme dei numeri algebrici è un campo e siccome $\mathbb{C}$ è algebricamente chiuso, questo campo è algebricamente chiuso (e contiene $\mathbb{Q}$): questo campo è $\overline{\mathbb{Q}}$, la chiusura algebrica di $\mathbb{Q}$. Se $z \in \mathbb{C} \setminus \overline{\mathbb{Q}}$ allora z è un *numero trascendente*. Siccome π, e sono trascendenti, $\overline{\mathbb{Q}} \neq \mathbb{C}$ (d'altra parte $\overline{\mathbb{Q}}$ è numerabile mentre $\mathbb{C}$ non lo è).

L'estensione $\overline{\mathbb{Q}}/\mathbb{Q}$ è algebrica (per definizione), <u>infinita</u> (cf Esercizio 7), quindi non tutte le estensioni algebriche sono finite!

Le estensioni $\mathbb{C}/\mathbb{Q}$, $\mathbb{R}/\mathbb{Q}$ non sono algebriche (esistono numeri trascendenti), l'estensione $\mathbb{C}/\mathbb{R}$ è algebrica finita ($\mathbb{C} = \mathbb{R}(i)$, $[\mathbb{C} : \mathbb{R}] = 2$).

Definizione 2.17. *Un* campo di numeri (number field) *è un'estensione finita di* $\mathbb{Q}$.

Se K è un campo di numeri: $\mathbb{Q} \subset K \subset \overline{\mathbb{Q}}$.

Anche se la teoria di Galois può essere sviluppata in tutta generalità su campi qualsiasi, i campi di numeri saranno il nostro ambito di lavoro preferito, questo per motivi storici e naturali e anche perché i legami con la teoria dei numeri sono molteplici e profondi (l'oggetto misterioso $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ (*il gruppo di Galois assoluto*) è uno dei Graal della ricerca contemporanea).

—— .. ——

Esercizi.

Esercizio 1 *Mostrare che in un dominio ogni elemento primo è irriducibile.*

Esercizio 2 *Sia* $\omega = i\sqrt{5}$ *e sia* $A = \{a + \omega b \mid a, b \in \mathbb{Z}\}$.

1. *Mostrare che* A *è un sotto anello di* $\mathbb{C}$.
2. *Se* $\alpha = a+\omega b \in A$ *si definisce* $N(\alpha) = a^2+5b^2 = (a+\omega b)(a-\omega b)$ *(si dice che* N *è la* norma *di* A*). Mostrare che* $\forall \alpha, \beta \in A$*:* $N(\alpha\beta) = N(\alpha)N(\beta)$.
3. *Mostrare che* 2 *è irriducibile in* A *(scrivere* $2 = (x+\omega y)(a+\omega b)$ *e prendere la norma).*
4. *Nello stesso modo vedere che* 3, $1-\omega$, $1+\omega$ *sono irriducibili.*
5. *Osservare che* $6 = 2 \cdot 3 = (1-\omega) \cdot (1+\omega)$. *Concludere che* A *non è fattoriale.*
6. *Mostrare che* $2 \mid (1+\omega)^2$, *ma* $2 \nmid 1+\omega$. *Concludere che* 2 *è irriducibile ma non è primo.*
7. *Se* $I = (a, b)$ *è un ideale allora l'ideale* I^2 *è generato da* a^2, ab, b^2. *Sia* $J = (2, 1+\omega) \subset A$ *l'ideale generato da* 2 *e* $1+\omega$. *Mostrare che* $J^2 \subset (2)$ *(*(2) *è l'ideale principale generato da* 2*). Vedere poi che* $2 \in J^2$. *Concludere che* $(2) = J^2$ *(si può mostrare che l'ideale* J *è primo:* 2 *è* ramificato *in* $\mathbb{Q}(\omega)$*).*

Esercizio 3 *Dimostrare la Proposizione 2.6.*

Esercizio 4 *Mostrare che ogni estensione finita* L/K *è algebrica.*

Esercizio 5 (Lemma di Gauss)
Scopo dell'esercizio è di dimostrare il seguente risultato dovuto a Gauss :

Sia $f(X) \in \mathbb{Q}[X]$ *un polinomio monico. Se* $f \mid P$ *dove* $P(X) \in \mathbb{Z}[X]$ *è monico, allora* $f(X) \in \mathbb{Z}[X]$.

Sia dunque $f(X) = X^n + a_{n-1}X^{n-1} + ... + a_0$, $a_i \in \mathbb{Q}$ $a_i = r_i/s_i$, $(r_i, s_i) = 1$ *e* $f(X) \cdot g(X) = P(X)$. *Chiaramente* $g(X) \in \mathbb{Q}[X]$ *è monico anche lui:* $g(X) = X^m + b_{m-1}X^{m-1} + ... + b_0$.

1. *Sia* d *il minimo comune multiplo dei denominatori,* s_i *degli* a_i. *Allora*
$$f(X) = \frac{1}{d}(dX^n + a'_{n-1}X^{n-1} + ... + a'_0)$$
dove $a'_i \in \mathbb{Z}$ *e dove* $d, a'_{n-1}, ..., a'_0$ *sono primi tra di loro.*
2. *In modo analogo:*
$$g(X) = \frac{1}{e}(eX^m + b'_{m-1}X^{m-1} + ... + b'_0)$$
con $(e, b'_{m-1}, ..., b'_0) = 1$
3. *Se* $f(X) \notin \mathbb{Z}[X]$, *esiste* p *un numero primo che divide* d. *Esiste* k *tale che* $p \mid a'_i$ *se* $i > k$, $p \nmid a'_k$ *(perché?)*

4. *Se $p \nmid e$ si pone $l = m, b'_m = e$; se $p \mid e$, come prima l è definito da: $p \mid b'_i$ se $i > l$, $p \nmid b'_l$.*
5. *Osservare che i coefficienti di*

$$(dX^n + a'_{n-1}X^{n-1} + ... + a'_0)(eX^m + b'_{m-1}X^{m-1} + ... + b'_0) \ (*)$$

sono multipli di de, quindi divisibili per p (hint: $P(X) \in \mathbb{Z}[X]$).
6. *Concludere considerando il coefficiente*

$$\sum_{i+j=k+l} a'_i b'_j$$

di X^{k+l} in $(*)$.

Esercizio 6 (Criterio di Eisenstein)
Il criterio di irriducibilità di Eisenstein è il seguente:

Sia $f(X) = X^n + ... + a_0 \in \mathbb{Z}[X]$ un polinomio di grado ≥ 1. Se esiste un numero primo p tale che: $p \mid a_i$ se $i < n$ e $p^2 \nmid a_0$, allora $f(X)$ è irriducibile in $\mathbb{Q}[X]$.

1. *Supponiamo $f(X) = g(X)h(X)$ con $g(X), h(X) \in \mathbb{Q}[X]$ polinomi non costanti. Siccome $f(X)$ è monico, possiamo assumere $g(X), h(X)$ monici. Quindi (Esercizio 5) $g(X), h(X) \in \mathbb{Z}[X]$.*
2. *Sia $g(X) = X^d + ... + b_0$, $h(X) = X^m + ... + c_0$. Siccome $a_0 = b_0c_0$, p divide uno e uno solo tra b_0, c_0: $p \nmid b_0$, $p \mid c_0$.*
3. *Se $p \mid c_i, \forall i$ si pone $r = m$, altrimenti sia $r = max\{i \mid p \nmid c_i\}$. Concludere considerando a_r.*

Esercizio 7 *Mostrare che l'estensione algebrica $\overline{\mathbb{Q}}/\mathbb{Q}$ non è finita (utilizzare l'Esercizio 6).*

Esercizio 8 *Sia $P(x) = x^4 + ax^2 + b^2$, con $a, b \in \mathbb{Z}$. Si pone:*

$$u = 2b - a\,,\ v = -2b - a\,,\ w = a^2 - 4b^2$$

1. *Verificare le uguaglianze: $P(x) = (x^2 + b)^2 - ux^2$, $P(x) = (x^2 - b)^2 - vx^2$, $P(x) = (x^2 + \frac{a}{2})^2 - \frac{w}{4}$. Concludere che se uno dei tre numeri u, v, w è un quadrato, allora $P(x)$ è riducibile su $\mathbb{Q}$.*
2. *Supponiamo $P(x) = f(x)g(x)$ in $\mathbb{Q}[x]$, con $\deg(f), \deg(g) \geq 1$. Siccome $P(x) = P(-x)$ possiamo assumere $\deg(f) = \deg(g) = 2$, f, g monici. Siccome $P(x)$ ha quattro radici in $\mathbb{C}$, ci sono tre fattorizzazioni come sopra (perché?). Siccome $P(x) = (x^2 - \sqrt{u}x + b)(x^2 + \sqrt{u}x + b)$, $P(x) = (x^2 - \sqrt{v}x - b)(x^2 + \sqrt{v}x - b)$ e $P(x) = (x^2 - \frac{a}{2} - \frac{\sqrt{w}}{2})(x^2 + \frac{a}{2} + \frac{\sqrt{w}}{2})$, concludere che se $P(x)$ è riducibile su $\mathbb{Q}$, allora uno dei tre numeri u, v, w è un quadrato.*
3. *Sia p un numero primo e sia $\overline{P}(x) = x^4 + \overline{a}x^2 + \overline{b}^2 \in \mathbb{F}_p$ ($\overline{n}$ indica la classe di n modulo p). Si ricorda che in $\mathbb{F}_p$ esiste sempre una radice primitiva, ξ, cioè $\mathbb{F}_p = \{1 = \xi^0, \xi, ..., \xi^{p-1}\}$). Mostrare che uno dei tre elementi $\overline{u}, \overline{v}, \overline{w}$ è un quadrato in $\mathbb{F}_p$. Concludere che $\overline{P}(x)$ è riducibile, per ogni p.*

Abbiamo quindi esempi di polinomi che sono riducibili modulo p per ogni p e che sono riducibili o irriducibili su $\mathbb{Q}$.

Esercizio 9 *Sia $P(x) \in \mathbb{Z}[x]$ un polinomio monico. Sia p un numero primo. Mostrare che se P è irriducibile modulo p, allora P è irriducibile su $\mathbb{Q}$ (confrontare con l'Esercizio 8). Mostrare che $x^3 - x - 1$ è irriducibile su $\mathbb{Q}$.*

2.2 Estensioni separabili, teorema dell'elemento primitivo.

In questa prima parte siamo interessati a studiare le soluzioni di equazioni $P(X) = 0$ dove $P(X) \in \mathbb{Q}[X]$; in altri termini siamo interessati alle estensioni finite di $\mathbb{Q}$. Avremo quindi da considerare estensioni finite di campi L/K dove K è un'estensione finita di $\mathbb{Q}$.

Sarà fondamentale assumere che tutti i campi considerati sono sotto campi di un *grande* campo Ω (l'universo); cioè che ogni polinomio $P(X) \in K[X]$ ha tutte le sue radici in Ω. Come Ω possiamo prendere un qualsiasi campo algebricamente chiuso contenente il campo *base* $\mathbb{Q}$; tradizionalmente si prende $\Omega = \mathbb{C}$, anche se sarebbe più naturale prendere $\Omega = \overline{\mathbb{Q}}$, la chiusura algebrica di $\mathbb{Q}$. Per noi sarà $\Omega = \overline{\mathbb{Q}}$.

Per riassumere:

Tutti i campi considerati nel seguito sono estensioni algebriche finite di $\mathbb{Q}$ e sono tutti sotto campi del campo algebricamente chiuso Ω ($\Omega = \overline{\mathbb{Q}}$). In particolare tutti i polinomi considerati hanno *tutte* le loro radici in Ω.

2.2.1 Separabilità.

Il lettore si convincerà facilmente che non c'è alcun problema nel rimpiazzare $\mathbb{Q}$ con un qualsiasi campo di caratteristica zero. Le cose invece non vanno così bene se si rimpiazza $\mathbb{Q}$ con un campo di caratteristica $p > 0$. Questo è dovuto al fatto che nel studiare le soluzioni di $P(X) = 0$, è opportuno distinguere i casi secondo cui $P(X)$ abbia o meno radici multiple.

Se $ch(K) = 0$ e se $P(X) \in K[X]$, allora $P(X)$ ha una radice multipla se e solo se $P(X)$ e $P'(X)$ hanno una radice comune. In particolare se $P(X)$ è irriducibile su K, $P(X)$ non ha radici multiple in K (Esercizio 10).

In caratteristica $p > 0$, questo ragionamento non regge più perché la derivata può essere identicamente nulla senza che il polinomio sia una costante, per esempio se $P(X) = X^p - a$ e $ch(K) = p$, allora $P'(X) = 0$. Questo fenomeno porta delle complicazioni (cf Esercizio 11).

Per tenere conto di questo fenomeno si introduce la nozione di *separabilità* (separare le radici).

Definizione 2.18. *Sia L/K e $a \in L$. L'elemento $a \in L$ è separabile su K se esiste un polinomio $P(X) \in K[X]$, senza radici multiple, tale che $P(a) = 0$. L'estensione L/K è separabile se ogni $a \in L$ è separabile su K.*

Non avremo molto da preoccuparci della separabilità nel caso delle estensioni di $\mathbb{Q}$ (ma dovremo ricordarcene quando avremo a che fare con campi di caratteristica $p > 0$, per esempio campi finiti):

Lemma 2.19. *Se $ch(K) = 0$ ogni estensione finita L/K è separabile.*

Dimostrazione. Sia $a \in L$. Il polinomio minimo $M_a(X) \in K[X]$ è irriducibile e quindi non ha nessuna radice in comune con la sua derivata, pertanto $M_a(X)$ non ha radici multiple (in $\overline{K}$). $\square$

2.2.2 Teorema dell'elemento primitivo.

Se K/L è un'estensione algebrica finita allora possiamo scrivere L nella forma: $L = K(\alpha_1, ..., \alpha_n)$ dove $\alpha_1, ..., \alpha_n \in L$ sono algebrici su K. Infatti se $[L : K] = n$ e se $(\alpha_1, ..., \alpha_n)$ è una base del K-spazio vettoriale L, ogni elemento $\alpha \in L$ si scrive: $\alpha = \sum a_i \alpha_i, a_i \in K$. Viceversa ogni polinomio $\sum a_{i_1 i_2 ... i_n} \alpha_1^{i_1} \alpha_2^{i_2} ... \alpha_n^{i_n}$, $a_{i_1 i_2 ... i_n} \in K$ si esprime nel modo precedente perché ogni monomio $\alpha_1^{i_1} \alpha_2^{i_2} ... \alpha_n^{i_n}$ è combinazione lineare degli α_i. Quindi $L = K[\alpha_1, ..., \alpha_n]$ e pertanto $L = K(\alpha_1, ..., \alpha_n)$ (perché, appunto, gli α_i sono algebrici su K, cf Lemma 2.12). Si dice che L è stato ottenuto *aggiungendo* (l'espressione è di Galois) a K gli elementi $\alpha_1, ..., \alpha_n$ (cioè si è esteso K con l'aggiunta degli α_i).

Il teorema dell'elemento primitivo permette di semplificare drasticamente la situazione.

Teorema 2.20. (Teorema dell'elemento primitivo)
Sia L/K un'estensione finita con $ch(K) = 0$. Allora esiste $\alpha \in L$ tale che $L = K(\alpha)$.

In queste condizioni $[L : K] = \deg(M_\alpha(X))$ dove $M_\alpha(X)$ è il polinomio minimo di α su K.

Dimostrazione. Induzione su $n = \dim_K(L)$. Se $n = 1$ non c'è nulla da dimostrare. Supponiamo l'asserto vero per le estensioni di K di dimensione $< n$. Sia L/K con $[L : K] = n$. Prendendo una base di L su K possiamo scrivere $L = K(\alpha_1, ..., \alpha_n) = K'(\alpha_n)$ con $K' = K(\alpha_1, ..., \alpha_{n-1})$. Siccome $[K' : K] < n$, per ipotesi di induzione $K' = K(a)$, $a \in K'$. In conclusione ci siamo ricondotti a dimostrare il teorema per $L = K(a, b)$.

Siano $M_a(X), M_b(X)$ i polinomi minimi di a, b su K. Questi polinomi fattorizzano completamente in Ω: $M_a(X) = \prod(X - a_i)$ $(a_1 = a)$, $M_b(X) = \prod(X - b_j)$ $(b_1 = b)$. Inoltre $a_i \neq a_l$ se $i \neq l$ perché $ch(K) = 0$ (idem per i b_j). Sia $R = \{\frac{(a_i - a)}{(b - b_j)} \mid i, j > 1\}$. Prendiamo $t \in K \setminus (K \cap R)$ (K è infinito perché $ch(K) = 0$) e poniamo $z = a + tb$. Per concludere basta mostrare che $K(a, b) = K(z)$.

Sia $H(X) = M_b(\frac{z - X}{t}) \in K[z](X)$. Abbiamo $H(a) = 0$. Sia $D(X) \in K[z](X)$ il M.C.D. di $H(X)$ e $M_a(X)$. Abbiamo $\deg(D(X)) \geq 1$ perché $D(a) = M_a(a) = 0$. Le altre radici di H sono $r_j = a + t(b - b_j)$. Per la scelta di t, $r_j \neq a_i$ se $i, j > 1$. Concludiamo che $D(X) = X - a \in K[z](X)$. Quindi $-D(0) = a \in K[z]$. Siccome $b = (z - a)/t$ anche $b \in K[z]$. Pertanto $K(a, b) = K(z)$.

L'ultima affermazione segue da 2.12. $\square$

Osservazione 2.21. La dimostrazione precedente mostra che basta scegliere t in K al di fuori dell'insieme finito $K \cap R$. Visto che (sotto le nostre ipotesi) K è infinito, abbiamo solo l'imbarazzo della scelta. Se K fosse un campo finito, ci sarebbe un problema. Il teorema dell'elemento primitivo è ancora vero se $ch(K) > 0$, sotto opportune ipotesi di separabilità.

Un elemento $z \in L$ tale che $L = K(z)$ si chiama *elemento primitivo* (su K). Da quanto precede un elemento generico di L ha una forte tendenza ad essere un elemento primitivo. Cercheremo di precisare questo discorso più avanti.

Osserviamo che se $K \subset F \subset L$ e se $L = K(z)$, allora $L = F(z)$ (perché $K(z) \subset F(z) \subset L$).

Esercizi.

Esercizio 10

1. *Sia L un campo e siano $P(x), Q(x) \in L[x]$. Si assume $P(x)$ irriducibile. Mostrare che se P e Q hanno una radice in comune (in qualche estensione di L), allora $P \mid Q$ in $L[x]$.*
2. *Sia k un campo di caratteristica zero e sia $P(X) \in k[X]$ un polinomio irriducibile. Mostrare che $P(X)$ non ha radici multiple (in qualsiasi estensione di k).*

Esercizio 11

1. *Sia $f(x) \in k[x]$ e sia L/k un campo di spezzamento di f. Mostrare che le seguenti affermazioni sono equivalenti:*
   a) *f ha una radice multipla in L*
   b) *esiste $\alpha \in L$ tale che $f(\alpha) = f'(\alpha) = 0$*
   c) *esiste $M(x) \in k[x]$ tale $M \mid f$ e $M \mid f'$*
2. *Si dice che $f(x)$ è separabile su k se ogni fattore irriducibile di f non ha radici multiple in L. Se f è irriducibile mostrare che f è inseparabile (non separabile) se e solo se $ch(k) = p > 0$ e $f(x) = g(x^p)$.*
3. *Sia K con $ch(K) = p$. Mostrare che se $x, y \in K$, allora $(x+y)^p = x^p + y^p$ (usare la formula del binomio). Concludere che $\Phi : K \to K : x \to x^p$ è un morfismo di campi (Φ è il morfismo di Frobenius).*
4. *Sia $K_0 \simeq \mathbb{F}_p$ il campo primo di K (quello dato dalla caratteristica, cioè l'intersezione di tutti i sotto campi di K). Sia $K^\Phi = \{z \in K \mid \Phi(z) = z\}$. Mostrare che $K^\Phi = K_0$.*
5. *Sia $K = \mathbb{F}_p$ e sia $f(x) \in K[x]$. Mostrare che se $f(x) = g(x^p)$, allora f non è irriducibile (usare il punto precedente o il piccolo teorema di Fermat per mostrare che $f = h^p$). Concludere che ogni $p(x) \in K[x]$ è separabile.*
   Nota: *Si può mostrare che se K ($ch(K) > 0$) è algebrico su il suo campo primo allora ogni $p(x) \in K[x]$ è separabile. Ma esistono polinomi inseparabili in caratteristica p.*

Esercizio 12 *Sia K un* campo quadratico *(cioè K è un'estensione di $\mathbb{Q}$ con $[K : \mathbb{Q}] = 2$).*

1. *Mostrare che ogni elemento di $K \setminus \mathbb{Q}$ è primitivo.*
2. *Più generalmente se $[K : \mathbb{Q}] = p$ dove p è un numero primo, mostrare che ogni elemento di $K \setminus \mathbb{Q}$ è primitivo.*

Esercizio 13 *Dare un'esempio di un'estensione $K/\mathbb{Q}$ di grado 4 (i.e. $[K : \mathbb{Q}] = 4$) con un elemento $\alpha \in K$ non primitivo.*

Esercizio 14 *Sia $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ e sia $\xi = \sqrt{2} + \sqrt{5}$.*

1. *Mostrare che $K = \mathbb{Q}(\xi)$*

2. *Determinare* $[K : \mathbb{Q}]$
3. *Determinare* $M_\xi(X)$*, il polinomio minimo di* ξ *su* $\mathbb{Q}$ *(osservare che* $\xi^2 = 7 + 2\sqrt{2}\sqrt{5}$*).*

Esercizio 15 *Sia* $K(\alpha)/K$ *un'estensione algebrica.*

1. *Mostrare che l'applicazione:* $m_\alpha : K(\alpha) \to K(\alpha) : z \to \alpha z$ *è un endomorfismo del* K*-spazio vettoriale* $K(\alpha)$*.*
2. *Mostrare che il polinomio caratteristico dell'endomorfismo* m_α *è il polinomio minimo,* $M_\alpha(X)$*, di* α *su* K*.*

Esercizio 16 *Sia* $K(\alpha)/K$ *un'estensione algebrica. Sia* $z \in K(\alpha)$ *e sia* $r = [K(\alpha) : K(z)]$*. Si ricorda che se* $B = (y_1, ..., y_q)$ *è una base del* K*-spazio vettoriale* $K(z)$ *e se* $(v_1, ..., v_r)$ *è una base del* $K(z)$*-spazio vettoriale* $K(\alpha)$*, allora* $C = (y_i v_j)$ *è una base del* K*-spazio vettoriale* $K(\alpha)$*.*

1. *Sia* M *la matrice del* K*-endomorfismo:* $m_z : K(z) \to K(z)$*. Allora* $P_M(X) = |X \cdot Id - M| = M_z(X)$ *(Esercizio 15). Sia* $M = (a_{ij})$*. Quindi* $zy_i = \sum_l a_{li} y_l$*. Considerare* $zy_i v_j$ *e scrivere* $mat(m_z; C, C)$*. Concludere che il polinomio caratteristico,* $C_z(X)$*, del* K*-endomorfismo:* $m_z : K(\alpha) \to K(\alpha)$ *è dato da:* $C_z(X) = M_z(X)^r$*.*
2. *Concludere che il grado di ogni* $z \in K' = K(\alpha)$ *divide* $[K' : K]$*; inoltre* z *è primitivo se e solo se* $M_z(X) = C_z(X)$*. (Il grado di* z *è il grado del polinomio minimo di* z *su* K*.)*

2.3 Estensioni normali.

2.3.1 Immersioni nell'universo.

Sia L/K finita (con K estensione finita di $\mathbb{Q}$, $\Omega = \overline{\mathbb{Q}}$).

Definizione 2.22. *Un K-morfismo di L è un morfismo di campi: $\varphi : L \to \Omega$ tale che $\varphi|K = Id_K$. Notiamo $Mor_K(L)$ l'insieme dei K-morfismi di L.*

Per il teorema dell'elemento primitivo (Teorema 2.20), $L = K(u)$. Sia $M(X) = X^n + ... + a_1X + a_0 \in K[X]$ il polinomio minimo di u su K. Dalla relazione $u^n + ... + a_1u + a_0 = 0$ segue $\varphi(u)^n + ... + a_1\varphi(u) + a_0 = 0$ (perché $\varphi|K = Id$).

Quindi φ manda u su un'altra radice di M.

Questa condizione necessaria è anche sufficiente:

Lemma 2.23. *Con le notazioni precedenti $Mor_K(L)$ è in biiezione con l'insieme delle radici di M.*

Dimostrazione. Sia w una radice di M. Ogni $z \in L$ si scrive in modo unico: $z = c_0 + c_1u + ... + c_mu^m = T(u)$ ($c_i \in K$, $m + 1 = deg(M)$). Definiamo $f : K(u) \to \Omega$ tramite $f(z) = T(w)$. È chiaro che $f(z + z') = f(z) + f(z')$. Se $z' = T'(u)$, sia $TT' = MP + Q$, $deg(Q) < deg(M)$ (divisione euclidea). Allora $zz' = T(u)T'(u) = Q(u)$ e $f(zz') = Q(w)$. D'altra parte $T(w)T'(w) = Q(w)$ (perché $M(w) = 0$), quindi $f(z)f(z') = f(zz')$ e f è un morfismo di campi. Chiaramente $f|K = Id$ e $f(u) = w$.

Siccome $\varphi \in Mor_K(L)$ è completamente determinato da $\varphi(u)$ (perché $\varphi|K = Id$), abbiamo la biiezione annunciata (osservare che le radici di M sono distinte). □

In particolare:

$$\boxed{\#Mor_K(L) = deg(M) = dim_K(L)} \tag{2.1}$$

Tra i K-morfismi $\varphi : L \to \Omega$ ci sono quelli che verificano: $\varphi(L) \subset L$: un tale K-morfismo è un K-automorfismo di L. Infatti l'applicazione $\varphi : L \to L$ è K-lineare (perché φ è un K-morfismo), ma φ è iniettivo (come ogni morfismo di campi); siccome $dim_K(L) < \infty$ l'endomorfismo φ del K-spazio vettoriale L, essendo iniettivo è anche suriettivo.

Denotando con $Aut_K(L)$ l'insieme degli K-automorfismi di L, abbiamo quindi $Aut_K(L) \subset Mor_K(L)$. Se $L = K(u)$, gli elementi di $Mor_K(L)$ corrispondono alle radici del polinomio minimo, $M(X) \in K[X]$, di u; gli elementi di $Aut_K(L)$ corrispondono invece alle radici di $M(X)$ *appartenenti a L*.
(Questa descrizione non è molto canonica perché ci sono tanti elementi primitivi, ma è molto comoda!)

In particolare:

$$\boxed{\#Aut_K(L) \leq dim_K(L)} \tag{2.2}$$

2.3.2 Estensioni normali.

Abbiamo visto che $Aut_K(L) \subset Mor_K(L)$ inoltre se $L = K(u)$ e se $M(X) \in K[X]$ è il polinomio minimo di u su K, allora gli elementi di $Mor_K(L)$ corrispondono alle radici di $M(X)$ in Ω, mentre gli elementi di $Aut_K(L)$ corrispondono *alle radici di $M(X)$ appartenenti ad L*. Quindi in generale l'inclusione può essere stretta.

Esempio 2.24. Sia $L = \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, il polinomio minimo di $u = \sqrt[3]{2}$ su $\mathbb{Q}$ è $M(X) = X^3 - 2$, questo polinomio ha un'unica radice reale (u) e due radici complesse coniugate (guardare la derivata). Siccome $L \subset \mathbb{R}$, L non contiene tutte le radici di $M(X)$, quindi $Aut_{\mathbb{Q}}(L) = \{Id\} \neq Mor_{\mathbb{Q}}(L)$.

Definizione 2.25. *L'estensione finita L/K è* normale *se e solo se $Aut_K(L) = Mor_K(L)$.*

Da quanto precede abbiamo subito:

Corollario 2.26. *Sia L/K finita. Sono equivalenti:*

1. *L/K è normale*
2. *Il polinomio minimo di ogni elelmento primitivo u ($L = K(u)$) ha tutte le sue radici in L*
3. *$\#Aut_K(L) = dim_K(L)$.*

Mostriamo adesso un'altra caratterizzazione delle estensioni normali.

Definizione 2.27. *Sia L/K un 'estensione e sia $G \subset Aut_K(L)$ un sottogruppo. Indichiamo con $L^G = \{z \in L \,|\, \sigma(z) = z, \forall \sigma \in G\}$. Si verifica facilmente che L^G è un sotto campo di L; L^G è il* campo fisso *di G.*

Proposizione 2.28. *Sia L/K finita e poniamo $G := Aut_K(L)$. Sono equivalenti:*

1. *L/K è normale*
2. *$L^G = K$.*

Dimostrazione. (1) $\Rightarrow$ (2): Abbiamo $K \subset L^G \subset L$ e $Aut_{L^G}(L) = G$. Infatti è chiaro che $Aut_{L^G}(L) = \{\sigma \in Aut(L) \,|\, \sigma|L^G = Id\}$ è contenuto in $Aut_K(L) = G$. D'altra parte se $\sigma \in G$, allora per ogni $z \in L^G$, $\sigma(z) = z$, quindi $\sigma|L^G = Id$.

Dalla formula (2.2) $dim_{L^G}(L) \geq |G|$. Abbiamo: $dim_K(L) = dim_{L^G}(L).dim_K(L^G)$. D'altra parte: $dim_K(L) = |G|$ (Corollario 2.26). Quindi $dim_K(L^G) \leq 1$, cioè $L^G = K$.
(2) $\Rightarrow$ (1): Sia $Aut_K(L) = G = \{\sigma_1 = Id, ..., \sigma_m\}$. Sia $L = K(u)$ e consideriamo il polinomio $P(X) = \prod_{i=1}^{m}(X - \sigma_i(u))$. A priori $P(X) \in L[X]$. I coefficienti di P sono (a meno del segno) le funzioni simmetriche elementari delle radici: $a_i = e_i(\sigma_1(u), ..., \sigma_m(u))$. Se $\sigma \in G$, $\sigma(a_i) = e_i(\sigma\sigma_1(u), ..., \sigma\sigma_m(u))$, cioè

l'effetto di σ è solo di permutare le variabili: $\sigma(a_i) = e_i(\sigma_{i_1}(u), ..., \sigma_{i_m}(u))$, siccome e_i è simmetrico, $\sigma(a_i) = a_i$. Quindi $a_i \in L^G = K$. Pertanto $P(X) \in K[X]$. Siccome $P(u) = 0$ ($\sigma_1 = Id$), il polinomio minimo di u su K, $M(X)$, divide $P(X)$, quindi: $dim_K(L) = deg(M) \leq deg(P) = |G|$. Dalla Formula (2.2), $dim_K(L) = |G|$ e quindi (Corollario 2.26) L/K è normale. □

Il lemma seguente sarà utile a varie riprese.

Lemma 2.29. *Sia $K \subset F \subset L$ una torre di estensioni (L/K finita). Sia $\sigma : F \to \Omega$ un K-morfismo. Esistono $n = [L : F]$ estensioni di σ: $\tilde{\sigma}_i : L \to \Omega$, $\tilde{\sigma}_i$ K-morfismi.*

Dimostrazione. Sia $L = F(u)$ e sia $M(X) \in F[X]$ il polinomio minimo di u su F. Se $P(X) = \sum a_i X^i \in F[X]$ si pone: $P_\sigma(X) = \sum \sigma(a_i) X^i \in \Omega[X]$. Siano $\omega_1, ..., \omega_n$ le radici di $M_\sigma(X)$ in Ω. Ogni $z \in L$ si scrive in modo unico: $z = T(u) := a_0 + a_1 u + ... + a_{n-1} u^{n-1}$, $a_i \in F$. Per ogni ω_i si definisce $\tilde{\sigma}_i : L \to \Omega$ tramite $\tilde{\sigma}_i(z) = T_\sigma(\omega_i)$. È chiaro che $\tilde{\sigma}_i \mid F = \sigma$ (quindi $\tilde{\sigma}_i \mid K = Id$) e che $\tilde{\sigma}_i(z + z') = \tilde{\sigma}_i(z) + \tilde{\sigma}_i(z')$. Se $z' = T'(u)$ sia $TT' = MP + Q$, $deg(Q) < deg(M)$ (divisione euclidea). Allora $zz' = T(u)T'(u) = (TT')(u) = Q(u)$ e $\tilde{\sigma}_i(zz') = Q_\sigma(\omega_i)$. D'altra parte $\tilde{\sigma}_i(z)\tilde{\sigma}_i(z') = T_\sigma(\omega_i)T'_\sigma(\omega_i) = Q_\sigma(\omega_i)$ (perché $M_\sigma(\omega_i) = 0$), quindi $\tilde{\sigma}_i(zz') = \tilde{\sigma}_i(z).\tilde{\sigma}_i(z')$.

Siccome $M(X)$ è irriducibile su F anche $M_\sigma(X)$ lo è (su $\sigma(F)$) e quindi le radici ω_i sono distinte. Siccome $\tilde{\sigma}_i(u) = \omega_i$, $\tilde{\sigma}_i \neq \tilde{\sigma}_j$ se $i \neq j$. □

Ancora un'altra caratterizzazione delle estensioni normali:

Lemma 2.30. *Sia L/K un'estensione finita. Sono equivalenti:*

1. *L/K è normale*
2. *ogni polinomio irriducibile $P(X) \in K[X]$ che ha una radice in L ha* tutte *le sue radici in L.*

Dimostrazione. (1) $\Rightarrow$ (2): Sia $g(X) \in K[X]$ irriducibile con $g(a) = 0$, $a \in L$. Sia $b \in \Omega$ una radice di g e consideriamo $\varphi : K(a) \to K(b)$ definito da $\varphi(a) = b$, $\varphi|K = Id$. È chiaro che φ è un K-morfismo ($a \notin K$ perchè g irriducibile su K). Per il Lemma 2.29 esiste $\tilde{\varphi} : L \to \Omega$, K-morfismo che estende φ. Siccome L/K è normale $\tilde{\varphi}(L) = L$, quindi $\tilde{\varphi}(a) = b \in L$.
(2) $\Rightarrow$ (1): Sia $L = K(u)$ e sia $M(X) \in K[X]$ il polinomio minimo di u, allora M è irriducibile su K e $M(u) = 0$. L'ipotesi implica che M ha tutte le sue radici in L, pertanto (Corollario 2.26) L/K è normale. □

Prima di dare l'ultima caratterizzazione delle estensioni normali, ricordiamo, in tutta generalità, alcuni fatti sul *campo di spezzamento* di un polinomio $f(x) \in k[x]$. Sia L/k un'estensione, il polinomio f spezza in L se esistono $r_1, ..., r_n \in L$ tali che $f(x) = \lambda(x - r_1)...(x - r_n)$.

Definizione 2.31. *Un campo di spezzamento di $f(x)$ su k è un'estensione K/k tale che f spezzi su K e tale che non esista nessun campo intermedio $k \subset F \subset K$ tale che f spezzi su F.*

Si dimostra che un campo di spezzamento esiste sempre (cf Esercizio 18). Per noi, visto la nostra convenzione, la situazione è abbastanza semplice: se K è un'estensione finita di $\mathbb{Q}$, allora $K \subset \Omega$ e ogni $f(x) \in K[x]$ ha tutte le sue radici in Ω, quindi il campo di spezzamento di f su K è $K(r_1, ..., r_n)$ dove $r_1, ..., r_n$ sono le radici di f in Ω.

Potrebbe sembrare che ci siano varie alternative nel costruire un campo di spezzamento: lo stesso polinomio $f(x) \in K[x]$, può essere visto come un polinomio (riducibile) a coefficienti in $K(r_i)$ dove r_i è una radice di f, ma si dimostra che il campo di spezzamento è unico modulo isomorfismi (cf Esercizio 19).

Passiamo ora all'ultima caratterizzazione delle estensioni normali, quella che poi ci interessa di più (relativamente alla teoria di Galois). Iniziamo con:

Lemma 2.32. *Sia L/K un'estensione, se L è il campo di spezzamento di un polinomio $P(X) \in K[X]$, allora L/K è normale.*

Dimostrazione. Sia $L = K(r_1, ..., r_n)$ dove $r_1, ..., r_n$ sono le radici (non necessariamente distinte) di $P(X) \in K[X]$. Ogni K-morfismo $\sigma : L \to \Omega$, manda una radice in un'altra radice (cioè $\sigma(r_i) \in \{r_1, ..., r_n\}, \forall i$). Pertanto $\sigma(L) \subset L$, i.e. $Mor_K(L) = Aut_K(L)$ e L/K è normale. □

Osservazione 2.33. Il polinomio P del Lemma 2.32 può avere radici multiple o non essere irriducibile.

Finalmente abbiamo:

Proposizione 2.34. *Sia L/K finita. Sono equivalenti:*

1. *L/K è normale*
2. *L è il campo di spezzamento di un polinomio $P(X) \in K[X]$ ($P(X)$ irriducibile o $P(X)$ separabile, cioè senza radici multiple).*

Dimostrazione. (1) $\Rightarrow$ (2): Sia $L = K(u)$ e sia $M(X) \in K[X]$ il polinomio minimo di u su K. Il polinomio $M(X)$ è irriducibile su K (quindi separabile, cioè non ha radici multiple) e ha tutte le sue radici in L (Corollario 2.26), quindi $L = K(u)$ è il campo di spezzamento di $M(X)$. (Un campo intermedio $K \subset F \subset L$ contenente tutte le radici di $M(X)$, contiene K e u, quindi $F = L$).
(2) $\Rightarrow$ (1): Viceversa se L è il campo di spezzamento di un polinomio $P(X) \in K[X]$, allora L/K è normale (Lemma 2.32). □

Per riassumere:

Proposizione 2.35. *Sia L/K finita, poniamo $G := Aut_K(L)$, $L^G := \{z \in L \,|\, \sigma(z) = z, \forall \sigma \in G\}$.*
Sono equivalenti:

1. *L/K è normale*

2. $|G| = dim_K(L)$
3. $L^G = K$
4. *ogni polinomio* $P(X) \in K[X]$, *irriducibile in* $K[X]$, *che ha una radice in* L, *ha* tutte *le sue radici in* L
5. L *è il campo di spezzamento di* $P(X) \in K[X]$
6. L *è il campo di spezzamento di* $P(X) \in K[X]$, *con* P *separabile (risp.* P *irriducibile).*

Concludiamo con un'ultima osservazione:

Lemma 2.36. *Sia* $K \subset F \subset L$ *una torre di estensioni con* L/K *finita. Se* L/K *è normale, allora anche* L/F *è normale.*

Dimostrazione. Sia u tale che $L = K(u)$, allora $L = F(u)$ (perché $L = K(u) \subset F(u) \subset L$). Siano M_K, M_F i polinomi minimi di u su K, F. In $F[X]$ abbiamo $M_K = M_F.P$; quindi tutte le radici di M_F sono radici di M_K e pertanto appartengono a L (perché L/K è normale; Corollario 2.26). Questo implica (Corollario 2.26) che anche L/F è normale. □

Osservazione 2.37. Sia $K \subset F \subset L$ una torre di estensioni con L/K normale. Dal Lemma 2.36 possiamo concludere che L/F è normale; ma *non possiamo concludere nulla su l'estensione* F/K (cf Esercizio 17).

—— .. ——

Esercizi.

Esercizio 17

1. *Sia $p \in \mathbb{N}$ un numero primo. Mostrare che il polinomio $f(x) = x^3 + p \in \mathbb{Q}[x]$ è irriducibile, con un'unica radice reale u.*
2. *Sia $F = \mathbb{Q}(u)$, $L = \mathbb{Q}(u, r_2, r_3)$ dove u, r_2, r_3 sono le radici di $f(x)$. Abbiamo: $\mathbb{Q} \subset F \subset L$. Mostrare che $L/\mathbb{Q}$ è normale.*
3. *Mostrare che L/F è normale*
4. *Mostrare che $F/\mathbb{Q}$ <u>non</u> è normale.*

Esercizio 18 *Scopo di questo esercizio è di mostrare l'esistenza di un campo di spezzamento.*

1. *Sia $h(x) \in k[x]$ un polinomio e sia L/k un'estensione tale che h spezzi in L: $h(x) = \lambda(x - r_1)...(x - r_n)$. Mostrare che $k(r_1, ..., r_n)$ è un campo di spezzamento di h su k.*
2. *Sia $f(x) \in k[x]$ un polinomio irriducibile. Osservare che $F := k[x]/(f(x))$ è un campo contenente k e mostrare che $f(X) \in F[X]$ fattorizza come $f(X) = h(X)f_1(X)$, $\deg(h), \deg(f_1) \geq 1$.*
3. *Dedurre l'esistenza di un campo di spezzamento per ogni $h(x) \in k[x]$.*
4. *Mostrare che se L è un campo di spezzamento di f su k, allora L/k è algebrica finita.*

Esercizio 19 *Scopo dell'esercizio è di mostrare l'unicità (modulo isomorfismi) del campo di spezzamento.*

Sia $f(x) \in K[x]$ e sia L un campo di spezzamento di f su K; inoltre sia $i : K \to F$ un morfismo di campi. Se $f(x) = \sum a_j x^j \in K[x]$ indichiamo con $i(f)(x) \in F[x]$ il polinomio $\sum i(a_j)x^j$.

1. *Mostrare che se esiste un morfismo di campi $\varphi : L \to F$ con $\varphi|K = i$, allora $i(f)$ spezza in F.*
2. *Si tratta adesso di mostrare che se $i(f)$ spezza in F, allora esiste un morfismo $\varphi : L \to F$ che estende i. Si procede per induzione su $n = \deg(f)$. Il caso $n = 1$ è immediato (perché?).*
   Sia $r_1 \in L$ una radice di f, r_1 è algebrico su K. Sia $m(x)$ il polinomio minimo di r_1 su K. Abbiamo $f(x) = m(x)h(x)$ in $K[x]$ (perché?). Quindi $i(f) = i(m)i(h)$ e siccome $i(f)$ spezza su F, anche $i(m)$ spezza su F: $i(m)(x) = \prod^t (x - \alpha_i)$, $\alpha_i \in F$. Mostrare che esiste $j : K(r_1) \to i(K)(\alpha_1)$, con $j(r_1) = \alpha_1$, che estende $i : K \to i(K)$.
3. *In $K(r_1)$ abbiamo $f(x) = (x - r_1)g(x)$, con $\deg(g) = n - 1$. Concludere usando l'ipotesi di induzione.*
4. *Concludere che il campo di spezzamento di un polinomio è unico modulo isomorfismi.*

Esercizio 20 *Sia $f(x) \in \mathbb{Q}[x]$ un polinomio (non necessariamente irriducibile) di grado n. Sia $L = \mathbb{Q}(r_1, ..., r_n)$ dove $r_1, ..., r_n$ sono le radici di f in Ω.*

1. *Mostrare che L è il campo di spezzamento di f*
2. *Mostrare che $[L : \mathbb{Q}]$ divide $n!$ (In particolare $L/\mathbb{Q}$ è algebrica finita).*

Esercizio 21 *Siano $\alpha, \beta \in \overline{\mathbb{Q}}$. Indichiamo con E_α, E_β i campi di spezzamento dei polinomi minimi $M_\alpha(X)$, $M_\beta(X)$ di α, β su $\mathbb{Q}$.*

1. *Mostrare che se $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\beta)$, allora $E_\alpha \subset E_\beta$. Concludere che se $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$, allora $E_\alpha = E_\beta$*
2. *Mostrare che l'implicazione inversa non è vera: cioè si può avere $E_\alpha = E_\beta$ senza che $\mathbb{Q}(\alpha)$ sia contenuto in $\mathbb{Q}(\beta)$ (o $\mathbb{Q}(\beta)$ in $\mathbb{Q}(\alpha)$). (Hint: $\alpha = \sqrt[3]{2}$, $\beta = j\sqrt[3]{2}$, j radice cubica primitiva dell'unità.)*

Esercizio 22 *Sia $z \in \mathbb{Q}(\alpha)$ (α algebrico su $\mathbb{Q}$). Si pone $n = [\mathbb{Q}(\alpha) : \mathbb{Q}]$, $r = [\mathbb{Q}(\alpha) : \mathbb{Q}(z)]$, $t = [\mathbb{Q}(z) : \mathbb{Q}]$. Siano $\sigma_1, ..., \sigma_n$ le n-immersioni di $\mathbb{Q}(\alpha)$ in Ω (cf Lemma 2.23). Mostrare che $C_z(T) = \prod_{i=1}^{n}(T - \sigma_i(z))$, dove $C_z(T)$ è il polinomio caratteristico del $\mathbb{Q}$-endomorfismo $m_z : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha) : t \to zt$. (Hint: usare il Lemma 2.29 e l'Esercizio 16.)*

2.4 Il gruppo di Galois.

2.4.1 Definizione moderna.

Iniziamo con un cambio di notazioni (dopotutto stiamo considerando la teoria di Galois!):

Definizione 2.38. *Sia $K \subset L$ un'estensione algebrica finita. Il* gruppo di Galois *dell'estensione L su K è: $Gal(L/K) := Aut_K(L)$.*

Questa, beninteso, è la definizione moderna, come si riallaccia al nostro problema della risoluzione delle equazioni algebriche?

Sia $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_0 \in \mathbb{Q}[x]$ un polinomio irriducibile. In Ω abbiamo: $f(x) = (x - r_1) \cdots (x - r_n)$, con $r_i \neq r_j$ se $i \neq j$ perché f è irriducibile. Consideriamo il campo di spezzamento di f: $L = \mathbb{Q}(r_1, ..., r_n)$. L'estensione $L/\mathbb{Q}$ è normale (Proposizione 2.35). Secondo la Definizione 2.38, $Gal(L/\mathbb{Q}) = Aut_{\mathbb{Q}}(L)$ è il gruppo degli automorfismi di L che lasciano fisso $\mathbb{Q}$ (l'estensione $L/\mathbb{Q}$ essendo normale, se $G = Aut_{\mathbb{Q}}(L)$, $L^G = \mathbb{Q}$, cf Proposizione 2.35). Più generalmente:

Definizione 2.39. *Sia $f(x) \in K[x]$ un polinomio separabile e sia L il campo di spezzamento di f su K. Il gruppo di Galois di $f(x)$ su K è: $Gal_K(f) = Aut_K(L)$.*

Se $\sigma \in Gal(L/\mathbb{Q})$, allora dalla relazione $0 = f(r_i) = r_i^n + a_{n-1}r_i^{n-1} + ... + a_0$, segue: $0 = \sigma(f(r_i)) = \sigma(r_i)^n + a_{n-1}\sigma(r_i)^{n-1} + ... + a_0 = f(\sigma(r_i))$. Infatti se $a \in \mathbb{Q}$: $\sigma(ar_i^k) = \sigma(a)\sigma(r_i^k) = a\sigma(r_i)^k$ perché σ è un morfismo di campi e $\sigma|\mathbb{Q} = Id$.

Vediamo quindi che $\sigma(r_i)$ è una radice di $f(x)$: $\sigma(r_i) = r_{\sigma(i)}$. Quindi σ induce una permutazione di $\{r_1, ..., r_n\}$. Dopo avere fissato un ordine sulle radici possiamo identificare $Gal(L/\mathbb{Q})$ a un sotto gruppo di S_n, il gruppo di <u>tutte</u> le permutazioni delle radici.

Un esempio stupido ci farà capire che in generale $Gal(L/\mathbb{Q}) \neq S_n$. Consideriamo $f(x) = (x^2 - 2)(x^2 - 3)$, non è irriducibile ma le sue radici $r_{1,2} = \pm\sqrt{2}, r_{3,4} = \pm\sqrt{3}$ sono distinte. Abbiamo $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ e l'estensione $L/\mathbb{Q}$ è normale. Quali elementi di S_4 sono in $Gal(L/\mathbb{Q})$? Siccome $x^2 - 2 \in \mathbb{Q}[x]$, se $\sigma \in Aut_{\mathbb{Q}}(L)$, dalla relazione $r_1^2 - 2 = 0$ deve seguire $\sigma(r_1)^2 - 2 = 0$, quindi $\sigma(r_1)$ non può essere che r_1 o r_2. Nello stesso modo ($x^2 - 3 \in \mathbb{Q}[x]$), $\sigma(r_3) = r_3$ o r_4. Vediamo quindi che $Gal(L/\mathbb{Q}) = \{(\tau_1, Id), (\tau_1, \tau_2), (Id, \tau_2), (Id, Id)\}$, dove τ_1 scambia r_1 con r_2, τ_2 scambia r_3 con r_4. In conclusione $Gal(L/\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ ha quattro elementi contro i 24 elementi di S_4.

Osserviamo che le permutazioni del gruppo di Galois sono il *cuore* dell'equazione. Infatti usando relazioni algebriche a coefficienti in $\mathbb{Q}$ noi possiamo distinguere $\pm\sqrt{2}$ da $\pm\sqrt{3}$: se $P(x) = x^2 - 2$, $P(\pm\sqrt{2}) = 0$, mentre $P(\pm\sqrt{3}) = 1$, <u>ma non abbiamo alcun modo</u>, usando polinomi a coefficienti in $\mathbb{Q}$, per distinguere $\sqrt{2}$ da $-\sqrt{2}$ e $\sqrt{3}$ da $-\sqrt{3}$ e la *complessità* (Galois direbbe

l'ambiguità) dell'equazione (su $\mathbb{Q}$) sta tutta lì. Il gruppo di Galois misura questa ambiguità.

É chiaro che il gruppo di Galois $Gal_{\mathbb{Q}}(f) := Gal(L/\mathbb{Q})$ dove L è il campo di spezzamento di f è un oggetto naturale, quindi importante, nello studio dell'equazione $f(x) = 0$. Non è altrettanto chiaro come possa essere utile nel problema della risoluzione per radicali.

Usando sempre il nostro esempio stupido $f(x) = (x^2 - 2)(x^2 - 3)$, cerchiamo di dare un'idea. Come già detto il gruppo di Galois consta di quattro permutazioni delle radici $r_1, ..., r_4$ che sono, con notazioni evidenti:

$$\tau_1 = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 2\ 1\ 3\ 4 \end{pmatrix},\ \tau_2 = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 1\ 2\ 4\ 3 \end{pmatrix},\ \rho = \tau_1 \circ \tau_2,\ Id.$$

Estraiamo la radice di 3, cioè invece di lavorare in $\mathbb{Q}$, lavoriamo in $F = \mathbb{Q}(\sqrt{3})$. In F possiamo distinguere $\sqrt{3}$ da $-\sqrt{3}$ (con il polinomio $x - \sqrt{3} \in \mathbb{Q}(\sqrt{3})[x]$), ma non $\pm\sqrt{2}$: il gruppo $Gal(L/F) = G_1 = \{Id, \tau_1\}$. Osserviamo che $L^{G_1} = \mathbb{Q}(\sqrt{3})$. Finalmente quando estraiamo la radice di due, cioè quando siamo in L, il gruppo di Galois si riduce a $\{Id\}$. Quindi alla torre $\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt{3}, \sqrt{2})$, che rappresenta la risoluzione per radicali della nostra equazione, corrisponde una torre di gruppi $G \supset G_1 \supset \{Id\}$.

Tutto questo è abbastanza ovvio visto che conosciamo le radici della nostra equazione. Ma si può fare di più! Sia $h(x) \in \mathbb{Q}[x]$ un polinomio del quarto grado con radici (in Ω) $r_1, ..., r_4$. Supponiamo di sapere che $h(x)$ ha lo stesso gruppo di Galois di $f(x)$: $Gal_{\mathbb{Q}}(h) = \{\tau_1, \tau_2, \rho, Id\} =: G$. Come già detto $L^G = \mathbb{Q}$ (L campo di spezzamento di h). Inoltre supponiamo anche di sapere che:

- Se $H := \{Id, \tau_1\}$, $L^H = \mathbb{Q}(r_3, r_4)$

Chiaramente $r_1 + r_2$ e $r_1 r_2$ sono fissati da τ_1, quindi da H, pertanto $r_1 + r_2$, $r_1 r_2 \in L^H = \mathbb{Q}(r_3, r_4)$. Pertanto r_1, r_2 sono radici dell'equazione $X^2 - (r_1 + r_2)X + r_1 r_2 = 0$, a coefficienti in $\mathbb{Q}(r_3, r_4)$. Risolvendo nel solito modo otteniamo:

$$r_{1,2} = (-\beta \pm \sqrt{\beta^2 - 4\alpha\gamma})/2\alpha \tag{2.3}$$

dove α, β, γ sono dei polinomi in r_3, r_4.

Adesso $r_3 + r_4$, $r_3 r_4$ sono fissati da τ_1 e da τ_2, quindi da tutto G. Questo implica $r_3 + r_4$, $r_3 r_4 \in \mathbb{Q}$. Quindi r_3, r_4 sono soluzioni di un'equazione del secondo grado, a coefficienti razionali: $r_{3,4} = (-b \pm \sqrt{b^2 - 4ac})/2a$, $a, b, c \in \mathbb{Q}$. Rimpiazzando questi valori nell'Equazione (2.3), abbiamo espresso tutte le radici in formule radicali a coefficienti razionali.

In conclusione, senza conoscere l'equazione ma avendo informazioni sulla struttura del suo gruppo di Galois siamo in grado di dire che l'equazione è risolubile per radicali (senza però dare la formula di risoluzione!).

L'esempio precedente ha messo in evidenza la corrispondenza tra campi intermedi $\mathbb{Q} \subset F \subset L$ e sotto gruppi del gruppo di Galois: $G \supset G_1 \supset \{1\}$. Lo studio generale di questa corrispondenza sarà l'oggetto della Sezione **??**, ma

prima facciamo una pausa di natura storica. Il lettore che non fosse interessato allo sviluppo storico può benissimo saltare il prossimo paragrafo (perderà solo un pó di bella matematica).

2.4.2 Il gruppo di Galois *à la Galois.*

Ripercorriamo adesso, aiutandoci dalla terminologia moderna, la prima parte della famosa memoria *Sur les conditions de résolubilité des équations par radicaux* in cui Galois introduce per la prima volta la nozione di gruppo e dove definisce il gruppo di Galois del polinomio $f(x)$.

Abbiamo quindi $f(x) = x^n + ... + a_0 \in K[x]$, polinomio irriducibile. Sia $f(x) = (x - r_1)...(x - r_n) \in \Omega[x]$ (quindi $r_i \neq r_j$ se $i \neq j$). Si nota $L = K(r_1, ..., r_n)$ il campo di spezzamento di f. L'esempio base è con $K = \mathbb{Q}$, ma nelle definizioni preliminari Galois spiega chiaramente che K può essere anche un'estensione finita di $\mathbb{Q}$.

Per prima cosa (sono i Lemma II e III della memoria) Galois dimostra una versione forte del Teorema dell'elemento primitivo, adatta alla sua situazione:

Proposizione 2.40. *Se $A_1, ..., A_n \in K$ e se $t = A_1r_1 + ... + A_nr_n$, si definisce, $\forall \sigma \in S_n$, l'elemento $\sigma(t) \in L$ tramite:*

$$\sigma(t) := A_1r_{\sigma(1)} + ... + A_nr_{\sigma(n)}$$

1. *Allora è possibile scegliere $A_1, ..., A_n$ (e addirittura con $A_i \in \mathbb{N}$) tali che: $\sigma(t) \neq \tau(t)$ se $\sigma \neq \tau$ ($\sigma, \tau \in S_n$).*
2. *Se (1) è verificato allora: $K(r_1, ..., r_n) = K(t)$.*

La dimostrazione data da Galois è solo una traccia. Infatti nel suo rapporto all'Académie des Sciences, Poisson scriverà: *La dimostrazione di questo lemma è insufficiente, ma il risultato è vero in virtù del no. 100 del trattato di Lagrange.* Nel rivedere il suo manoscritto, Galois aveva riportato, come nota, questo commento di Poisson e aveva aggiunto: *On jugera* (si giudicherà, si vedrà). Nella versione pubblicata a cura di Liouville della memoria di Galois ([9]), c'è scritto: *Questa proposizione è citata da Abel senza dimostrazione, nella memoria postuma sulle funzioni ellitiche.* Altrove Galois dice: *In ogni caso mi sarebbe facile dimostrare che non conoscevo neanche il nome di Abel quando ho presentato per la prima volta all'Institut le mie ricerche sulle equazioni e che la soluzione di Abel non avrebbe potuto essere pubblicata prima della mia.* Comunque sia la Proposizione è vera e il lettore curioso ne troverà una dimostrazione nell'appendice.

Un t che verifica la proposizione viene chiamato *risolvente di Galois.*

Dopodiché Galois considera il polinomio: $F(X) = \prod_{\sigma \in S_n} (X - \sigma(t))$. Abbiamo:

Lemma 2.41. *Sia t una risolvente di Galois e sia $F(X) = \prod_{\sigma \in S_n} (X - \sigma(t))$, allora $F(X) \in K[X]$.*

Dimostrazione. A priori $F(X) \in K(r_1, ..., r_n)[X]$, ma i suoi coefficienti, C_i sono i polinomi elementari simmetrici nelle radici: $C_i = e_i(\sigma_1(t), ..., \sigma_{n!}(t))$. Ogni $\sigma_i(t)$ è un polinomio a coefficienti in K negli $r_1, ..., r_n$ ($\sigma_i(t) \in K[r_1, ..., r_n]$). Quindi $e_i(\sigma_1(t), ..., \sigma_{n1}(t)) \in K[r_1, ..., r_n]$. Se permutiamo le radici r_i, questo torna a permutare i $\sigma_i(t)$, siccome e_i è simmetrico negli $\sigma_i(t)$, questo non cambia C_i, cioè $C_i = C_i(r_1, ..., r_n)$ è un polinomio simmetrico negli r_i, a coefficienti in K. Per il Teorema delle funzioni simmetriche, esiste un polinomio h a coefficienti in K tale che: $C_i = h(e_1(r_1, ..., r_n), ..., e_n(r_1, ..., r_n))$. Siccome gli $e_i(r_1, ..., r_n)$ sono i coefficienti del nostro polinomio $f(x) \in K[x]$, $C_i \in K$. $\square$

Siccome $F(X) \in K[X]$ possiamo considerare la sua fattorizzazione in fattori irriducibili su K:

$$F(X) = F_1(X)...F_r(X) \ , \ \ F_i(X) \in K[X] \tag{2.4}$$

Siccome $F(t) = 0$ (possiamo assumere $\sigma_1 = Id$), esiste j tale che $F_j(t) = 0$, riordinando semmai gli indici, possiamo assumere $F_1(t) = 0$. Osserviamo che se $j \neq 1$, allora $F_j(t) \neq 0$. Infatti abbiamo $F(X) = \prod_{\sigma \in S_n} (X - \sigma(t))$, ma siccome $\sigma(t) \neq \sigma'(t)$ se $\sigma \neq \sigma'$, $F(x)$ non ha radice multiple e quindi ogni radice di $F(X)$ individua uno ed uno solo fattore $F_i(X)$ nella fattorizzazione (2.4). Perciò il fattore F_1 è univocamente determinato dalla condizione $F_1(t) = 0$.

Siccome $F(X) = \prod_{\sigma \in S_n} (X - \sigma(t))$, le radici di $F_1(X)$ sono tutte della forma: $\sigma_1(t), ..., \sigma_m(t)$ ($\sigma_1 = Id$), cioè:

$$F_1(X) = (X - \sigma_1(t))(X - \sigma_2(t))...(X - \sigma_m(t)) \ , \ \ \sigma_1 = Id \tag{2.5}$$

La relazione (2.5) individua un sotto insieme, G, di S_n: $G := \{\sigma_1, ..., \sigma_m\}$.

Osserviamo che $F_1(X)$ è il polinomio minimo di t e possiamo anticipare che:

Definizione 2.42. *Con le notazioni precedenti, G è il gruppo di Galois di $f(x)$.*

A questo punto **l'osservazione cruciale** di Galois è che **ogni** elemento $\sigma(t)$ è un elemento primitivo.

Infatti se $t' = \sigma(t)$, $\tau(t') = \tau'(t') \Leftrightarrow \tau(\sigma(t) = \tau'(\sigma(t))$, quindi $\tau\sigma = \tau'\sigma$ e questo implica $\tau = \tau'$. Quindi t' verifica (1) della Proposizione 2.40 e pertanto è un elemento primitivo.

Quindi se $\sigma(t)$ è radice di $F_i(X)$ in (2.4), $F_i(X)$ è il polinomio minimo di $\sigma(t)$ (perché irriducibile) e quindi ha grado m. Pertanto la relazione (2.4) fornisce una partizione di S_n in r sotto insiemi, ognuno di cardinalità m: $G = G_1, G_2, ..., G_r$ (sono le classi di equivalenza nella relazione $\sigma R \tau \Leftrightarrow \sigma\tau^{-1} \in G$, cf Esercizio 23). É proprio questa partizione (presentazione) che ha fatto venire in mente a Galois la struttura di gruppo.

In particolare: $mr = n!$ cioè: $|G|$ divide $|S_n|$ (teorema di Lagrange).

Vediamo adesso che le permutazioni in G sono proprio quelle che rispettano le relazioni algebriche su K, cioè $G = Aut_K(L)$.

Ogni permutazione $\sigma \in S_n$ definisce un'applicazione: $\tilde{\sigma} : L \to L$ nel modo seguente: se $z \in L$, z si scrive in modo unico: $z = b_0 + b_1 t + ... + b_{m-1} t^{m-1}$ e si pone: $\tilde{\sigma}(z) = b_0 + b_1 \sigma(t) + ... + b_{m-1} \sigma(t)^{m-1}$. Siccome $\sigma(t) \in L, \forall \sigma \in S_n$, l'applicazione è ben definita.

Chiaramente $\tilde{\sigma}_{|K} = Id_K$ ($\tilde{\sigma}$ fissa K).

Proposizione 2.43. *Sia $\sigma \in S_n$. L'applicazione $\tilde{\sigma} : L \to L$ è un morfismo di campi se e solo se $\sigma \in G$.*

Dimostrazione. (i) Mostriamo che se $\sigma \in G$, $\tilde{\sigma}$ è un morfismo.

La condizione $\tilde{\sigma}(z + z') = \tilde{\sigma}(z) + \tilde{\sigma}(z')$ è ovviamente verificata. Siano $z = b_0 + b_1 t + ... + b_{m-1} t^{m-1} = P(t)$, $z' = Q(t)$ due elementi di L. Allora $zz' = P(t)Q(t) = (PQ)(t)$. Dividiamo PQ per il polinomio minimo $M = F_1$ di t: $PQ = MT + R$ $(+)$ dove $deg(R) < m$. Allora: $zz' = (PQ)(t) = R(t)$ (perché $M(t) = 0$). Quindi: $\tilde{\sigma}(zz') = R(\sigma(t))$. D'altra parte $\tilde{\sigma}(z)\tilde{\sigma}(z') = P(\sigma(t))Q(\sigma(t)) = (PQ)(\sigma(t))$. Siccome $\sigma \in G$, $\sigma(t)$ è radice di M, quindi usando $(+)$ viene: $(PQ)(\sigma(t)) = R(\sigma(t))$. Pertanto $\tilde{\sigma}(zz') = \tilde{\sigma}(z)\tilde{\sigma}(z')$.

(ii) Sia $\sigma \in S_n \setminus G$ e mostriamo che $\tilde{\sigma}$ *non* è un morfismo di campi.

Come prima prendiamo $z = P(t)$, $z' = Q(t)$ ma questa volta prendiamo per P e Q dei polinomi unitari di grado $m-1$. Quindi $zz' = (PQ)(t)$ dove PQ ha grado $2m-2$. Come prima $PQ = F_1 T + R$, $deg(R) < m$ e $deg(T) = m-2$. Abbiamo $\tilde{\sigma}(zz') = R(\sigma(t))$ e $\tilde{\sigma}(z)\tilde{\sigma}(z') = F_1(\sigma(t))T(\sigma(t)) + R(\sigma(t))$. Quindi:

$$\tilde{\sigma} \ \text{è un morfismo} \Leftrightarrow F_1(\sigma(t)).T(\sigma(t)) = 0$$

Siccome $\sigma \notin G$, $F_1(\sigma(t)) \neq 0$. Quindi deve essere: $T(\sigma(t)) = 0$. Ma $\sigma(t)$ è radice di $F(X)$ e quindi di un suo fattore irriducibile, diciamo F_r. Siccome F_r e T hanno una radice comune, essendo F_r irriducibile, F_r divide T, ma questo è assurdo perché $m - 2 = deg(T) < deg(F_r) = m$. □

Se $\tilde{\sigma} : L \to L$ è un morfismo di campi, allora $\tilde{\sigma}$ è iniettivo (come ogni morfismo di campi), inoltre $\tilde{\sigma}$ è un endomorfismo del K-spazio vettoriale L, essendo iniettivo è anche suriettivo. In conclusione $\forall \sigma \in G$, $\tilde{\sigma} \in Aut_K(L)$.

Per mostrare che G è un gruppo, Galois mostra che: $\sigma \in G, \tau \in G \Rightarrow \sigma\tau \in G$ (*Donc, si dans un pareil groupe on a les substitutions S et T, on est sûr d'avoir la substitution ST. Telles sont les définitions que nous avons cru devoir rappeler*, cioè: *Quindi se in un tale gruppo abbiamo le permutazioni S e T, siamo sicuri di avere la permutazione ST. Tali sono le definizioni che ci è sembrato opportuno dovere ricordare*).

Lemma 2.44. *Con le notazioni precedenti se $\sigma, \tau \in G$, allora $\sigma\tau \in G$. In particolare G è un gruppo.*

Dimostrazione. Sia α una radice di $F_1(X) = c_0 + c_1 X + ... + X^m$, il polinomio minimo di t. Se $\sigma \in G$: $F_1(\alpha) = 0 \Rightarrow \tilde{\sigma}(F_1(\alpha)) = F_1(\tilde{\sigma}(\alpha)) = 0$ (σ permuta le

radici di F_1). Se $\tau \in G$, allora $\tau(t) = \alpha$ per una qualche radice α di $F_1(X)$ (è la definizione). Abbiamo appena visto che $\sigma(\alpha) = \sigma(\tau(t))$ è ancora radice di F_1, quindi $\sigma\tau \in G$.

Segue che per ogni $\sigma \in G$ abbiamo un'applicazione: $\varphi_\sigma : G \to G : \sigma_i \to \sigma\sigma_i$. L'applicazione φ_σ è chiaramente iniettiva, e quindi suriettiva (G è un insieme finito), perciò esiste $\tau \in G$ tale che $\varphi_\sigma(\tau) = \sigma\tau = Id$, quindi $\tau = \sigma^{-1} \in G$ e G è un (sotto)gruppo (di S_n). $\square$

Quindi in realtà Galois ha preso per buono che S_n fosse un gruppo (cosa abbastanza evidente: c'è chiaramente il neutro, i simmetrici e la composizione è palesamente interna ed associativa) e ha dimostrato che G è un sotto gruppo di S_n (cf Esercizio 25).

Per concludere che G non dipende dalle scelte fatte (l'ordine sulle radici, la scelta di t), Galois osserva dapprima che quello che conta nelle permutazioni non è l'ordine nel quale vengono scritti gli elementi, ma la funzione (differenza tra *sostituzioni* e *permutazioni*); poi, sostanzialmente, osserva che $G = Aut_K(L)$ (cosa per noi chiara in virtù della Proposizione 2.43, cf Esercizio 24).

Per costruzione $|G| = \deg(F_1)$, quindi $|G| = [L : K]$. Inoltre (f irriducibile) $n = \deg(f) \mid |G|$ (Esercizio 26).

Questa è la sostanza delle prime sei pagine della memoria (16 pagine in tutto) che non solo risolve un grande problema, ma soprattutto introduce per la prima volta il concetto, fondamentale in tutta la matematica, di gruppo.

Lo stile è molto conciso e le idee rivoluzionarie. Non è sorprendente che i suoi contemporanei non abbiano colto subito l'importanza di questo lavoro.

Finalmente osserviamo come le nozioni moderne di separabilità, campo di spezzamento e soprattutto di estensione normale abbiano un'origine naturale.

—— .. ——

Esercizi.

Esercizio 23 *Sia G un gruppo e $H \subset G$ un sotto insieme. Mostrare che la relazione $xRy \Leftrightarrow xy^{-1} \in H$ è una relazione d'equivalenza se e solo se H è un sotto gruppo di G.*

Esercizio 24 *Si prende la definizione originale di gruppo di Galois: $G = \{\sigma_1, ..., \sigma_m\}$ dove $F_1(X) = (X - \sigma_1(t))...(X - \sigma_m(t))$. Sappiamo che $G \subset Aut_K(L)$ (perché?). Mostrare che $Aut_K(L) = G$ (hint: $L = K(r_1, ..., r_n)$).*

Esercizio 25 *Sia $(G, .)$ un gruppo finito e sia $H \subset G$ un sotto insieme. Si assume $x, y \in H \Rightarrow xy \in H$ e $1 \in H$. Mostrare che H è un sotto gruppo di G.*

É ancora vero questo se G è infinito?

Esercizio 26 *Sia $f(x) \in K[x]$ irriducibile.*

1. *Mostrare che $n := \deg(f) \mid |G|$, dove $G = Gal_K(f)$. Abbiamo quindi: $n \mid |G| \mid n!$.*
2. *Mostrare che G agisce transitivamente su $R = \{r_1, ..., r_n\}$, l'insieme delle radici di f (cioè se r_j, $r_k \in R$, esiste $\sigma \in G$ tale che $\sigma(r_j) = r_k$).*

Esercizio 27 *Determinare tutti i sotto gruppi di S_3 (usare il teorema di Lagrange: se $H \leq G$, allora $|H| \mid |G|$; in particolare l'ordine di ogni elemento divide l'ordine del gruppo).*

Esercizio 28 *Sia $f(x) \in \mathbb{Q}[x]$ un polinomio del terzo grado. Siano r_1, r_2, r_3 le radici di f in Ω.*

1. *Mostrare che i casi possibili sono:*
   (A) r_1, r_2 e r_3 sono razionali
   (B) $r_1 \in \mathbb{Q}$; $r_2, r_3 \in (\mathbb{C} \setminus \mathbb{R})$ (radici complesse coniugate)
   (C) $r_1 \in \mathbb{Q}$; $r_2, r_3 \in \mathbb{R}$, r_2, r_3 irrazionali ($r_i \notin \mathbb{Q}$)
   (D) r_1 irrazionale; $r_2, r_3 \in (\mathbb{C} \setminus \mathbb{R})$ (radici complesse coniugate)
   (E) r_1 irrazionale; $r_2, r_3 \in \mathbb{R}$, r_2, r_3 irrazionali.
2. *Sia $f(x) = x^3 + mx + 1$ con $m \in \mathbb{N}$, $m > 0$. Mostrare che $f(x)$ ha tre radici distinte di cui una radice reale irrazionale e due radici complesse coniugate (caso (D))*
3. *Sia $f(x) = x^3 - mx + 1$, $m \in \mathbb{N}$, $m \geq 3$. Mostrare che $f(x)$ ha tre radici distinte, tutte reali, irrazionali (caso (E)).*
4. *Concludere che ognuno dei cinque casi qui sopra è effettivo.*
5. *Determinare $Gal_{\mathbb{Q}}(f)$ nei casi (A), (B), (C).*
6. *Se f è irriducibile, siamo nel caso (D) o nel caso (E). Mostrare che nel caso (D), $Gal_{\mathbb{Q}}(f) \simeq S_3$ (usare l'Esercizio 27).*

Esercizio 29 *Sia $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_0 \in K[x]$ (K campo di numeri) e siano $r_1, ..., r_n$ le radici di f in Ω. Si pone $L = K(r_1, ..., r_n)$ e $G := Gal(L/K)$.*

Sia $\delta = \prod_{i<j}(r_i - r_j) \in L$.

1. *Se* $\sigma \in S_n$, *si pone* $\sigma(\delta) = \prod_{i<j}(r_{\sigma(i)} - r_{\sigma(j)})$. *Si ricorda (corso di Geometria I) che* $\sigma(\delta) = \varepsilon(\sigma) \cdot \delta$ *dove* $\varepsilon(\sigma)$ *è la segnatura della permutazione* σ. *Mostrare che se* $\delta \in K$, *allora* $G \subset A_n$ *dove* $A_n \leq S_n$ *è il gruppo alterno (sotto gruppo delle permutazioni pari).*
2. *Il* discriminante *di* f *è* $D := \prod_{i<j}(r_i - r_j)^2$, *cioè* $D = \delta^2$. *Mostrare che* $D \in K$.
3. *Se* $\sqrt{D} \notin K$, *allora* $G \nsubseteq A_n$ *e* $[K(\delta) : K] = 2$.

Esercizio 30 *(Il determinante di Vandermonde)*
Sia $\delta(a_1, ..., a_n) = \det A$ *dove:*

$$A = A(a_1, ..., a_n) := \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ \vdots & \vdots & & \vdots \\ a_1^{n-1} & a_2^{n-1} & \cdots & a_n^{n-1} \end{pmatrix}$$

Si tratta di mostrare:

$$\delta(a_1, ..., a_n) = \prod_{1 \leq i < j \leq n} (a_j - a_i) \ \ (*)$$

1. *Se* $f(x) = x^{n-1} + b_{n-2}x^{n-2} + ... + b_0$, *mostrare che:*

$$\delta(a_1, ..., a_n) = \begin{vmatrix} 1 & 1 & \cdots & \cdots & 1 \\ a_1 & a_2 & \cdots & \cdots & a_n \\ \vdots & \vdots & & \vdots & \vdots \\ a_1^{n-2} & a_2^{n-2} & \cdots & \cdots & a_n^{n-2} \\ f(a_1) & f(a_2) & \cdots & \cdots & f(a_n) \end{vmatrix}$$

2. *Dimostrare* $(*)$ *per induzione su* $n \geq 2$ *usando (1) e un* f *opportuno.*
3. *Sia* $f(x) = x^2 + bx + c = (x - r_1)(x - r_2)$. *Da quanto precede il discriminante di* f *è:* $det(A^t A)$ *dove* $A = \begin{pmatrix} 1 & 1 \\ r_1 & r_2 \end{pmatrix}$

Nota: *Mentre Lagrange che, dal nome, sembra francese, è italiano, Vandermonde che sembra olandese, è francese. Vandermonde non ha mai calcolato un determinante di Vandermonde, l'appellativo è dovuto ad un errore di trascrizione. La matrice simmetrica* $A^t A$ *si presta bene per calcolare il discriminante in funzione dei coefficienti, ma i calcoli sono lunghi. Se avete mezz'ora da perdere potete verificare così che il discriminante di* $f(x) = x^3 + px + q$ *vale* $-4p^3 - 27q^2$.

Esercizio 31 *Sia $f(x) \in \mathbb{Q}[x]$ un polinomio irriducibile del terzo grado. Siano r_1, r_2, r_3 le radici di f in Ω. Infine sia D il discriminante di f (cf Esercizio 29).*

1. *Mostrare che $D > 0 \Leftrightarrow r_i \in \mathbb{R}, \forall i$*
2. *Si assume $D > 0$ (caso (E) dell'Esercizio 28). Mostrare che:*
   - $\sqrt{D} \in \mathbb{Q} \Leftrightarrow Gal_{\mathbb{Q}}(f) = A_3$
   - $\sqrt{D} \notin \mathbb{Q} \Leftrightarrow Gal_{\mathbb{Q}}(f) = S_3$.
3. *Dare degli esempi espliciti di polinomi del terzo grado con gruppo di Galois A_3 (risp. S_3) (usare l'Esercizio 28 e la Nota dell'Esercizio 30).*
4. *Osservare che ogni sotto gruppo di S_3 (cf Esercizio 27) è un gruppo di Galois su $\mathbb{Q}$.*

2.5 La corrispondenza di Galois.

Osserviamo che se $K \subset F \subset L$ è una torre di estensioni allora $Gal(L/F) \subset Gal(L/K)$, cioè $Gal(L/F)$ è un sottogruppo di $Gal(L/K)$. Quindi ad un *campo intermedio*, F, corrisponde un sottogruppo di $G := Gal(L/K)$.

Se $H \subset G = Gal(L/K)$, possiamo considerare il campo fisso $L^H := \{z \in L \,|\, \sigma(z) = z, \forall \sigma \in H\}$. Abbiamo $K \subset L^H$ perché ogni $\sigma \in H$ è un K-automorfismo e lascia fisso K. Quindi ad ogni sottogruppo di G, H, corrisponde un campo intermedio ($K \subset L^H \subset L$).

Indichiamo con $\mathcal{G}$ l'insieme dei sottogruppi di $Gal(L/K)$ e con $\mathcal{F}$ l'insieme dei campi intermedi:

$$\boxed{\begin{array}{l} \mathcal{G} = \{H \,|\, H \subset G := Gal(L/K), H \text{ sottogruppo } \} \\ \mathcal{F} = \{F \,|\, K \subset F \subset L, F \text{ sottocampo di } L\} \end{array}}$$

Definiamo:

$$f : \mathcal{G} \to \mathcal{F} : H \to L^H$$

$$g : \mathcal{F} \to \mathcal{G} : F \to Gal(L/F)$$

Scopo di quanto segue è di mostrare che <u>se L/K è normale</u>, allora f è biiettiva con $f^{-1} = g$, quindi in questo caso esiste una corrispondenza perfetta tra i sottogruppi di $Gal(L/K)$ e i campi intermedi tra K e L; inoltre in questa corrispondenza sottogruppi normali corrispondono ad estensioni F/K normali.

Abbiamo bisogno del seguente:

Lemma 2.45. (E. Artin.)
Sia L un campo e G un sottogruppo finito di $Aut(L)$. Sia $F \subset L$ il sotto campo $F = L^G$. Allora $dim_F(L) = |G|$.

Dimostrazione. Sia $G = \{\sigma_1, ..., \sigma_n\}$. Per $\alpha \in L$ sia $P_\alpha(x) = \prod_1^n (x - \sigma_i(\alpha))$. I coefficienti, a_i, di P_α sono le funzioni simmetriche elementari delle radici: $a_i = e_i(\sigma_1(\alpha), ..., \sigma_n(\alpha))$. Abbiamo $\sigma_k[e_i(\sigma_1(\alpha), ..., \sigma_n(\alpha))] = e_i(\sigma_1(\alpha), ..., \sigma_n(\alpha))$ perché σ_k permuta le variabili e e_i è simmetrico. Quindi $\sigma_k(a_i) = a_i, \forall k$ e $a_i \in F = L^G$, cioè $P_\alpha(x) \in F[x]$.

Questo mostra che *ogni* $\alpha \in L$ è algebrico su F con $[F(\alpha) : F] \leq n$.

Per mostrare che $[L : F] \leq n$ basta mostrare che ogni volta che si prendono $n + 1$ vettori $\alpha_1, ..., \alpha_{n+1}$ in L, questi sono dipendenti su F.

Consideriamo $F(\alpha_1, ..., \alpha_{n+1})/F$. L'estensione è algebrica finita perché ogni α_i è algebrico su F (aggiungendo un numero finito di elementi algebrici si ottiene un'estensione finita: induzione su n). Per il teorema dell'elemento primitivo: $F(\alpha_1, ..., \alpha_{n+1}) = F(\beta)$. Da quanto precede: $[F(\beta) : F] \leq n$. Quindi $[F(\alpha_1, ..., \alpha_n) : F] \leq n$ e pertanto $\alpha_1, ..., \alpha_{n+1}$ sono dipendenti su F.

Segue che $[L : F] \leq n$.

D'altra parte dalla Formula (2.2), $dim_F(L) \geq |Aut_F(L)|$. È chiaro che $G \subset Aut_F(L)$, quindi $dim_F(L) \geq |G| = n$. Concludiamo che $dim_F(L) = n$.

□

Possiamo dimostrare la prima parte della corrispondenza di Galois:

Teorema 2.46. *Sia L/K un'estensione finita, normale.*
L'applicazione $f : \mathcal{G} \to \mathcal{F} : H \to L^H$ è biiettiva con

$$f^{-1} = g : \mathcal{F} \to \mathcal{G} : F \to Gal(L/F).$$

Inoltre se F è un campo intermedio: $dim_K(F) = \frac{|Gal(L/K)|}{|Gal(L/F)|}$.

Dimostrazione. Abbiamo $(g \circ f)(H) = Gal(L/L^H)$. Per il Lemma 2.45: $dim_{L^H}(L) = |H|$. D'altra parte, siccome L/L^H è normale (cf Lemma 2.36): $dim_{L^H}(L) = |Gal(L/L^H)|$ (Corollario 2.26). Abbiamo $Gal(L/L^H) = Aut_{L^H}(L) = \{\varphi \in Aut(L) \,|\, \varphi_{|L^H} = Id\}$ e $L^H = \{z \in L \,|\, \sigma(z) = z, \forall \sigma \in H\}$. Quindi se $\sigma \in H$ e $z \in L^H$, $\sigma(z) = z$ cioè $\sigma_{|L^H} = Id$, ossia $\sigma \in Gal(L/L^H)$. In conclusione $H \subset Gal(L/L^H)$, $|H| = |Gal(L/L^H)| = dim_{L^H}(L)$, pertanto $(g \circ f)(H) = H$.

Se F è un campo intermedio $(f \circ g)(F) = L^H$ dove $H := Gal(L/F)$. Siccome L/F è normale (Lemma 2.36): $L^H = F$ (Proposizione 2.28), ossia $(f \circ g)(F) = F$.

Se $K \subset F \subset L$, allora $dim_K(L) = dim_F(L).dim_K(F)$. Abbiamo $dim_K(L) = |Gal(L/K)|$, $dim_F(L) = |Gal(L/F)|$ (L/K e L/F sono normali).

Quindi: $dim_K(F) = \frac{|Gal(L/K)|}{|Gal(L/F)|}$. □

Osservazione 2.47. Siccome $Gal(L/K)$ è finito ($|Gal(L/K)| = dim_K(L)$), il Teorema 2.46 mostra che i campi intermedi tra K e L sono in numero finito.

Abbiamo già visto che data una torre $K \subset F \subset L$, con L/K normale, allora L/F è normale, ma F/K non è necessariamente normale (cf Lemma 2.36). É lecito aspettarsi che i campi intermedi F tali che F/K sia normale corrispondano a sottogruppi *particolari* nella corrispondenza di Galois, in effetti è proprio così:

Definizione 2.48. *Sia G un gruppo finito e $H \leq G$ un sotto gruppo. Il sotto gruppo H è* normale *($H \lhd G$) se: $\forall x \in G : xHx^{-1} = H$ (cioè H è invariante sotto gli automorfismi* interni *di G).*

Osservazione 2.49.

1. Si vede facilmente che $H \leq G$ è normale se e solo se l'insieme quoziente (nella relazione $xRy \Leftrightarrow xy^{-1} \in H$) G/H è un gruppo. Segue quindi un'altra caratterizzazione: $H \leq G$ è normale se e solo se $H = Ker(f)$ per un qualche morfismo di gruppi $f : G \to T$ (cf Esercizio 32).

2. Si osserverà come la terminologia sia naturale. Vedremo più avanti come questa nozione si introduce naturalmente nel problema della risoluzione per radicali delle equazioni algebriche.

Detto questo abbiamo:

Teorema 2.50. *Nella corrispondenza del Teorema 2.46 estensioni normali F/K corrispondono a sottogruppi normali $H \lhd G := Gal(L/K)$ (cioè $H \lhd G$ se e solo se L^H/K è normale).*

Inoltre se F/K è normale: $Gal(F/K) \simeq Gal(L/K)/Gal(L/F)$.

Dimostrazione. Sia $K \subset F \subset L$ con F/K normale.

Sia $\varphi : Gal(L/K) \to Gal(F/K) : \sigma \to \sigma_{|F}$. L'applicazione è ben definita, infatti l'immagine di $\sigma|F : F \to L$ è contenuta in F perché $\sigma_{|F}$ è un K-morfismo e F/K è normale.

Si verifica facilmente che φ è un morfismo di gruppi.

(a) Mostriamo che φ è suriettivo.

Sia $\tau \in Gal(F/K)$. Per il Lemma 2.29 τ si estende in un K-morfismo: $\tilde{\tau} : L \to \Omega$. Siccome L/K è normale, $\tilde{\tau}(L) = L$, cioè $\tilde{\tau} \in Gal(L/K)$. Chiaramente $\tilde{\tau}_{|F} = \tau$.

(b) Abbiamo $Ker(\varphi) = \{\sigma \in Gal(L/K) \,|\, \sigma_{|F} = Id\}$, cioè $Ker(\varphi) = Gal(L/F)$. Essendo il Ker di un morfismo, $Gal(L/F)$ è un sotto gruppo normale di $Gal(L/K)$ (cf Osservazione 2.49). Abbiamo sempre $Gal(L/K)/Ker(\varphi) \simeq Im(\varphi)$, da quanto precede:

$$Gal(L/K)/Gal(L/F) \simeq Gal(F/K).$$

Viceversa sia $H \lhd Gal(L/K)$ un sottogruppo normale.

Se $F = L^H$ sappiamo dal Teorema 2.46 che $Gal(L/F) = H$. Sia $F = K(u)$ e sia $M(X) \in K[X]$ il polinomio minimo di u su K. Sia b una radice di $M(X)$. Siccome L/K è normale, $b \in L$ (Lemma 2.30). Sia $\sigma : F = K(u) \to K(b) \subset L$, il K-morfismo definito da $\sigma(u) = b$. Per il Lemma 2.29 esiste $\tilde{\sigma} : L \to L$ che estende σ. Siccome $Gal(L/F)$ è un sotto gruppo normale di $Gal(L/K)$, per ogni $\rho \in Gal(L/F)$, $\tilde{\sigma}^{-1}\rho\tilde{\sigma} \in Gal(L/F)$. Quindi $\tilde{\sigma}^{-1}\rho\tilde{\sigma}(u) = u$ (perché $u \in F$), cioè: $\rho\tilde{\sigma}(u) = \tilde{\sigma}(u)$, $\forall \rho \in Gal(L/F)$. Ossia $\rho(b) = b, \forall \rho \in Gal(L/F)$. Pertanto $b \in F$. Quindi il polinomio minimo di u su K ha tutte le sue radici in F e F/K è normale (Lemma 2.30). □

Possiamo raccogliere i due teoremi in un unico enunciato:

Teorema 2.51. (Corrispondenza di Galois.)
Sia L/K un'estensione finita, <u>normale</u>.

Esiste una corrispondenza biunivoca tra sottogruppi di $Gal(L/K)$ e campi intermedi F ($K \subset F \subset L$) data nel modo seguente: siano $\mathcal{G}$ l'insieme dei sottogruppi di $Gal(L/K)$, $\mathcal{F}$ l'insieme dei campi intermedi, allora l'applicazione:

$$f : \mathcal{G} \to \mathcal{F} : H \to L^H$$

è biiettiva e

$$f^{-1} = g : \mathcal{F} \to \mathcal{G} : F \to Gal(L/F)$$

Se F è un campo intermedio: $dim_K(F) = \frac{|Gal(L/K)|}{|Gal(L/F)|}$.

Inoltre sotto gruppi normali corrispondono ad estensioni normali e viceversa (cioè: $H \lhd Gal(L/K) \Leftrightarrow L^H = F/K$ è normale).

Se F/K è normale, $Gal(F/K) \simeq Gal(L/K)/Gal(L/F)$.

Osservazione 2.52. In particolare se $K \subset F \subset L$ è una torre di estensioni con L/K e F/K normali (quindi anche L/F è normale), allora $Gal(L/F) \lhd Gal(L/K)$ e $Gal(F/K) \simeq Gal(L/K)/Gal(L/F)$.

Inoltre se $\sigma \in Gal(F/K)$, $\exists \tilde{\sigma} \in Gal(L/K)$ tale che $\tilde{\sigma}_{|F} = \sigma$.

Se $\tau \in Gal(L/K)$, allora $\tau_{|F} \in Gal(F/K)$.

—— .. ——

Esercizi.

Esercizio 32 *Sia G un gruppo finito e $H \leq G$ un sottogruppo. Le affermazioni seguenti sono equivalenti:*

1. $H \lhd G$
2. *La legge di gruppo passa al quoziente modulo H, i.e. l'insieme quoziente G/H (per la relazione $xRy \Leftrightarrow xy^{-1} \in H$) è un gruppo*
3. $H = Ker(f)$ *per un qualche morfismo di gruppi $f : G \to T$.*

In particolare se G è abeliano, ogni sotto gruppo è normale.

Esercizio 33 *Mostrare che A_n, il sotto gruppo delle permutazioni pari, è un sottogruppo normale di S_n ($A_n \lhd S_n$).*

Determinare tutti i sotto gruppi normali di S_3 (cf Esercizio 27).

Esercizio 34 *Sia G un gruppo e H, K due sotto gruppi di G. In generale $H \cup K$ non è un sotto gruppo di G. Si nota $H \vee K$ il sotto gruppo di G generato da H e K, cioè $H \vee K$ è l'intersezione di tutti i sotto gruppi di G contenenti $H \cup K$.*

1. *Mostrare che $H \vee K = \{h_1 g_1 h_2 g_2 ... h_n g_n \mid h_i \in H, g_i \in K\}$*
2. *Se $\forall h \in H, \forall g \in K$, $hg = gh$, allora $H \vee K = HK$ dove $HG = \{hg \mid h \in H, g \in K\}$*
3. *Se $H \lhd G$, $K \lhd G$ e $H \cap K = \{1\}$, allora $H \vee K = HK$.*

Esercizio 35 *Sia K un'estensione finita di $\mathbb{Q}$ e sia L/K un'estensione normale. Siano E_1, E_2 due campi intermedi ($K \subset E_i \subset L$, $1 \leq i \leq 2$). Si pone $H_i = Gal(L/E_i)$.*

Mostrare che: $Gal(L/E_1 \cap E_2) = H_1 \vee H_2$ e $Gal(L/E_1 \vee E_2) = H_1 \cap H_2$ (vedere Esercizio 34 per la definizione di $H_1 \vee H_2$; $E_1 \vee E_2 = E_1(E_2)$ è il più piccolo sotto campo di L contenente $E_1 \cup E_2$).

Esercizio 36 *Sia G un gruppo e siano H, K due sotto gruppi di G. Si dice che G è il prodotto diretto (interno) di H con K ($G \simeq H \times K$) se l'applicazione:*

$$f : H \times K \to G : (h, g) \to hg$$

è un isomorfismo di gruppi.

Mostrare che $G \simeq H \times K$ se e solo se le tre condizioni seguenti sono verificate: (a) $HK = G$ (b) $H \cap K = \{1\}$ (c) $H \lhd G$ e $K \lhd G$.

Esercizio 37 *Sia K un'estensione finita di $\mathbb{Q}$ e sia L/K un'estensione normale. Siano E_1, E_2 due campi intermedi ($K \subset E_i \subset L$, $1 \leq i \leq 2$).*

1. *Si suppone E_i/K normale ($1 \leq i \leq 2$), $E_1 \vee E_2 = L$ e $E_1 \cap E_2 = K$. In queste condizioni mostrare che:*

$$Gal(L/K) \simeq Gal(L/E_1) \times Gal(L/E_2)$$

(Usare l'Esercizio 35.)

2. *Viceversa se* $Gal(L/K) \simeq H \times K$, *siano* $E_1 = L^H$, $E_2 = L^K$. *Mostrare che* $E_1 \vee E_2 = L$, $E_1 \cap E_2 = K$.
3. *Nelle condizioni di (1) mostrare che:*

$$Gal(L/K) \simeq Gal(E_1/K) \times Gal(E_2/K)$$

4. *Siano* $f(x), g(x) \in \mathbb{Q}[x]$ *due polinomi irriducibili, senza radici comuni in* Ω, *è vero che* $Gal_{\mathbb{Q}}(fg) \simeq Gal_{\mathbb{Q}}(f) \times Gal_{\mathbb{Q}}(g)$*?*

Esercizio 38 *Sia* $f(x) \in \mathbb{Q}[x]$ *un polinomio irriducibile e sia* $L = \mathbb{Q}(r_1, ..., r_n)$ *il suo campo di spezzamento su* $\mathbb{Q}$. *Mostrare che se* $Gal(L/\mathbb{Q})$ *è abeliano, allora, per ogni i:* $L = \mathbb{Q}(r_i)$ *(cioè ogni radice di* f *è un elemento primitivo).*

Esercizio 39 *Sia* $f(x) \in \mathbb{Q}[x]$ *un polinomio irriducibile e sia* L *il suo campo di spezzamento su* $\mathbb{Q}$. *Mostrare che se* $[L : \mathbb{Q}]$ *è dispari, allora tutte le radici di* f *in* Ω *sono reali.*

Esercizio 40 *Sia* $f(x) = x^3 + x + 1 \in \mathbb{Q}[x]$ *e sia* L *il campo di spezzamento di* f *su* $\mathbb{Q}$. *Determinare* $Gal(L/\mathbb{Q})$ *e tutti i campi intermedi* $\mathbb{Q} \subset F \subset L$. *Per ogni campo intermedio,* F, *di grado due (cioè con* $[F : \mathbb{Q}] = 2$*), determinare un elemento primitivo di* F.

Esercizio 41 *Sia* $f(x) \in \mathbb{Q}[x]$ *un polinomio irriducibile di grado* n. *Mostrare che ci sono al più* $2^{n!-1}$ *campi intermedi,* K, $\mathbb{Q} \subset K \subset L$, *dove* L *è il campo di spezzamento di* f *su* $\mathbb{Q}$.

3

Risolubilità per radicali delle equazioni algebriche.

3.1 La strategia di Galois.

Sia $f(x) \in K[x]$ dove K è un'estensione finita di $\mathbb{Q}$. Il gruppo di Galois di f è $Gal(L/K)$, dove $L = K(r_1, ..., r_n)$ ($r_1, ..., r_n$ sono tutte le radici di f in Ω).

Lo scopo di Galois era di dare delle condizioni sul gruppo di Galois, G, di $f(x) \in K[x]$ affinché l'equazione $f(x) = 0$ fosse risolubile per radicali. Cerchiamo di seguire, nella sua terminologia (molto moderna per la sua epoca) il suo ragionamento.

L'equazione è risolubile per radicali se <u>tutte</u> le sue radici possono essere espresse in termini di *quantità note* tramite le quattro operazioni ($\pm, \times, \div$) o estrazioni di radici.

Per estrarre una radice n-esima di a, se $n = pq$ possiamo prima estrarre una radice p-esima, $a^{\frac{1}{p}}$ e poi una radice q-esima di $a^{1/p}$: $(a^{1/p})^{1/q} = a^{1/pq} = a^{1/n}$. Possiamo quindi limitarci a considerare estrazioni p-esime dove p è un numero primo.

A questo punto è conveniente assumere che tutte le radici p-esime dell'unità che ci servono sono *quantità note*. Questo perché se α è una radice p-esima dell'unità ($\alpha \neq 1$) e se $z^p = a$ allora le p radici p-esime di a sono: $\alpha z, \alpha^2 z, ..., \alpha^p z = z$. Quindi se K contiene α, $K(z)$ contiene <u>tutte</u> le radici di $X^p - a$ (e quindi l'estensione $K(z)/K$ è *normale*). Quindi se partiamo con $f(x) \in \mathbb{Q}[x]$ e se nella risoluzione abbiamo usato delle estrazioni di radici p_i-esime, $1 \leq i \leq t$, allora $K = \mathbb{Q}(\alpha_1, ..., \alpha_t)$ (α_i radice p_i-esima dell'unità) sarà il campo delle *quantità note*. Galois glissa su questo punto, per lui, le radici primitive dell'unità erano considerate quantità note senza alcun commento. Questo è forse dovuto al fatto che Gauss aveva già mostrato che le radici p-esime dell'unità si potevano calcolare (risolvere) per radicali. Per chi (come noi) vuole mantenere $\mathbb{Q}$ come campo base (cioè $K = \mathbb{Q}$ con le notazioni precedenti), questo comporta una complicazione tecnica.

Finché usiamo le quattro operazioni rimaniamo in K (è la definizione di campo!). Se nel corso della risoluzione dobbiamo prendere la radice p-esima

di un elemento $a \in K$ è molto probabile che dobbiamo uscire da K (in generale K non conterrà nessuna radice p-esima di a). Sia $z \in \Omega$ tale che $z^p = a$. Per proseguire la risoluzione della nostra equazione, dobbiamo *aggiungere* (l'espressione è di Galois) z alle quantità note. Cioè dobbiamo estendere il campo K al campo $K(z)$. Le *quantità note* sono adesso gli elementi di $K_1 := K(z)$. Rimaniamo in K_1 finché la risoluzione dell'equazione non richiede l'estrazione di una radice p_2-esima di un elemento $a_1 \in K_1$ (e K_1 non contiene nessuna radice p_2-esima di a_1). Allora (assumendo ancora che K_1 contenga una radice primitiva p_2-esima dell'unità), aggiungiamo una tale radice alle quantità note: $K_2 = K_1(z_1)$ ($z_1^{p_2} = a_1$). Abbiamo: $K \subset K_1 \subset K_2$, dove ogni estensione K_i/K_{i-1} è una p_i-estensione pura, cioè $K_i = K_{i-1}(z_i)$, con $z_i^{p_i} \in K_{i-1}$ (e dove K_{i-1} contiene $\alpha \neq 1$ con $\alpha^{p_i} = 1$).

Si procede così $K = K_0 \subset K_1 \subset K_2 ... \subset K_t$ finché le radici $r_1, ..., r_n$ di f non siano diventate *quantità note*; cioè finché $r_i \in K_t, \forall i$. Cioè finché $L = K(r_1, ..., r_n) \subset K_t$. In conclusione se l'equazione $f(x) = 0$ è risolubile per radicali, esiste una successione di campi:

$$K = K_0 \subset K_1 \subset K_2 \subset ... \subset K_t$$

con $K(r_1, ..., r_n) \subset K_t$, dove per ogni i, K_i/K_{i-1} è una p_i-estensione pura (e dove K_{i-1} contiene una radice primitiva p_i-esima dell'unità).

Detto ciò guardiamo G, il gruppo di Galois di f. Se il campo K viene esteso, il gruppo di Galois o rimane uguale a G o si riduce a un sottogruppo di G . Quindi mentre il campo viene esteso: $K \subset K_1 \subset ... \subset K_t$, il gruppo decresce: $G \supset G_1 \supset ... \supset G_t$. Alla fine $r_i \in K_t, \forall i$, quindi il gruppo di Galois su K_t è $\{Id\}$. Infatti un elemento del gruppo $\tilde{\sigma}$ è indotto da una permutazione σ delle radici, ma siccome $\tilde{\sigma}_{|K_t} = Id$ e $r_i \in K_t$, $\sigma(r_i) = r_i, \forall i$, cioè $\tilde{\sigma} = Id$.

Rimane quindi da vedere come cambia il gruppo quando si fa una p-estensione pura. Vedremo (cf Proposizione 3.4) che il nuovo gruppo, G', è un sottogruppo *normale* di G di indice p ($G/G' \simeq \mu_p$).

In conclusione (sotto opportune ipotesi sull'esistenza di radici primitive p-esime dell'unità in K): se $f(x) = 0$ è risolubile per radicali esiste una successione di sottogruppi di G:

$$\{Id\} \subset G_k \subset ... \subset G_1 \subset G_0 = G$$

tali che $G_i \lhd G_{i-1}$ (dove $\lhd$ significa è un sottogruppo *normale*) di indice un numero primo.

In queste condizioni si dice (terminologia introdotta da E. Artin) che il gruppo G è *risolubile*. Quindi se $f(x) = 0$ è risolubile per radicali, il suo gruppo di Galois è un gruppo risolubile.

Abbiamo quindi una condizione necessaria affinché un'equazione sia risolubile per radicali. A questo punto basta trovare un'equazione del quinto grado con gruppo di Galois non risolubile per ritrovare il teorema di Abel.

Galois mostra poi il viceversa: se G è un gruppo risolubile, allora l'equazione $f(x) = 0$ è risolubile per radicali. L'idea di base è la seguente: grazie

alla corrispondenza ci possiamo limitare alla seguente situazione: L/K è normale e $\#(Gal(L/K) = p$ (p primo), K contiene una radice primitiva p-esima dell'unità.

Si tratta di mostrare che L/K è p-pura cioè che esiste $\beta \in L$ tale che $L = K(\beta)$ e $\beta^p \in K$ (cioè se $a = \beta^p$, $L = K(a^{1/p})$ è ottenuta tramite l'estrazione di una radice p-esima di un elemento di K).

Il gruppo di Galois è ciclico di ordine p: $Gal(L/K) = \{\sigma, \sigma^2, ..., \sigma^p = Id\}$; anche il gruppo delle radici p-esime dell'unità è ciclico: $\mu_p = \{\alpha, \alpha^2, ..., \alpha^p = 1\}$. Se $x \in L$ verifica $\sigma(x) = x/\alpha$, allora siamo a posto. Intanto $x \notin K$ perché $\sigma(x) \neq x$ quindi $x \notin L^G = K$; segue che x è primitivo ($[L : K] = p$). Poi $\sigma(x^p) = (\sigma(x))^p = x^p/\alpha^p = x^p$. Questo implica $\sigma^i(x^p) = x^p, \forall i$, quindi $x^p \in L^G = K$ e si può prendere $\beta = x$.

Per trovare un tale x, rispolverando la risolvente di Lagrange, lo si cerca sotto la forma $x = v+\alpha\sigma(v)+\alpha^2\sigma^2(v)+...+\alpha^{p-1}\sigma^{p-1}(v)$, dove v è un elemento primitivo qualsiasi (cf Proposizione 3.25 e anche Esercizio 43, Esercizio 47 per delle dimostrazioni alternative).

Vediamo adesso tutto questo in dettaglio.

—— .. ——

3.2 Estensioni cicliche, p-pure.

Passiamo ora a studiare le p-estensioni pure.

Lemma 3.1. *Sia K un sottocampo di Ω. Sia $a \in K$ tale che K non contenga nessuna radice p-esima di a (p un numero primo). Allora $P(X) := X^p - a$ è irriducibile in $K[X]$.*

Dimostrazione. (a) Iniziamo col mostrare che per ogni t, $1 \leq t \leq p-1$, a^t non è una potenza p-esima in K (cioè K non contiene nessuna radica p-esima di a^t). Siccome p è primo t e p sono primi tra di loro, quindi esistono degli interi tali che: $mt + rp = 1$. Abbiamo: $a = a^{mt+rp} = (a^t)^m.(a^r)^p$. Se $a^t = b^p, b \in K$, allora: $a = (b^p)^m.(a^r)^p = (b^m.a^r)^p$, ma questo contraddice l'ipotesi che K non contiene alcuna radice p-esima di a.
(b) Supponiamo $P(X) = A(X).B(X)$ in $K[X]$. Sia v una radice p-esima di a in Ω. Se α è una radice p-esima dell'unità ($\alpha \neq 1$), le p radici p-esime di a sono: $\alpha v, \alpha^2 v, ..., \alpha^p v = v$, cioè: $P(X) = \prod_{1 \leq i \leq p} (X - \alpha^i v)$ in $\Omega[X]$. Questo implica che in $\Omega[X]$: $A(X) = \prod_{i \in T}(X - \alpha^i v)$ e $B(X) = \prod_{i \in S}(X - \alpha^i v)$, dove T, S sono due sotto insiemi di $I := \{1, ..., p\}$ tali che $T \cup S = I$, $T \cap S = \emptyset$. Il termine costante, b, di A è: $b = [\prod_{i \in T}(\alpha^i)](-1)^t v^t$ dove $t = card(T)$. Prendendo la potenza p-esima: $b^p = ((-1)^t v^t)^p$. Siccome $v^p = a$, viene: $a^t = ((-1)^t b)^p$. Siccome $b \in K$, (a) implica $t = 0$ (cioè $A(X)$ è una costante) o $t = p$ (in questo caso $B(X)$ è una costante). □

Corollario 3.2. *Sia K un sotto campo di Ω contenente una radice primitiva p-esima dell'unità. Sia $a \in K$ tale che K non contenga alcuna radice p-esima di a. Se $v \in \Omega$ è una radice p-esima di a, l'estensione $K(v)/K$ è normale.*

Dimostrazione. Per il Lemma 3.1, $P(X) = X^p - a$ è irriducibile in $K[X]$. Quindi $P(X)$ è il polinomio minimo di v su K. Siccome K contiene una radice primitiva p-esima dell'unità, tutte le radici di $P(X)$ sono in $K(v)$, quindi (Corollario 2.2.26) $K(v)/K$ è normale. □

Abbiamo quindi mostrato che la p-estensione pura: $K(a^{1/p})/K$ è normale se K contiene una radice primitiva p-esima dell'unità.

Lemma 3.3. *Con le notazioni e ipotesi del Corollario 3.2, $Gal(K(v)/K) \simeq \mu_p$ dove μ_p è il gruppo moltiplicativo delle radici p-esime dell'unità (gruppo ciclico di ordine p).*

Dimostrazione. Siccome il polinomio minimo di v su K è $X^p - a$ (dimostrazione del Corollario 3.2), $p = dim_K(K(v)) = |Gal(K(v)/K)|$ (l'estensione è normale, Corollario 2.2.26). Ogni gruppo, G, di ordine p è ciclico (se $x \in G$, $x \neq 1$, per il teorema di Lagrange, l'ordine del sottogruppo $\langle x \rangle = \{x^i\}$ divide p, siccome $\langle x \rangle \neq \{1\}$, $\langle x \rangle = G$) e isomorfo a μ_p. □

Finalmente abbiamo:

Proposizione 3.4. *Sia $f(x) \in \mathbb{Q}[x]$ irriducibile con radici (in Ω) $r_1, ..., r_n$. Sia K un'estensione algebrica finita di $\mathbb{Q}$ contenente una radice primitiva p-esima dell'unità (p un numero primo). Sia $a \in K$ tale che K non contenga alcuna radice p-esima di a. Sia v una radice p-esima di a in Ω tale che:*

$$K \subset K(v) \subset L = K(r_1, ..., r_n)$$

Allora $Gal(L/K(v))$ è un sottogruppo normale di indice p di $Gal(L/K)$.

Dimostrazione. Tutte le estensioni L/K, $L/K(v)$, $K(v)/K$ sono normali. Per le prime due questo segue da 2.2.52, per l'ultima dal Corollario 3.2. Si conclude con 2.2.52. □

Abbiamo mostrato che se K contiene una radice primitiva p-esima dell'unità, l'aggiunzione di una radice p-esima di un elemento di K, riduce il gruppo di Galois, G, a un sottogruppo, G', tale che G' sia un sottogruppo normale di G, di indice p: abbiamo praticamente finito; abbiamo recuperato l'essenza del ragionamento di Galois. Rimangono però alcuni problemi tecnici: intanto vorremo liberarci da quella condizione che K contenga tutte le radici primitive dell'unità *che ci servono*. In definitiva vorremo un criterio applicabile ad un polinomio $f(x) \in \mathbb{Q}[x]$. Serve ancora un pò di lavoro (tecnico, perché le idee principali ci sono già tutte) per avere un criterio pulito di risoluzione per radicali di un'equazione $f(x) = 0$ con $f(x) \in \mathbb{Q}[x]$.

—— .. ——

Esercizi.

Esercizio 42 *Sia K un'estensione finita di $\mathbb{Q}$ contenente le radici n-esime dell'unità (n non necessariamente primo). Sia $a \in K$ tale che K non contenga alcuna radice n-esima di a. Finalmente sia $v \in \Omega$ tale che $v^n = a$.*

1. *Mostrare che $K(v)/K$ è normale*
2. *Sia $G := Gal(K(v)/K)$. Se $\sigma \in G$, mostrare che $\sigma(v).v^{-1} \in \mu_n$ (μ_n è il gruppo delle radici n-esime dell'unità).*
3. *Mostrare che $f : G \to \mu_n : \sigma \to \sigma(v).v^{-1}$ è un morfismo iniettivo di gruppi.*
4. *Concludere che G è ciclico (cf con il Lemma 3.3).*

Esercizio 43 *Sia K un'estensione finita di $\mathbb{Q}$. L'estensione L/K è detta* ciclica *(risp.* abeliana*) se L/K è normale e se $G := Gal(L/K)$ è ciclico (risp. abeliano).*

Sia L/K un'estensione ciclica di ordine n (cioè $[L : K] = n$). Sia $G = \langle\sigma\rangle$. Si suppone che K contenga una radice primitiva n-esima dell'unità. Si considera $\sigma : L \to L$ come un K-endomorfismo del K-spazio vettoriale L.

1. *Mostrare che ogni autovalore di σ è una radice n-esima dell'unità. Mostrare che 1 è autovalore*
2. *Mostrare che gli autovalori di σ sono precisamente le radici n-esime dell'unità. Concludere che σ è diagonalizzabile.*
3. *Mostrare che esiste $b \in L$ tale che $b^n \in K$ e $L = K(b)$. (Hint: considerare un autovettore associato a α, radice primitiva n-esima dell'unità.)*

Esercizio 44 *Sia L/K un'estensione finita. Per $\alpha \in L$ si nota m_α il K-endomorfismo: $m_\alpha : L \to L : z \to \alpha.z$. Si pone poi:*

$$Tr_{L/K}(\alpha) = Tr(m_\alpha)\,,\ N_{L/K}(\alpha) = \det(m_\alpha)$$

Si assume L/K separabile e si nota $Mor_K(L)$ l'insieme delle K-immersioni di L in $\overline{K}$ (se K è un'estensione finita di $\mathbb{Q}$ si può prendere Ω al posto di $\overline{K}$).

1. *Sia $P_\alpha(X)$ il polinomio caratteristico dell'endomorfismo m_α. Mostrare che:*
$$P_\alpha(X) = \prod_{\sigma \in Mor_K(L)} (X - \sigma(\alpha))$$
(cf Esercizio 22)
2. *Mostrare che*
$$Tr_{L/K}(\alpha) = \sum_{\sigma \in Mor_K(L)} \sigma(\alpha)$$
e
$$N_{L/K}(\alpha) = \prod_{\sigma \in Mor_K(L)} \sigma(\alpha)$$

3. *Mostrare che* $Tr_{L/K}(\alpha) \in K, N_{L/K}(\alpha) \in K$. *Inoltre* $Tr_{L/K}(\alpha+\beta) = Tr_{L/K}(\alpha) + Tr_{L/K}(\beta)$; $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha).N_{L/K}(\beta)$.

Esercizio 45 (Lemma di Artin sull'indipendenza dei caratteri.)
Sia G un gruppo e K un campo. Un carattere di G a valori in K è un morfismo di gruppi: $\chi : G \to K^*$ (K^* gruppo moltiplicativo di K). Un carattere è un elemento di $\mathcal{A}(G,K)$, il K-spazio vettoriale delle applicazioni di G in K.

Si tratta di mostrare che se $\chi_1, ..., \chi_r$ sono dei caratteri distinti, allora $\chi_1, ..., \chi_r$ sono indipendenti in $\mathcal{A}(G,K)$.

1. *Sia $n = min\{k \mid$esistono k caratteri dipendenti$\}$. Quindi $\sum_{i=1}^{n} \lambda_i\chi_i = 0$ per dei caratteri $\chi_1, ..., \chi_n$ di G a valori in K; $\lambda_i \in K$ non tutti nulli. Osservare che $n > 1$ e $\lambda_i \neq 0, \forall i$.*
2. *Mostrare che esiste $x \in G$ tale che: $\chi_1(x) \neq \chi_2(x)$ e $\sum_{i=1}^{n} \lambda_i\chi_i(y)\chi_1(x) = 0$, $\forall y \in G$*
3. *Ottenere un assurdo e concludere che se $\chi_1, ..., \chi_r$ sono dei caratteri di G a valori in K, allora $\forall(\lambda_1, ..., \lambda_r) \in K^r$: $\sum \lambda_i\chi_i = 0 \Leftrightarrow \lambda_i = 0, \forall i$.*

Esercizio 46 (Il teorema 90 di Hilbert.)
Sia L/K un'estensione finita normale. Ogni $\sigma \in G := Gal(L/K)$ induce un carattere del gruppo L^* a valori in $\overline{K}$ (o Ω se K è un campo di numeri). Segue che gli elementi di G sono liberi in $End_K(L)$ (cf Esercizio 45).

Sia adesso L/K un'estensione ciclica di grado n con $G = Gal(L/K)$. Si pone $G = \langle\sigma\rangle$.

1. *Mostrare che se $z \in L$, verifica $z = y/\sigma(y)$ per un qualche $y \in L$, allora $N_{L/K}(z) = 1$. (Usare l'Esercizio 44.)*
2. *Sia $z \in L$ tale che $N_{L/K}(z) = 1$. Sia f la seguente combinazione lineare (a coefficienti in L) dei K-automorfismi σ^i:*

$$f = Id + z.\sigma + (z\sigma(z))\sigma^2 + ... + (z\sigma(z)...\sigma^{n-2}(z))\sigma^{n-1}$$

   Mostrare che esiste $y \in L$ tale che $f(y) = x \neq 0$. Mostrare che $z = x/\sigma(x)$.
3. *Concludere che: $N_{L/K}(z) = 1 \Leftrightarrow z = x/\sigma(x)$ (Teorema 90).*

Nota: *Nel 1893 la Deutsche Mathematiker-Vereinigung (D.M.V. l'unione matematica tedesca) commissionò a Hilbert e Minkowski un rapporto sullo stato dell'arte in teoria dei numeri. Minkowski doveva occuparsi della teoria elementare dei numeri, Hilbert del resto. Solo il rapporto di Hilbert fu portato a termine, scritto e pubblicato nel 1897 sotto il titolo* Die Theorie der algebraischen Zahlkörper *([13]), noto come il* Zahlbericht. *Hilbert colse l'occasione per rivedere e rifondare la teoria algebrica dei numeri. Questo rapporto rimase per circa trenta anni la referenza assoluta in teoria algebrica dei numeri; E. Artin, H. Hasse, E. Hecke e molti altri hanno studiato su quel libro. Una particolarità di questo rapporto è che i teoremi sono numerati in modo sequenziale, dall'inizio alla fine, senza alcun riferimento alle sezioni, capitoli; in questo*

modo si parte con il teorema 1 e si finisce con il teorema 169. Ovviamente non tutti i teoremi sono dovuti a Hilbert. Il teorema 90 (dimostrato per la prima volta da Hilbert) è uno dei più famosi.

Esercizio 47 *Scopo dell'esercizio è di ridimostrare il risultato dell'Esercizio 43 usando il Teorema 90 di Hilbert.*

Sia L/K un'estensione ciclica di ordine n (cioè $[L : K] = n$). Sia $G = \langle\sigma\rangle$. Si suppone che K contenga una radice primitiva n-esima dell'unità, α.

1. *Mostrare che $N_{L/K}(\alpha^{-1}) = 1$*
2. *Mostrare che esiste $b \in L$ tale che $\sigma(b) = \alpha b$ (usare il Teorema 90)*
3. *Concludere che $L = K(b)$ con $b^n \in K$.*

3.3 Estensioni ciclotomiche.

Sia $P(x) = x^n - 1 \in \mathbb{Q}[x]$, le radici di P sono le *radici n-esime dell'unità*. Notiamo μ_n l'insieme delle radici n-esime dell'unità. Siccome $P(x)$ non ha radici multiple, $|\mu_n| = n$. Se $\alpha, \varepsilon \in \mu_n$, allora $(\alpha\varepsilon^{-1})^n = 1$, quindi $(\mu_n, \cdot)$ è un sotto gruppo del gruppo moltiplicativo $(\mathbb{C}^*, \cdot)$. Ricordiamo il seguente risultato di algebra:

Teorema 3.5. *Sia K un campo. Ogni sotto gruppo* finito *del gruppo moltiplicativo K^* è ciclico.*

Corollario 3.6. *Il gruppo moltiplicativo μ_n delle radici n-esime dell'unità è un gruppo ciclico.*

Osservazione 3.7. In questo caso (radici dell'unità in $\mathbb{C}$) abbiamo usato un grosso cannone per un piccolo moscerino. Infatti sia $f : \mathbb{Z} \to \mathbb{C}^* : k \to e^{\frac{2i\pi k}{n}}$. Allora $Ker(f) = n\mathbb{Z}$ e l'immagine $\mu_n = \{e^{\frac{2i\pi k}{n}} \mid 1 \leq k \leq n\}$ è un gruppo isomorfo al gruppo ciclico $(\mathbb{Z}_n, +)$. D'altra parte se $\xi = e^{\frac{2i\pi}{n}}$, allora $\mu_n = \{\xi, \xi^2, ..., \xi^n = 1\}$. Le n radici dell'unità appartengono tutte alla circonferenza unità e la dividono in n parti uguali (da cui il nome di ciclotomia).

Definizione 3.8. *Una radice n-esima dell'unità, α, è* primitiva *se $n = min\{k \mid \alpha^k = 1\}$.*

Equivalentemente (cf Esercizio 48) una radice n-esima dell'unità, α, è primitiva se e solo α è un generatore di μ_n, ossia $\mu_n = \{\alpha, \alpha^2, ..., \alpha^n\}$.

Indichiamo con $\overline{\mu}_n$ l'insieme delle radici primitive n-esime dell'unità. Se ε è una radice primitiva, allora ε genera μ_n, in particolare genera $\overline{\mu}_n$.

Lemma 3.9. *Sia ε una radice primitiva n-esima dell'unità. Abbiamo:*

$\overline{\mu}_n = \{\varepsilon^{n_1}, \varepsilon^{n_2}, ..., \varepsilon^{n_k}\}$ dove $n_1 = 1, ..., n_k$ sono esattamente tutti gli interi t, $1 \leq t \leq n$, primi con n. In particolare:

$$\{n_1, ..., n_k\} \simeq U_n$$

dove U_n è il gruppo moltiplicativo degli elementi invertibili di $\mathbb{Z}_n$.

Dimostrazione (Dimostrazione). Se $d|n_i$ e $d|n$, diciamo $n_i = dt$, $n = ds$ e se $\beta = \varepsilon^{n_i}$, allora $\beta^s = \varepsilon^{n_i s} = \varepsilon^{dts} = 1$, se $d > 1$, $s < n$ e quindi β non è primitiva.

Sia $(n, n_i) = 1$ (n e n_i primi tra di loro). Se $\beta^t = 1$, allora $\varepsilon^{n_i t} = 1$ e quindi $n_i t \geq n$ perché ε è primitiva. Sia $n_i t = an + r$, $0 \leq r < n$ (divisione euclidea). Abbiamo $\varepsilon^{n_i t} = \varepsilon^r = 1$ quindi $r = 0$ e $n_i t = an$, siccome $(n_i, n) = 1$, n divide t, pertanto $t \geq n$. Chiaramente $\beta^n = (\varepsilon^{n_i})^n = 1$, quindi β è una radice primitiva n-esima dell'unità.

Questo mostra che gli n_i sono esattamente gli interi t, $1 \leq t \leq n$, primi con n. Per Bezout $(m, n) = 1 \Leftrightarrow \exists a, b$ tali che $an + bm = 1$, questo è equivalente a: $\overline{m}\overline{b} \equiv \overline{1}$ in $\mathbb{Z}_n$, quindi $\{\overline{n}_i\} = U_n$.

Osservazione 3.10. La funzione di Eulero (indicatore d'Eulero), $\varphi : \mathbb{N} \to \mathbb{N}$, è definita da: $\varphi(n) = \#\{m \mid 1 \leq m \leq n \text{ e } (m,n) = 1\}$. Quindi $\varphi(n) = \#(U_n)$ è il numero di radici primitive n-esime dell'unità.

Abbiamo $x^n - 1 = \prod_{\varepsilon}(x - \varepsilon)$ dove il prodotto è fatto su tutte le radici n-esime dell'unità. Ogni radice n-esima dell'unità è una radice primitiva per un qualche d che divide n (Esercizio 48). Se $d \mid n$ possiamo raggruppare tutte i fattori dove ε è una radice primitiva d-esima:

Definizione 3.11. *L'ennesimo polinomio ciclotomico, $\Phi_n(x)$ è:*

$$\Phi_n(x) = \prod_{\varepsilon}(x - \varepsilon)$$

dove il prodotto è fatto sulle radici primitive n-esime dell'unità. In particolare $\deg(\Phi_n(x)) = \varphi(n)$.

Abbiamo quindi:

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

I primi polinomi ciclotomici sono:

$$\begin{aligned}
\Phi_1(x) &= x - 1 \\
\Phi_2(x) &= x + 1 \\
\Phi_3(x) &= x^2 + x + 1 \\
\Phi_4(x) &= x^2 + 1 \\
\Phi_5(x) &= x^4 + x^3 + x^2 + x + 1 \\
\Phi_6(x) &= x^2 - x + 1 \\
\Phi_7(X) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1
\end{aligned}$$

Il risultato fondamentale è:

Teorema 3.12. (Gauss)
Per ogni $n \geq 1$, $\Phi_n(x) \in \mathbb{Z}[x]$ e $\Phi_n(x)$ è irriducibile su $\mathbb{Q}$.

Con questo teorema abbiamo facilmente quello che ci serve per il seguito:

Proposizione 3.13. *Sia L il campo di spezzamento di $\Phi_n(x)$. Allora $L = \mathbb{Q}(\varepsilon)$ dove ε è una radice primitiva n-esima dell'unità e $Gal(\mathbb{Q}(\varepsilon)/\mathbb{Q}) \simeq U_n$. In particolare $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ è normale e $Gal(\mathbb{Q}(\varepsilon)/\mathbb{Q})$ è abeliano.*

Dimostrazione (Dimostrazione). Segue dal Lemma 3.9 che $L = \mathbb{Q}(\varepsilon)$. Se $\sigma \in G := Gal(\mathbb{Q}(\varepsilon)/\mathbb{Q})$, σ è completamente determinato da $\sigma(\varepsilon) = \varepsilon^{n_i}$. Abbiamo quindi: $\varphi : G \to U_n : \sigma \to \overline{n}_i$. Si verifica facilmente che φ è un morfismo di gruppi. Se $\varphi(\sigma) = \overline{1}$, allora $\sigma(\varepsilon) = \varepsilon$ e σ è l'identità, quindi φ è iniettiva. Sia $\overline{n}_j \in U_n$. Per il Lemma 3.9, ε^{n_j} è radice di $\Phi_n(x)$. Per il Teorema 3.12, $\Phi_n(x)$ è irriducibile e quindi esiste $\tau \in G$ tale che $\tau(\varepsilon) = \varepsilon^{n_j}$ (cf 2-Esercizio 26), quindi φ è suriettiva.

Ci sarebbe molto da dire ancora sulle estensioni ciclotomiche, ma per il momento ci fermiamo qua.

—— .. ——

Esercizi.

Esercizio 48 *Per definizione una radice n-esima dell'unità, ε, è primitiva se $n = min\{k \mid \varepsilon^k = 1\}$.*

1. *Mostrare che ε è primitiva se e solo se ε genera μ_n*
2. *Se ε è una radice n-esima dell'unità allora ε è una radice primitiva d-esima dell'unità per un qualche d che divide n.*

Esercizio 49 *Sia ξ una radice primitiva n-esima dell'unità. Sia K un campo intermedio: $\mathbb{Q} \subset K \subset \mathbb{Q}(\xi)$. Mostrare che $K/\mathbb{Q}$ è normale.*

Esercizio 50 *Sia $\varphi(n)$ la funzione d'Eulero.*

1. *Se p è primo: $\varphi(p) = p - 1$ e $\varphi(p^a) = p^a - p^{a-1} = p^a(1 - \frac{1}{p})$*
2. *Se $(m, n) = 1$, allora $\varphi(mn) = \varphi(m)\varphi(n)$ (φ è moltiplicativa)*
3. *Se $n = \prod_i p_i^{a_i}$, dove i p_i sono primi distinti, allora $\varphi(n) = n.\prod_i(1 - \frac{1}{p_i})$*
4. *$\varphi(n)$ è sempre pari.*

Esercizio 51 *Sia G un gruppo ciclico di ordine n ($G \simeq (\mathbb{Z}_n, +)$). Mostrare che se $d \mid n$ esiste uno ed un unico sottogruppo, H, di G di ordine d; H ha $\varphi(d)$ generatori.*

Ogni elemento, $x \in G$, genera un sotto gruppo di G.

Concludere che $n = \sum_{d|n} \varphi(d)$.

Esercizio 52 *Sia p un numero primo. Mostrare che $\Phi_p(x) = x^{p-1} + ... + 1$. Usando il criterio di Eisenstein mostrare che $\Phi_p(x+1)$ è irriducibile in $\mathbb{Z}[x]$. Concludere che $\Phi_p(x) \in \mathbb{Z}[x]$ è irriducibile.*

Esercizio 53 *Sia ξ una radice primitiva p-esima dell'unità (p un numero primo). Mostrare che esiste uno ed un unico campo intermedio quadratico: $\mathbb{Q} \subset K \subset \mathbb{Q}(\xi)$ (K quadratico $\Leftrightarrow [K : \mathbb{Q}] = 2$). (Hint: usare l'Esercizio 51.)*

Esercizio 54 *Con il cambio di variabile $y = x + \frac{1}{x}$, determinare le quattro radici complesse di $x^4 + x^3 + x^2 + x + 1 = 0$. Si mostrerà che le radici sono della forma $r_i = \frac{r \pm \sqrt{r^2-4}}{2}$ dove $r = \frac{-1 \pm \sqrt{5}}{2}$.*

Sia $\xi = e^{2i\pi/5}$. Scrivere ξ,...,ξ^4 usando $r_1, ..., r_4$.

Determinare l'unico campo quadratico contenuto in $\mathbb{Q}(\xi)$ (cf Esercizio 53).

3.4 Estensioni radicali.

Iniziamo col riformulare bene la nozione di risolubilità per radicali:

Definizione 3.14. *L'estensione di campi L/K è* pura *se $L = K(a)$ con $a^n \in K$ per un qualche intero n.*
Se $n = min\{t \in \mathbb{N} \,|\, a^t \in K\}$, n è l'esponente dell'estensione. Se l'esponente è un numero primo p, si dice che L/K è una p-estensione pura.

Definizione 3.15. *L'estensione L/K è* radicale *se esiste una torre:*

$$K = K_0 \subset K_1 \subset ...K_t = L$$

tale che ogni K_i/K_{i-1}, $1 \leq i \leq t$, sia pura.

Osservazione 3.16. Come già osservato L/K è radicale se e soltanto se esiste una torre:

$$K = K'_0 \subset K'_1 \subset ...K'_m = L$$

dove ogni K'_i/K'_{i-1} è p_i-pura (p_i un numero primo).

Definizione 3.17. *Sia $f(x) \in \mathbb{Q}[x]$ irriducibile su $\mathbb{Q}$ con radici (in Ω) $r_1, ..., r_n$. L'equazione $f(x) = 0$ è* risolubile per radicali *se e soltanto se esiste un'estensione $F/\mathbb{Q}$ radicale, con $\mathbb{Q}(r_1, ..., r_n) \subset F$.*

Dobbiamo ancora sistemare un piccolo problema tecnico: se f è risolubile per radicali abbiamo quindi:

$$\mathbb{Q} = K_0 \subset K_1 \subset ... \subset K_t \quad (*)$$

dove (cf Osservazione 3.16) K_i/K_{i-1} è una p_i-estensione pura e dove:

$L := \mathbb{Q}(r_1, ..., r_n) \subset K_t$. Per usare i risultati precedenti bisogna che K_{i-1} contenga una radice primitiva p_i-esima dell'unità, e questo non è un grosso problema: possiamo facilmente modificare la torre $(*)$ di modo che questa condizione sia verificata. Il problema più grosso è che l'inclusione $L \subset K_t$ può essere stretta e in questo caso non possiamo affermare che $K_t/\mathbb{Q}$ è un'estensione normale (sappiamo solo che K_t/K_{t-1} è normale): anzi in generale questo è falso. Sia per esempio: $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$. L'estensione $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ è una 2-estensione pura (e $\mathbb{Q}$ contiene -1, radice primitiva seconda dell'unità), quindi $K_1 = \mathbb{Q}(\sqrt{2})/\mathbb{Q}$ è normale (Corollario 3.2). Aggiungiamo a K_1 una radice quadrata di $\sqrt{2}$ (cioè una radice quarta di 2): $K_2 = K_1(\sqrt[4]{2})/K_1$; come prima questa estensione è normale. Adesso l'estensione $K_2 = \mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ non è normale perché K_2 non contiene tutte le radici di $X^4 - 2$.

Possiamo sistemare questo problema nel modo seguente:

Proposizione 3.18. *Sia R/K un'estensione radicale. Esiste un'estensione N/R tale che N/K sia radicale e normale.*

Dimostrazione. Sia

$$K \subset R_1 = K(a_1) \subset R_2 = K(a_2) = K(a_1, a_2) \subset ... \subset R_t = R = K(a_1, ..., a_t)$$

Sia $P_i(X)$ il polinomio minimo di a_i su K. Sia A_i l'insieme delle radici di P_i. Poniamo $N := K(A_1, ..., A_t)$. L'estensione N/K è normale perché è il campo di spezzamento del polinomio $P(X) = \prod P_i(X) \in K[X]$ (cf 2-Lemma 2.32). Rimane da vedere che N/K è radicale. Per ipotesi $a_i^{n_i} = \theta_i \in R_{i-1}$. Mostriamo che se $a \in A_i$ allora $a^{n_i} \in R_{i-1}$. Questo permette di concludere: basta considerare la torre ottenuta aggiungendo a K, uno alla volta, gli elementi di A_1, poi quelli di A_2, ecc... e finalmente quelli di A_t.

Se $a \in A_1$ esiste $\sigma \in Gal_K(P_1)$ tale che $\sigma(a_1) = a$ (perché P_1 è irriducibile, cf 2-Esercizio 26); quindi $\sigma(a_1^{n_1}) = (\sigma(a_1))^{n_1} = a^{n_1}$. Quindi $a^{n_1} = \sigma(\theta_1) \in K$.

Sia $i > 1$. L'estensione $K(A_i)/K$ è normale ($K(A_i)$ è il campo di spezzamento di $P_i(X)$) e $Gal(K(A_i)/K)$ è il gruppo di Galois di P_i. Siccome P_i è irriducibile esiste $\sigma \in Gal(K(A_i)/K)$ tale che $\sigma(a_i) = a$. Consideriamo: $K \subset K(A_i) \subset K(A_1, ..., A_i)$: tutte le estensioni sono normali ($K(A_1, ..., A_i)$ è il campo di spezzamento di $P_1(X)...P_i(X)$). Quindi (2.2.52) σ può essere esteso a $\tilde{\sigma} \in Gal(K(A_1, ..., A_i)/K)$. Adesso consideriamo: $K \subset K(A_1, ..., A_{i-1}) \subset K(A_1, ..., A_i)$: tutte le estensioni sono normali e quindi (2.2.52):
$\tilde{\sigma}_| \in Gal(K(A_1, ..., A_{i-1})/K)$. Adesso abbiamo $a_i^{n_i} \in R_{i-1} \subset K(A_1, ..., A_{i-1})$. Quindi $\tilde{\sigma}_|(a_i^{n_i}) \in K(A_1, ..., A_{i-1})$. Siccome $\tilde{\sigma}(a_i^{n_i}) = (\tilde{\sigma}(a_i))^{n_i} = \sigma(a_i)^{n_i} = a^{n_i}$, concludiamo che $a^{n_i} \in K(A_1, ..., A_{i-1})$. □

Siamo quasi pronti per dimostrare la versione "forte" (cioè su $\mathbb{Q}$) del primo teorema di Galois: se $f(x) \in \mathbb{Q}[x]$ è risolubile per radicali esiste:

$$\mathbb{Q} = K_0 \subset K_1 \subset ... \subset K_t \quad (+)$$

dove ogni K_{i+1}/K_i è p_i-pura, $L \subset K_t$ (L campo di spezzamento di f su $\mathbb{Q}$) e dove $K_t/\mathbb{Q}$ è normale. Per potere usare a pieno i nostri risultati (3.3, 3.4) bisogna che K_i contenga una radice primitiva p_i-esima dell'unità: per questo, come vedremo, basta modificare la torre (+), non è un problema. Siamo quindi più o meno nella situazione annunciata all'inizio: il gruppo di Galois, G, ha una filtrazione:

$$G = G_0 \supset G_1 \supset ... \supset G_t = \{1\}$$

con sottogruppi tali che: G_{i+1} è un sottogruppo normale di G_i e G_i/G_{i+1} è un gruppo ciclico di ordine un numero primo. Un gruppo con questa proprietà si dice *gruppo risolubile.*

Anzi oggi la definizione più comune di gruppo risolubile è:

Definizione 3.19. *Un gruppo finito G è* risolubile *se esiste una filtrazione con sottogruppi:*

$$\{1\} = G_t \subset ... \subset G_{i+1} \subset G_i \subset ... \subset G_1 \subset G$$

dove ogni G_{i+1} è un sottogruppo normale di G_i e dove G_i/G_{i+1} è abeliano.

Osservazione 3.20. Nella Definizione 3.19, G_{i+1} *non è necessariamente* un sottogruppo normale di G.

Ogni gruppo abeliano finito è chiaramente risolubile.

Ricordiamo il teorema di struttura dei gruppi abeliani finiti:

Teorema 3.21. *Ogni gruppo abeliano finito, G, è isomorfo a un prodotto di gruppi ciclici*

$$G \simeq \mathbb{Z}_{d_1} \times ... \times \mathbb{Z}_{d_s}$$

con $d_1|d_2|...|d_s$. Il numero s è caratterizzato dalla proprietà che G può essere generato da s elementi ma non da $s-1$ elementi.

Usando il Teorema 3.21 si dimostra:

Lemma 3.22. *Un gruppo finito G è risolubile se ammette una filtrazione:*

$$\{1\} = G_k \subset ... \subset G_{i+1} \subset G_i \subset ... \subset G_1 \subset G$$

dove ogni G_{i+1} è un sottogruppo normale di G_i e dove G_i/G_{i+1} è ciclico di ordine un numero primo.

Avremo bisogno del seguente:

Lemma 3.23. *Sia G un gruppo finito.*

1. *Se G è risolubile ogni sottogruppo o gruppo quoziente di G è risolubile.*
2. *Sia $H \lhd G$ un sottogruppo normale, allora: G è risolubile $\Leftrightarrow$ H e G/H sono risolubili.*

—— .. ——

Esercizi.

Esercizio 55 *Sia $G \leq S_n$ un sotto gruppo del gruppo simmetrico e sia $X = \{1, 2, ..., n\}$. Si considera su X la relazione binaria:*

$$xRy \Leftrightarrow x = y \text{ o } \tau_{xy} \in G$$

dove τ_{xy} indica la trasposizione che scambia x con y.

1. *Dimostrare che R è una relazione d'equivalenza*
2. *Si assume G transitivo (i.e. $\forall x, y \in X, \exists \sigma \in G$ tale che $\sigma(x) = y$). Mostrare che tutte le classi di equivalenza, $R(x)$, hanno lo stesso numero di elementi.*
3. *Concludere che se $n = p$ è primo e se G, transitivo, contiene una trasposizione, allora $G = S_p$.*

Esercizio 56 *Sia $f(x) \in \mathbb{Q}[x]$ un polinomio irriducibile di grado p, p primo.*

1. *Mostrare che se $f(x)$ ha esattamente $p-2$ radici reali, allora $Gal_{\mathbb{Q}}(f) = S_p$ (usare l'Esercizio 55)*
2. *Mostrare che $f(x) = x^5 - 4x + 2$ è irriducibile su $\mathbb{Q}$ con $Gal_{\mathbb{Q}}(f) = S_5$.*

Esercizio 57 *Mostrare che S_n è risolubile se $n \leq 4$. (Quindi anche $\mathcal{A}_n$ è risolubile se $n \leq 4$.)*

Esercizio 58 *Sia $X = \{x_1, ..., x_k, ..., x_n\}$. Si indica con $(x_1, ..., x_k)$ la permutazione σ di X definita da: $\sigma(x_i) = x_{i+1}$ se $1 \leq i \leq k-1$, $\sigma(x_k) = x_1$, $\sigma(x_i) = x_i$ se $i > k$. Si dice che $(x_1, ..., x_k)$ è un ciclo di lunghezza k (o un k-ciclo). Per esempio i due cicli sono esattamente le trasposizioni.*

1. *Mostrare che per $n \geq 3$, ogni elemento di $\mathcal{A}_n$ si scrive come un prodotto di tre-cicli (hint: ogni elemento di $\mathcal{A}_n$ è un prodotto di un numero pari di trasposizioni, basta quindi considerare il prodotto di due trasposizioni).*
2. *Sia $G \leq S_n$. Mostrare che $\mathcal{A}_n \leq G$ se e solo se G contiene tutti i tre cicli di S_n.*

Esercizio 59 *Siano G, H due sotto gruppi di S_n (risp. $\mathcal{A}_n$) tali che: $H \lhd G$ e G/H sia abeliano. Si assume $n \geq 5$. Mostrare che se G contiene tutti i 3-cicli di S_n, allora anche H contiene tutti i 3-cicli; cioè se $\mathcal{A}_n \subset G$, allora $\mathcal{A}_n \subset H$ (cf Esercizio 58). (Hint: mostrare che ogni 3-ciclo si scrive $\sigma^{-1}\rho^{-1}\sigma\rho$ dove σ e ρ sono 3-cicli.)*

Concludere che se $n \geq 5$, S_n e $\mathcal{A}_n$ non sono risolubili.

Concludere che esistono polinomi irriducibili del quinto grado, $f(x) \in \mathbb{Q}[x]$, con $Gal_{\mathbb{Q}}(f)$ non risolubile.

3.5 Il teorema di Galois.

Abbiamo tutto in mano per dimostrare il primo risultato di Galois:

Teorema 3.24. *Sia $f(x) \in \mathbb{Q}[x]$ irriducibile, con radici (in Ω): $r_1, ..., r_n$. Sia $L := \mathbb{Q}(r_1, ..., r_n)$. Se l'equazione $f(x) = 0$ è risolubile per radicali, il gruppo di Galois di f, $Gal(L/\mathbb{Q})$, è un gruppo risolubile.*

Dimostrazione. Siccome f è risolubile per radicali, abbiamo una torre:

$$\mathbb{Q} \subset R_1 \subset ... \subset R_t$$

dove ogni R_i/R_{i-1}, $1 \leq i \leq t$, è una p_i-estensione pura: $R_i = R_{i-1}(a_i)$ con $a_i^{p_i} = \theta_i \in R_{i-1}$ e dove $L = \mathbb{Q}(r_1, ..., r_m) \subset R_t$ (cf Osservazione 3.16). Inoltre possiamo assumere $R_t/\mathbb{Q}$ normale (Proposizione 3.18). Il polinomio $X^{p_i} - \theta_i \in R_{i-1}[X] \subset R_t[X]$ ha una radice (a_i) in R_t e quindi ha tutte le sue radici in R_t (R_t/R_{i-1} è normale perché $R_t/\mathbb{Q}$ lo è). Le radici sono $\alpha_i a_i, ..., \alpha_i^{p_i} a_i = a_i$ dove α_i è una radice primitiva p_i-esima dell'unità. Quindi $\alpha_i = (\alpha_i a_i)/a_i \in R_t$. Sia $n = p_1 p_2 ... p_t$ e sia α una radice primitiva n-esima dell'unità. Modifichiamo la torre iniziale:

$$\mathbb{Q} \subset \mathbb{Q}(\alpha) = K_0 \subset K_1 = R_1(\alpha) \subset ... \subset K_t = R_t(\alpha) = R_t$$

(Osservare che $\alpha \in R_t$.)

(a) Mostriamo che $G_0 := Gal(K_t/K_0)$ è risolubile.

Consideriamo $K_{i-1} \subset K_i \subset K_t$. Tutte le estensioni sono normali: K_t/K_{i-1} e K_t/K_i perché $K_t/\mathbb{Q}$ è normale; K_i/K_{i-1} per il Corollario3.2, infatti $K_{i-1} = R_{i-1}(\alpha)$ contiene una radice primitiva p_i-esima dell'unità (se $\beta := \alpha^{p_1 \cdots \hat{p}_i \cdots p_n}$ allora β è una radice primitiva p_i-esima dell'unità). Abbiamo: $G_i := Gal(K_t/K_i) \lhd Gal(K_t/K_{i-1}) := G_{i-1}$ e $G_{i-1}/G_i \simeq Gal(K_i/K_{i-1})$ (2-Osservazione 2.52). Dal Lemma 3.1 $Gal(K_i/K_{i-1})$ è ciclico di ordine p_i. Abbiamo quindi:

$$G_0 = Gal(K_t/K_0) \supset G_1 = Gal(K_t/K_1) \supset ...$$

$$... \supset G_{t-1} = Gal(K_t/K_{t-1} \supset G_t = Gal(K_t/K_t) = \{1\}$$

dove ogni G_i è un sottogruppo normale di G_{i-1} e dove ogni G_{i-1}/G_i è ciclico di ordine un numero primo. Quindi (Lemma 3.22) G_0 è risolubile.

(b) $Gal(K_t/\mathbb{Q})$ è risolubile.

Consideriamo $\mathbb{Q} \subset K_0 = \mathbb{Q}(\alpha) \subset K_t$. Tutte le estensioni sono normali (per $\mathbb{Q}(\alpha)/\mathbb{Q}$, vedere Proposizione 3.13). Quindi (2-Osservazione 2.52): $G_0 \lhd G := Gal(K_t/\mathbb{Q})$ e il quoziente è $Gal(\mathbb{Q}(\alpha)/\mathbb{Q})$. Per la Proposizione 3.13 quest'ultimo gruppo è abeliano quindi risolubile (Osservazione 3.20). Per (a) e il Lemma 3.23, G è risolubile.

(c) $Gal(L/\mathbb{Q})$ è risolubile.

Consideriamo: $\mathbb{Q} \subset L = \mathbb{Q}(r_1, ..., r_n) \subset K_t$. Tutte le estensioni sono normali quindi: $Gal(K_t/L) \lhd Gal(K_t/\mathbb{Q}) = G$ e il quoziente è $Gal(L/\mathbb{Q})$. Quindi $Gal(L/\mathbb{Q})$ è un quoziente del gruppo risolubile $Gal(K_t/\mathbb{Q})$, pertanto (Lemma 3.23) $Gal(L/\mathbb{Q})$ è risolubile. $\square$

Cerchiamo adesso di dimostrare la seconda parte del teorema di Galois (se $Gal(f)$ è un gruppo risolubile, allora $f(x) = 0$ è risolubile per radicali).

Come già osservato l'idea di base è nel risultato seguente che permette di fabbricare le p-estensioni pure dell'estensione radicale:

Proposizione 3.25. *Sia L/K un'estensione normale con $|Gal(L/K)| = p$ (p un numero primo). Se K contiene una radice primitiva p-esima dell'unità allora $L = K(\beta)$ con $\beta^p \in K$, cioè L/K è p-pura.*

Questa Proposizione è già stata dimostrata (cf Esercizio 43, Esercizio 47), la dimostrazione che segue, più vicina all'originale, usa la risolvente di Lagrange:

Dimostrazione. Per il teorema dell'elemento primitivo, $L = K(v)$ (quindi $v \notin K$). Sia $\alpha \in K$ una radice primitiva p-esima dell'unità (quindi $\alpha \neq 1$). Osserviamo che K contiene *tutte* le radici p-esime che sono $\alpha, \alpha^2, ..., \alpha^p = 1$. L'ipotesi $|Gal(L/K)| = p$ implica che $Gal(L/K)$ è ciclico, ogni elemento diverso dall'identità è un generatore: $Gal(L/K) = \{\sigma, \sigma^2, ..., \sigma^p = Id\}$. Poniamo, *per ogni* radice p-esima, ζ, dell'unità: $t(\zeta) = v + \zeta\sigma(v) + \zeta^2\sigma^2(v) + ... + \zeta^{p-1}\sigma^{p-1}(v)$.

(a) Abbiamo $\sigma(t(\zeta)) = \zeta^{-1}t(\zeta)$. Infatti: $\sigma(t(\zeta)) = \sigma(v)+\zeta\sigma^2(v)+...+\zeta^{p-1}v$ e si conclude perché $\zeta^{-1} = \zeta^{p-1}$.

(b) $\exists\zeta \neq 1$ con $t(\zeta) \neq 0$. Abbiamo:

$$\begin{cases} v + \sigma(v) + \sigma^2(v) + ... + \sigma^{p-1}(v) & = & t(1) \\ v + \alpha\sigma(v) + \alpha^2\sigma^2(v) + ... + \alpha^{p-1}\sigma^{p-1}(v) & = & t(\alpha) \\ \vdots & \vdots & \vdots \\ v + \alpha^{(i)}\sigma(v) + \alpha^{2i}\sigma^2(v) + ... + \alpha^{(i)(p-1)}\sigma^{p-1}(v) & = & t(\alpha^i) \\ \vdots & \vdots & \vdots \\ v + \alpha^{(n-1)}\sigma(v) + \alpha^{2(n-1)}\sigma^2(v) + ... + \alpha^{(p-1)^2}\sigma^{p-1}(v) & = & t(\alpha^{p-1}) \end{cases}$$

Se $t(\alpha) = ... = t(\alpha^{p-1}) = 0$, allora $v = \frac{1}{p}t(1)$ (sommare tutte le equazioni, cf 1.Lemma 1.7). Quindi $\sigma(v) = \frac{1}{p}\sigma(t(1))$, cioè (cf (a)): $\sigma(v) = v$. Questo implica $\sigma^i(v) = v$ quindi $v \in K$ il campo fisso di $Gal(L/K)$ (L/K è normale); in contraddizione con $L = K(v)$.

Sia $\beta = t(\zeta)$, $\zeta \neq 1$ e con $t(\zeta) \neq 0$. Da (a): $\sigma(\beta) = \zeta^{-1}\beta$, quindi $\beta \notin K$ (perché $\zeta \neq 1$, quindi $\sigma(\beta) \neq \beta$). Inoltre $\sigma(\beta^p) = (\sigma(\beta))^p = (\zeta^{-1}\beta)^p = \beta^p$. Quindi $\sigma^i(\beta^p) = \beta^p$ e questo implica $\beta^p \in K$.

Abbiamo $K \subset K(\beta) \subset L$, quindi $p = dim_K(L) = dim_{K(\beta)}L.dim_K K(\beta)$. Siccome $dim_K K(\beta) > 1$ ($\beta \notin K$), $dim_K K(\beta) = p$, pertanto $K(\beta) = L$. □

Rimane ancora da sistemare un problema tecnico collegato all'esistenza (o meglio, non esistenza) di radici primitive dell'unità: come nella dimostrazione del primo teorema vogliamo lavorare su $\mathbb{Q}(\varepsilon)$ dove ε è una radice primitiva n-esima dell'unità ($n = |Gal(f)|$). Il problema è che $\mathbb{Q}(\varepsilon)$, in generale, non è un campo intermedio tra $\mathbb{Q}$ e $\mathbb{Q}(r_1, ..., r_n)$. Questo si sistema nel modo seguente:

Proposizione 3.26. (Natural irrationalities)
Sia $f(x) \in K[x]$ un polinomio irriducibile. Notiamo $M = K(r_1, ..., r_n)$ il campo di spezzamento di f su K. Sia L/K un'estensione e sia $N = L(r_1, ..., r_n)$ il campo di spezzamento di f su L. Allora $Gal(N/L)$ è isomorfo al sottogruppo $Gal(M/M \cap L)$ di $Gal(M/K)$.

Dimostrazione. Abbiamo la situazione seguente:

$$\begin{array}{ccccc} & N = L(r_1, ..., r_n) & & & \\ \nearrow & \uparrow & \nwarrow & & \\ L \leftarrow & L \cap M & \rightarrow M = K(r_1, ..., r_n) & & \\ \nwarrow & \uparrow & \nearrow & & \\ & K & & & \end{array}$$

Definiamo $\psi : Aut_L(N) \to Aut_{L\cap M}(M) : \sigma \to \sigma_{|M}$. Mostriamo che ψ è ben definita. È chiaro che la restrizione di σ è un K-morfismo: $\sigma_{|M} : M \to N \subset \Omega$. Siccome M/K è normale (2-Proposizione 2.34), $\sigma_{|M}(M) = M$ e quindi $\sigma_{|M} \in Aut(M)$. È chiaro che $\sigma_{|M\cap L} = Id$ e quindi ψ è ben definita. Si verifica facilmente che ψ è un morfismo di gruppi.

(a) ψ è iniettiva: se $\psi(\sigma) = Id$, allora $\sigma_{|M} : M = K(r_1, ..., r_n) \to M = K(r_1, ..., r_n)$ verifica $\sigma(r_i) = r_i$, questo implica $\sigma = Id_L$.

(b) ψ è suriettiva: sia $G' = \psi(Gal(N/L))$, G' è un sottogruppo di $Gal(M/M \cap L)$. Sia $F = M^{G'}$, il sotto campo di M fissato da G'. Abbiamo: $M \cap L \subset F$. Se $x \in M$, $x \notin M \cap L$, siccome L è il campo fisso di $Gal(N/L)$ (perché N/L è normale, 2-Proposizione 2.34), esiste $\tau \in Aut_L(N)$ tale che $\tau(x) \neq x$. Pertanto $\psi(\tau(x)) \neq x$. Concludiamo che $F = M \cap L$. Siccome M/K è normale, per la corrispondenza di Galois (2-Teorema 2.51), $G' = Gal(M/M \cap L)$. □

Possiamo finalmente dimostrare il secondo teorema di Galois:

Teorema 3.27. *Sia $f(x) \in \mathbb{Q}[x]$ un polinomio irriducibile. Sia $L = \mathbb{Q}(r_1, ..., r_n)$ il campo di spezzamento di f su $\mathbb{Q}$. Se $Gal(L/\mathbb{Q})$ è un gruppo risolubile allora l'equazione $f(x) = 0$ è risolubile per radicali.*

Dimostrazione. Sia $k = |Gal(L/\mathbb{Q})|$ e sia ε una radice primitiva k-esima dell'unità. Consideriamo $\mathbb{Q}(\varepsilon)/\mathbb{Q}$: è un'estensione pura, quindi radicale. Sia $N = \mathbb{Q}(\varepsilon, r_1, ..., r_n)$, per la Proposizione 3.26 $G := Gal(N/\mathbb{Q}(\varepsilon)$ è isomorfo a un sottogruppo di $Gal(L/\mathbb{Q})$; pertanto (Lemma 3.23), G è risolubile. Abbiamo quindi una filtrazione:

$$G = G_0 \supset G_1 \supset ... \supset G_r = \{1\}$$

con $G_{i+1} \lhd G_i$ e G_i/G_{i+1} ciclico di ordine un numero primo. Per la corrispondenza di Galois (2-Teorema 2.51), abbiamo la corrispondente torre di estensioni:

$$\mathbb{Q}(\varepsilon) = K_0 \subset K_1 \subset ... \subset K_r = N$$

dove K_{i+1}/K_i è normale con $Gal(K_{i+1}/K_i) \simeq \frac{Gal(N/K_i)}{Gal(N/K_{i+1})} \simeq \frac{G_i}{G_{i+1}}$.

Quindi $Gal(K_{i+1}/K_i)$ è ciclico di ordine un numero primo. Sia $d = |G|$, abbiamo $d|k$ (Teorema di Lagrange). Siccome $|G_i|$ e $|G_{i+1}|$ dividono d, $p = |Gal(K_{i+1}/K_i)|$ divide k, diciamo $pt = k$. Abbiamo $\varepsilon^t \in K_0 \subset K_i$, quindi K_i contiene una radice primitiva p-esima dell'unità ($\beta = \varepsilon^t$ appunto). Questo implica (Proposizione 3.25) $K_{i+1} = K_i(a_i)$ con $a_i^p \in K_i$. Pertanto $N/\mathbb{Q}(\varepsilon)$ è radicale. Siccome $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ è radicale, $N/\mathbb{Q}$ è radicale. Siccome $r_1, ..., r_n \in N$, la nostra equazione è risolubile per radicali. □

Mettendo assieme i teoremi 3.24, 3.27:

Teorema 3.28. (Galois)
Sia $f(x) \in \mathbb{Q}[x]$ un polinomio irriducibile. Sia $L = \mathbb{Q}(r_1, ..., r_n)$ il campo di spezzamento di f su $\mathbb{Q}$. L'equazione $f(x) = 0$ è risolubile per radicali se e solo se $Gal(L/\mathbb{Q})$ è un gruppo risolubile.

Questo risultato chiude definitivamente, almeno da un punto di vista teorico, il problema della risoluzione per radicali delle equazioni algebriche. Da un punto di vista pratico, come dice lo stesso Galois: *les calculs sont impraticables* (i calcoli [per determinare il gruppo di Galois] sono impraticabili); infatti data un'equazione è spesso impossibile determinare il suo gruppo di Galois.

Comunque sia, adesso che abbiamo un bel giocattolo (il Teorema 3.28), possiamo iniziare a giocare:

Teorema 3.29. (Abel)
L'equazione generale, a coefficienti in $\mathbb{Q}$, del quinto grado non è risolubile per radicali.

Dimostrazione. Basta trovare un'equazione del quinto grado con gruppo di Galois non risolubile: S_5 non è risolubile (Esercizio 59) e se $f(x) = x^5 - 4x + 2$, $Gal_{\mathbb{Q}}(f) = S_5$ (Esercizio 56). □

Teorema 3.30. (Abel)
Sia $f(x) \in \mathbb{Q}[x]$ irriducibile tale che $Gal_{\mathbb{Q}}(f)$ sia abeliano, allora $f(x) = 0$ è risolubile per radicali.

Dimostrazione. Ogni gruppo abeliano è chiaramente risolubile. □

É in onore di questo risultato che i gruppi commutativi vengono chiamati anche gruppi abeliani.

Per illustrare l'importanza della sua teoria, Galois non poteva limitarsi a ridimostrare i teoremi di Abel, aveva bisogno di un risultato nuovo, generale. L'ultimo teorema della memoria di Galois è:

Teorema 3.31. (Galois)
Sia $f(x) \in \mathbb{Q}[x]$ un polinomio irriducibile di grado un numero primo p. Siano $r_1, ..., r_p$ le radici in Ω di f e sia $L = \mathbb{Q}(r_1, ..., r_p)$ il campo di spezzamento. Allora $f(x) = 0$ è risolubile per radicali se e solo se $\forall i, j, i \neq j$, $L = \mathbb{Q}(r_i, r_j)$ (cioè, detto alla Galois, se e solo se tutte le radici sono funzioni razionali di due qualsiasi tra di loro).

Dimostrazione. Cf Esercizi. □

—— .. ——

Esercizi.

Esercizio 60 *Nel seguito G e X sono insiemi finiti. Un'azione del gruppo G sull'insieme X è un morfismo di gruppi: $\varphi : G \to Sym(X)$, dove $Sym(X)$ indica il gruppo simmetrico (gruppo delle biiezioni) di X. Indicheremo con $\varphi_g(x)$ (o anche $g.x$, gx) l'immagine di $x \in X$ tramite la biiezione φ_g.*

Lo stabilizzatore di $x \in X$ è $G_x = \{g \in G \mid \varphi_g(x) = x\}$; è un sotto gruppo di G. L'orbita (o traiettoria) di x è $O(x) = \{\varphi_g(x) \mid g \in G\}$. Un elemento $x \in X$ è fisso se $\varphi_g(x) = x, \forall g \in G$; cioè $O(x) = \{x\}$. Si nota X^G l'insieme dei punti fissi.

1. *Mostrare che la relazione su X: $xRy \Leftrightarrow x$ e y sono nella stessa orbita, è una relazione d'equivalenza.*
2. *Concludere che*
$$\#(X) = \sum_{i=1}^{r} \#(O(x_i)) + \#(X^G) \tag{3.1}$$
*dove $\#(O(x_i)) > 1, 1 \leq i \leq r$ (*prima equazione delle classi*).*
3. *Fissiamo un punto $x \in X$. La relazione su G: $gTh \Leftrightarrow gh^{-1} \in G_x$ è una relazione d'equivalenza. Mostrare che $f : G/G_x \to O(x) : \overline{g} \to g.x$ è ben definita e biiettiva. Concludere che:*
$$\#(G) = \#(G_x).\#(O(x)) \tag{3.2}$$
*(*seconda equazione delle classi*). Le equazioni delle classi sono tutto quello che serve per dimostrare la maggior parte dei teoremi di base della teoria dei gruppi finiti.*

Esercizio 61 *Sia $G \leq S_n$ un sotto gruppo abeliano e transitivo. Mostrare che $\#(G) = n$. (Hint: mostrare che se $\sigma \in G, \sigma \neq Id$, allora σ non ha punti fissi; concludere con l'Esercizio 60).*

Esercizio 62 *Sia $G \leq S_n$ un sotto gruppo transitivo. Sia $H \lhd G$ un sotto gruppo normale non banale.*

1. *Mostrare che tutte le orbite $O_H(x)$ hanno lo stesso numero di elementi.*
2. *Concludere che se $n = p$ è primo, allora H è transitivo.*

Esercizio 63 (Il gruppo affine di $\mathbb{F}_p$)
Il gruppo $W := GA(p)$ delle affinità di $\mathbb{F}_p$ (considerato come spazio vettoriale su $k = \mathbb{F}_p$) è: $W = \{f_{a,b} \mid a \in \mathbb{F}_p^\times, b \in \mathbb{F}_p\}$ dove $f_{a,b} : \mathbb{F}_p \to \mathbb{F}_p : x \to ax + b$.

Mostrare che $\#(W) = p(p-1)$ e che W è risolubile (considerare il morfismo parte lineare *che ad ogni affinità associa la sua parte lineare). Concludere che W è un sotto gruppo transitivo e risolubile di S_p.*

Esercizio 64 *Scopo dell'esercizio è mostrare che ogni sotto gruppo, $G \leq S_p$, p primo, transitivo e risolubile è il coniugato di un sotto gruppo del gruppo affine $W = GA(p)$; cioè $G = \varphi H \varphi^{-1}$, con $H \leq W$.*

1. *Si indica con t l'affinità $f_{1,1}$ ($f_{1,1,}(x) = x + 1$). Osservare che t non è altro che il p-ciclo $(0, 1, ..., p-1)$ (dove $X = \mathbb{F}_p = \{0, 1, ..., p-1\}$).*
   Mostrare che se $\alpha \in S_p$ è tale che $\alpha t \alpha^{-1} \in W$, allora $\alpha \in W$ (osservare che $\alpha t \alpha^{-1} = f_{a,b}$ non ha punti fissi, quindi $a = 1, b \neq 0$ e considerare $\alpha t \alpha^{-1} \alpha = f_{a,b} \alpha$).
2. *Sia $G \leq S_p$ transitivo e risolubile. Quindi esiste:*
$$\{1\} = G_n \lhd G_{n-1} \lhd ... \lhd G_1 \lhd G_0 = G$$
   con $G_{n-1} \neq \{1\}$ e G_{i-1}/G_i ciclico.
   Osservare che G_1 e quindi tutti i G_i, $i < n$, sono transitivi (Esercizio 62). Concludere che $T = G_{n-1}$, essendo transitivo e ciclico, è isomorfo a $\mathbb{Z}_p$ (usare l'Esercizio 61). Quindi $T = \langle \sigma \rangle$ dove σ ha ordine p, cioè σ è un p-ciclo: $\sigma = (x_0 x_1 ... x_{p-1})$.
3. *Osservare che in generale non tutti i p-cicli sono delle affinità (fare un esempio con $p = 5$).*
   Verificare che se $\varphi : X = \{x_0, x_1, ..., x_{p-1}\} \to X = \{0, 1, ..., p-1\} : x_i \to i$, allora $\sigma = \varphi^{-1} t \varphi$.
4. *Osservare che se $H \lhd H' \leq G$, allora $\forall g \in G$, $gHg^{-1} \lhd gH'g^{-1}$*
5. *Per il punto (4) abbiamo:*
$$\{1\} = H_n \lhd H_{n-1} = \langle t \rangle \lhd ... \lhd H_1 \lhd H_0 = H$$
   dove $H_i = \varphi G_i \varphi^{-1}$ (i G_i come in (2)). Mostrare che $H_i \leq W$ (usare (1)). Concludere che $H = \varphi G \varphi^{-1} \leq W$; quindi G è il coniugato del sotto gruppo H di W.

Esercizio 65 *Scopo dell'esercizio è mostrare il seguente risultato:*

Sia $G \leq S_p$, p primo, un sotto gruppo transitivo, allora: G è risolubile $\Leftrightarrow$ l'unica permutazione di G che ha due punti fissi è l'identità.

1. *Usando l'Esercizio 64 mostrare la prima implicazione (se G è risolubile l'unica permutazione di G con due punti fissi è l'identità).*
2. *Mostrare che $\forall x, y \in X = \{0, ..., p-1\}$, $\#(G_x) = \#(G_y)$ (usare l'Esercizio 60) e che $G_x \cap G_y = \{Id\}$ se $G_x \neq G_y$.*
3. *Concludere che se $A = \{\sigma \in G \mid \sigma$ non ha punti fissi$\}$, allora $\#(A) = p-1$.*
4. *Sia $\sigma \in A$, si tratta di mostrare che σ è un p-ciclo. Si considera l'azione del gruppo $\langle \sigma \rangle$ su X. Sia n l'ordine di σ ($n = \#\langle \sigma \rangle$). Mostrare che se $\sigma^i(x) = x$ allora $\sigma^i = Id$ (considerare $\sigma^{i+1}(x)$). Concludere che tutte le orbite $O(x)$ hanno n elementi (Esercizio 60).*
5. *Concludere che $n = p$ (Esercizio 60) e che σ è un p-ciclo.*
6. *Siccome σ è un p-ciclo, σ è coniugato a t (cf (1) dell'Esercizio 64): $\sigma = \varphi t \varphi^{-1}$. Mostrare che se $\rho \in G$, allora $\rho \sigma \rho^{-1}$ non ha punti fissi, concludere che $\rho \sigma \rho^{-1} \in \langle \sigma \rangle$. Quindi $\varphi^{-1}(\rho \sigma \rho^{-1})\varphi \in \langle t \rangle$, ossia $(\varphi^{-1} \rho \varphi) t ((\varphi^{-1} \rho \varphi)^{-1} \in W$. Concludere che $\varphi^{-1} G \varphi \subset W$ (usare (1) dell'Esercizio 64).*
7. *Concludere che G è risolubile.*

Esercizio 66 *Dimostrare il Teorema 3.31 (usare la corrispondenza di Galois).*

Sia $f(x) \in \mathbb{Q}[x]$*, irriducibile, di grado* p *dove* $p \geq 5$ *è primo. Mostrare che se* f *ha esattamente due radici reali, allora* $f(x) = 0$ *non è risolubile per radicali.*

Parte II

Il problema inverso

4

Il problema inverso di Galois.

4.1 Il problema inverso.

4.1.1 Il problema generale.

Sia K un'estensione finita di $\mathbb{Q}$. Abbiamo visto che ad ogni estensione finita, normale (e separabile), L/K, corrisponde un gruppo finito $G := Gal(L/K)$.

Più generalmente sia K un campo. Allora ad ogni estensione finita, normale e separabile (una tale estensione viene detta di Galois o galoisienne), associamo il gruppo finito $Aut_K(L) =: Gal(L/K) =: G$. In queste condizioni si dice che G è di Galois su K (o che G è realizzato (come gruppo di Galois) su K).

Il problema inverso di Galois su K consiste nel chiedersi quali sono i gruppi finiti che possono essere realizzati come gruppi di Galois su K (in queste condizioni si dirà che K è il *campo base*).

Una versione più generale (e più facile) del problema consiste nel chiedersi quali sono i gruppi finiti che possono essere realizzati come gruppi di Galois su un qualche campo K.

Posto in questa generalità il problema ammette una risposta semplice:

Teorema 4.1. *Se G è un gruppo finito, esiste un campo K tale che G sia di Galois su K.*

Più precisamente si può prendere per K un'estensione finita di $\mathbb{Q}$.

Dimostrazione. Esercizio 68. □

Se invece vogliamo lavorare su un campo base K, la risposta dipende molto dal campo K scelto. Per esempio se $K = \mathbb{F}_p$, allora si può dimostrare che ogni gruppo di Galois su K è ciclico; quindi non tutti i gruppi finiti sono di Galois su K.

Se invece si prende $K = \mathbb{C}(x)$, si può dimostrare che ogni gruppo finito è di Galois su K.

Nel caso del nostro campo prediletto, $K = \mathbb{Q}$, il problema è ancora aperto e molto difficile.

Chiaramente il caso $K = \mathbb{Q}$ è quello più naturale, perché $\mathbb{Q}$ è il campo primo di ogni campo di caratteristica zero e anche perché $\mathbb{Q}$ è il campo dei quozienti di $\mathbb{Z}$ e quindi le connessioni con l'aritmetica sono numerose.

Nel seguito ci occuperemo esclusivamente del problema inverso di Galois sul campo base $\mathbb{Q}$

Definizione 4.2. *Un gruppo finito G è detto di Galois (su $\mathbb{Q}$) se esiste un'estensione finita, normale, $L/\mathbb{Q}$ con $Gal(L/\mathbb{Q}) \simeq G$.*

E quindi il nostro problema diventa:

Problema 4.3. *(Problema inverso)*
Determinare i gruppi finiti che sono di Galois su $\mathbb{Q}$.

Si congettura che ogni gruppo finito sia di Galois. Un risultato spettacolare in questa direzione è il seguente:

Teorema 4.4. (Shafarevich)
Ogni gruppo risolubile è di Galois su $\mathbb{Q}$.

La dimostrazione di questo teorema richiede tecniche molto avanzate. Malgrado questo risultato siamo ancora ben lontani dall'avere una dimostrazione completa della congettura. Nel seguito cercheremo di risolvere il problema per alcune classi di gruppi, di spiegare quali sono le difficoltà in generale e di illustrare alcuni metodi per affrontare la questione.

4.1.2 Il problema inverso effettivo.

Se G è di Galois, $G \simeq Gal(L/\mathbb{Q})$ e se $\alpha \in L$ è un elemento primitivo, il gruppo di Galois del suo polinomio minimo, $f(x)$, è proprio G: $G \simeq Gal_{\mathbb{Q}}(f)$. Abbiamo così un polinomio irriducibile $f(x) \in \mathbb{Q}[x]$ il cui gruppo di Galois è il nostro gruppo G; cioè abbiamo una realizzazione *effettiva* di G come gruppo di Galois.

Il problema inverso effettivo consiste nel determinare per ogni gruppo, G, di Galois un polinomio irriducibile con gruppo di Galois G:

Problema 4.5. *(Problema inverso effettivo)*
Determinare per ogni gruppo di Galois, G, un polinomio irriducibile $f(x) \in \mathbb{Q}[x]$ con $Gal_{\mathbb{Q}}(f) \simeq G$.

Per risolvere questo problema ci sono vari ostacoli. Per esempio se $G = Gal(L/\mathbb{Q})$, allora bisogna avere una buona conoscenza di L per sperare di trovare un elemento primitivo (anche se sappiamo che un generico $\alpha \in L \setminus \mathbb{Q}$ è

primitivo). Ma una volta trovato α rimane ancora da trovare il suo polinomio minimo e questo, anche se è teoricamente facile, nella pratica non è banale (*les calculs sont impraticables*).

Osserviamo che esistono vari software (PARI/GP, SAGE, GAP ecc...) che possono essere di aiuto per questi problemi. Torneremo più avanti su questo aspetto computazionale del problema.

Comunque non è che possiamo andare avanti gruppo per gruppo, bisogna quindi cercare di risolvere il problema per famiglie di gruppi. Per esempio

Teorema 4.6. *Per ogni $n \geq 2$ sia $f_n(x) = x^n - x - 1$. Allora $f_n(x)$ è irriducibile su $\mathbb{Q}$ con $Gal_{\mathbb{Q}}(f_n) = S_n$.*

Dimostrazione. La dimostrazione usa tecniche di teoria algebrica dei numeri. □

Questo risolve il problema inverso effettivo per i gruppi simmetrici S_n.

A questo punto sorge inevitabilmente un problema di fondo: bisognerebbe potere organizzare tutti i gruppi in famiglie, cioè bisognerebbe avere una classificazione dei gruppi finiti, ma come vedremo, la classificazione dei gruppi finiti non è finita!

4.1.3 Gradi delle realizzazioni.

Se G è di Galois, $G = Gal(L/\mathbb{Q})$ e $G = Gal_{\mathbb{Q}}(f)$ dove f è il polinomio minimo di un elemento primitivo di $L/\mathbb{Q}$. Se $n = \deg(f)$, allora $n = [L : \mathbb{Q}] = \#(G)$.

D'altra parte se $f(x) \in \mathbb{Q}[x]$ è un polinomio irriducibile con $Gal_{\mathbb{Q}}(f) = G$, allora $\deg(f) \mid \#(G)$, ma possiamo avere $\deg(f) < \#(G)$ (Esercizio 69).

Definizione 4.7. *Un polinomio irriducibile $f(x) \in \mathbb{Q}[x]$ realizza (o rappresenta) G se $Gal_{\mathbb{Q}}(f) = G$. Il grado della realizzazione (o rappresentazione) è* $\deg(f)$.

Una realizzazione di grado $\#(G)$ sarà detta di grado massimo o massimale.

A questo punto viene naturale chiedersi:

Problema 4.8. Se G è di Galois quali sono i possibili gradi delle rappresentazioni di G?

Abbiamo appena visto che se G è di Galois, allora G ammette sempre rappresentazioni massimali.

Ovviamente un modo per affrontare questo problema (e anche il problema inverso) consiste nel classificare i sotto gruppi transitivi di S_n. Una tale classificazione è nota per valori bassi di n ([2]), ma al crescere di n il problema diventa presto impraticabile...

Esercizi.

Esercizio 67 (Teorema di Cayley)
Sia G un gruppo finito. Una rappresentazione transitiva (di permutazione) è un morfismo di gruppi $\varphi : G \to S_n$ tale che l'azione indotta di G su $X = \{1, 2, ..., n\}$ sia transitiva ($\forall x \neq y \in X$, $\exists g \in G$ tale che $\varphi_g(x) = y$).

La rappresentazione si dice fedele *se φ è iniettivo.*

Dimostrare il teorema di Cayley: per ogni gruppo finito G esiste una rappresentazione transitiva, fedele $\varphi : G \to S_n$ (hint: prendere $n = \#(G)$ e fare agire G su se stesso).

Esercizio 68 *Si prenderà per buono che per ogni $n \geq 2$, il gruppo simmetrico S_n è di Galois su $\mathbb{Q}$ (cf Teorema 4.6).*

Mostrare che se G è un gruppo finito esiste una torre $\mathbb{Q} \subset K \subset L$ con $L/\mathbb{Q}$ finita tale che $Gal(L/K) \simeq G$ (ogni gruppo finito è di Galois su un campo di numeri).

Esercizio 69 *Dare un esempio di un gruppo G di Galois (su $\mathbb{Q}$) che ammette una rappresentazione di grado $< \#(G)$ (cioè esiste $f(x) \in \mathbb{Q}[x]$, irriducibile di grado $n < \#(G)$, con $Gal_{\mathbb{Q}}(f) = G$).*

Esercizio 70 *Sia G un gruppo finito di ordine g.*

1. *Mostrare che se $f(x) \in \mathbb{Q}[x]$ irriducibile, di grado k, realizza G, allora $k \mid g$ e $g \mid k!$.*
2. *Mostrare che ogni realizzazione di S_n ha grado $\geq n$. Concludere che il grado minimo di una realizzazione di S_n è n.*
3. *Determinare tutti i gradi delle realizzazioni di S_3.*
4. *Cosa potete dire sui gradi delle realizzazioni di S_4?*

Esercizio 71 *Sia G un gruppo finito tale che ogni sotto gruppo di G sia normale.*

1. *Mostrare che ogni realizzazione di G come gruppo di Galois è massimale.*
2. *Concludere che se G è abeliano ogni realizzazione è massimale.*

Esercizio 72

1. *Sia G un gruppo finito e $H \leq G$. Mostrare che se H ha indice due, allora $H \lhd G$.*
2. *Sia G un gruppo di ordine 8 in cui esiste un unico elemento di ordine due. Mostrare che ogni sotto gruppo di G è normale*
3. *Il* gruppo dei quaternioni *è $\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ dove:*

$$\begin{cases} -1^2 = 1 \\ i^2 = j^2 = k^2 = -1 \\ ij = -ji = k \\ jk = -kj = i \\ ki = -ik = j \end{cases}$$

Verificare che $\mathbb{H}_8$ *è un gruppo non abeliano (si prenderà per buono che il prodotto è associativo). Mostrare che ogni sotto gruppo di* $\mathbb{H}_8$ *è normale. La proprietà di avere tutti i sotto gruppi normali* non *caratterizza i gruppi abeliani. Ogni realizzazione di* $\mathbb{H}_8$ *è massimale (cf Esercizio 71).*

Esercizio 73

1. *Sia* G *un gruppo finito. Se ogni elemento* ($\neq 1$) *di* G *ha ordine due, allora* G *è abeliano*
2. *Sia* G *un gruppo non abeliano di ordine* 8. *Mostrare che* G *ha un elemento,* x, *di ordine* 4. *Sia* $N = \langle x \rangle$. *Nel seguito si assume che ogni elemento di* $G \setminus N$ *ha ordine* 4.
3. *Mostrare che* $G = \{1, x, x^2, x^3, y, y^3, yx, y^3x\}$, *dove* $y \notin N$ *e* $y^2 = x^2$.
4. *Concludere che* $G \simeq \mathbb{H}_8$

4.2 Un teorema di Dedekind.

Scopo di questa sezione è la dimostrazione del seguente risultato:

Teorema 4.9. (Dedekind)
Sia $f(x) \in \mathbb{Z}[x]$ un polinomio monico, irriducibile di grado n. Sia p un numero primo tale che la riduzione modulo p di f, $\overline{f}(x) \in \mathbb{F}_p[x]$ non abbia radici multiple (nel campo di spezzamento di $\overline{f}$). Se $\overline{f} = \overline{f}_1 ... \overline{f}_r$ è la fattorizzazione in fattori irriducibili di $\overline{f}(x)$ in $\mathbb{F}_p[x]$, allora $Gal_{\mathbb{Q}}(f) \leq S_n$ contiene una permutazione σ la cui decomposizione in cicli disgiunti è:

$$\sigma = \gamma_1 ... \gamma_r, \quad con \;\; l(\gamma_i) = \deg(\overline{f}_i)$$

dove $l(\gamma)$ indica la lunghezza del ciclo $\gamma \in S_n$.

Chiaramente questo risultato può essere di grande utilità nel determinare il gruppo di Galois di un polinomio irriducibile.

Ci sono almeno due modi di dimostrare questo risultato: (i) usando la risolvente di Galois, (ii) usando strumenti della teoria algebrica dei numeri; useremo il primo.

4.2.1 Richiami sulle risolventi di Galois.

Ricordiamo velocemente i fatti di base sulle risolventi di Galois (cf prima parte Capitolo II, sez. 4.2).

Sia $f(x) \in \mathbb{Q}[x]$ un polinomio irriducibile di grado n con campo di spezzamento $L = \mathbb{Q}(r_1, ..., r_n)$.

Galois mostra che se $(t_1, ..., t_n) \in \mathbb{Z}^n$ è sufficientemente generale allora $t := t_1 r_1 + ... + t_n r_n$, verifica $\sigma.t \neq \tau.t$, $\forall \sigma, \tau \in S_n, \sigma \neq \tau$, dove $\sigma.t = t_1 r_{\sigma(1)} + ... + t_n r_{\sigma(n)}$.

Inoltre mostra che ogni t che verifica questa proprietà è un elemento primitivo di L. Detto ciò considera il polinomio:

$$s(x) = \prod_{\sigma \in S_n} (x - \sigma.t) \tag{4.1}$$

Per il teorema delle funzioni simmetriche, $s(x) \in \mathbb{Q}[x]$. Sia:

$$s(x) = h_1(x) ... h_t(x) \tag{4.2}$$

la fattorizzazione in fattori irriducibili di $s(x)$ in $\mathbb{Q}[x]$. Osserviamo che (4.1) mostra che L è il campo di spezzamento di $s(x)$ ($\sigma.t \in L, \forall \sigma \in S_n$). Quindi ogni radice di h_i è un qualche $\sigma.t$ e ogni $\sigma.t$ è radice di un qualche h_i. Possiamo quindi assumere che $Id.t = t$ sia radice di h_1. Abbiamo $h_1(x) = \prod_{\sigma \in G}(x - \sigma.t)$, questo individua un sottoinsieme $G = \{Id, \sigma_1, ..., \sigma_{m-1}\} \subset S_n$. Si mostra dopo che $G = Gal_{\mathbb{Q}}(f)$, visto come gruppo di permutazioni delle radici.

Osservazione 4.10. Ovviamente questa descrizione dipende dall'ordine scelto sulle radici e anche dalla scelta dei t_i. Se cambiamo l'ordine delle radici: $\varphi : \{r_i\} \to \{r_{\varphi(i)}\}$, come sotto gruppo di permutazioni ($G_{\mathbb{Q}}(f) \leq S_n$), otteniamo un sotto gruppo coniugato. Cosa succede se cambiamo i t_i?

Dalla definizione "moderna": $Gal_{\mathbb{Q}}(f) = Aut_{\mathbb{Q}}(L) =: Gal(L/\mathbb{Q})$. Adesso è chiaro che, una volta scelto un ordine delle radici, ogni elemento di $Aut_{\mathbb{Q}}(L)$ induce una permutazione delle radici e questo ci permette di vedere $Aut_{\mathbb{Q}}(L)$ come un sotto gruppo di S_n. In questo modo $Gal(L/\mathbb{Q})$ è un sotto gruppo di S_n ben definito a meno di coniugo. In particolare la struttura ciclica di ogni $\sigma \in Gal(L/\mathbb{Q})$, visto come elemento di S_n, è univocamente definita.

Questo non è altrettanto chiaro dalla definizione "classica", *à la Galois*. Osserviamo che esistono sotto gruppi isomorfi di S_n che non sono coniugati. Per esempio in S_4, se $\tau = (12)$ e se $\rho = (12)(34)$, allora $\langle\tau\rangle$ e $\langle\rho\rangle$ sono entrambi isomorfi a $\mathbb{Z}_2$, ma non sono coniugati in S_4 (la decomposizione in cicli disgiunti è diversa).

L'osservazione fondamentale di Galois è che ogni $\sigma.t$ è un elemento primitivo di L (perché $\tau.(\sigma.t) \neq \rho.(\sigma.t)$ se $\tau \neq \rho$), quindi gli h_i hanno tutti lo stesso grado: $\deg(h_i) = m = \#(G), \forall i$ (perché se $\sigma.t$ è radice di h_i, h_i è il polinomio minimo di $\sigma.t$ che è primitivo).

Otteniamo così una partizione di S_n in r sotto insiemi di cardinalità $\#(G)$ che non sono altro che le classi dell'insieme quoziente S_n/G per la relazione d'equivalenza $xRy \Leftrightarrow y^{-1}x \in G$.

Quindi se $\sigma.t$ è radice di h_i, $\sigma.t$ è primitivo, con polinomio minimo h_i. Abbiamo $\{\theta \in S_n \mid \theta.h_i = h_i\} = \sigma G \sigma^{-1}$, infatti $\theta.h_i = h_i$ implica $\theta\sigma(t) = \sigma_i(t)$ con $\sigma_i R \sigma$, cioè $\sigma_i \in \sigma G$. Quindi, senza tenere conto dell'ordine delle radici, possiamo dire che se h è un fattore irriducibile di $s(x)$, allora $\{\sigma \in S_n \mid \sigma.h = h\}$, che è palesamente un sottogruppo di S_n, è un coniugato di $Gal_{\mathbb{Q}}(f)$.

Per quanto riguarda i t_i, siccome i risultati precedenti sono validi per dei t_i generici (quindi senza relazioni tra di loro), questo suggerisce di considerarli come delle variabili. Pertanto invece di $s(x)$ consideriamo il polinomio:

$$s(\underline{u}, x) = \prod_{\sigma \in S_n} (x - (u_1 r_{\sigma(1)} + ... + u_n r_{\sigma(n)})) \in L[u_1, ..., u_n, x] \tag{4.3}$$

Osserviamo che abbiamo un'azione di $Gal(L/\mathbb{Q})$ su $L[u_1, ..., u_n, x]$ definita nel modo seguente: se $P(u_1, ..., u_n, x) = \sum a_I u_1^{\alpha_1} ... u_n^{\alpha_n}.x^{\alpha}$ e se $\tau \in Gal(L/\mathbb{Q})$, allora $\tau.P = \sum \tau(a_I) u_1^{\alpha_1} ... u_n^{\alpha_n}.x^{\alpha}$. Chiaramente $\tau.s(\underline{u}, x) = s(\underline{u}, x), \forall \tau \in Gal(L/\mathbb{Q})$, quindi $s(\underline{u}, x) \in \mathbb{Q}[u_1, ..., u_n, x]$.

Abbiamo anche un'azione di S_n su $L[u_1, ..., u_n, x]$, data dalle permutazioni degli u_i: $\sigma \times P = \sum a_I u_{\sigma(1)}^{\alpha_1} ... u_{\sigma(n)}^{\alpha_n}.x^{\alpha}$, $\sigma \in S_n$.

Ovviamente S_n agisce anche su $\mathbb{Q}[u_1, ..., u_n, x]$ per permutazioni degli u_i, ma l'azione di $Gal(L/\mathbb{Q})$ su $\mathbb{Q}[u_1, ..., u_n, x]$ è triviale.

4.2.2 La risolvente di Galois generica.

Continuiamo le considerazioni precedenti ma in un ambito più generale. Sia F un campo qualsiasi, $f(x) \in F[x]$ un polinomio monico, irriducibile, di grado n. Sia $L = F(r_1, ..., r_n)$ il campo di spezzamento di f su F. Siccome F potrebbe avere caratteristica positiva, assumiamo $r_i \neq r_j$ (i.e. f separabile). Come prima consideriamo il polinomio $s(\underline{u}, x) \in L[\underline{u}, x]$ (usiamo la notazione $\underline{u} = u_1, ..., u_n$). L'equazione

$$s(\underline{u}, x) = \prod_{\sigma \in S_n} (x - (u_1 r_{\sigma(1)} + ... + u_n r_{\sigma(n)})) \tag{4.4}$$

mostra che $s(\underline{u}, x) \in F[\underline{u}, x]$ e che $s(\underline{u}, x)$ spezza su L (in (4.4) ogni fattore ha grado uno). Abbiamo:

Teorema 4.11. *Con le notazioni precedenti se h è un fattore irriducibile di $s(\underline{u}, x)$ in $F[\underline{u}, x]$, allora $\{\tau \in S_n \mid \tau \times h = h\}$ è un sotto gruppo di S_n coniugato a $Gal_F(f)$.*

Dimostrazione. Siccome (4.4) è lo spezzamento di $s(\underline{u}, x)$ su L, se $h \mid s(\underline{u}, x)$, esiste $l := l(\underline{u}, x) = x - (u_1 r_{\sigma(1)} + ... + u_n r_{\sigma(n)})$ che divide h in $L[\underline{u}, x]$.

Sia adesso

$$\bar{l} := \prod_{\rho \in Gal(L/F)} \rho.l = \prod_{\rho \in Gal(L/F)} (x - (u_1 r_{\rho\sigma(1)} + ... + u_n r_{\rho\sigma(n)}))$$

Se $\tau \in Gal(L/F)$: $\tau\bar{l} = \prod_{\rho \in Gal(L/F)} \tau.(\rho.l) = \bar{l}$, quindi $\bar{l} \in F[\underline{u}, x]$.

Siccome $h \in F[\underline{u}, x]$, $\forall \rho \in Gal(L/F)$, $\rho.h = h$. Siccome $l \mid h$ in $L[\underline{u}, x]$, $\forall \rho \in Gal(L/F)$, $\rho.l \mid \rho.h = h$, quindi $\bar{l} \mid h$ in $L[\underline{u}, x]$, ma siccome $\bar{l}$ e h sono in $F[\underline{u}, x]$, $\bar{l} \mid h$ in $F[\underline{u}, x]$. Ma h è irriducibile in $F[\underline{u}, x]$, questo implica che $\bar{l} = h$ (a meno di una costante).

Sia $\tau \in S_n$ tale che $\tau \times h = h$. Siccome $l \mid h$ (su L), $\tau \times l \mid \tau \times h = h$. Quindi $\tau \times l$ divide $\bar{l}$ (perché $\bar{l} = h$). Siccome $\bar{l}$ spezza su L, viene $\tau \times l = \rho.l$ per un qualche $\rho \in Gal(L/F)$. In conclusione:

$$x - (u_{\tau(1)} r_{\sigma(1)} + ... + u_{\tau(n)} r_{\sigma(n)}) = x - (u_1 r_{\rho\sigma(1)} + ... + u_n r_{\rho\sigma(n)})$$

Se $\tau(i) = j$, $r_{\sigma(i)} = r_{\rho\sigma(j)}$ (perché le variabili u_i sono indipendenti), cioè: $r_{\sigma\tau^{-1}(j)} = r_{\rho\sigma(j)}$. Siccome gli r_i sono distinti: $\sigma\tau^{-1}(j) = \rho\sigma(j)$ e questo implica $\tau = \sigma^{-1}\rho^{-1}\sigma \in \sigma^{-1}Gal(L/F)\sigma$. Quindi $H \subset \sigma^{-1}Gal(L/F)\sigma$, dove $H = \{\theta \in S_n \mid \theta \times h = h\}$.

Rimane da vedere che $\sigma^{-1}Gal(L/F)\sigma \subset H$, cioè bisogna vedere che se $\varphi \in Gal(L/F)$, allora $(\sigma^{-1}\varphi\sigma) \times h = h$. Abbiamo $h = \bar{l} = \prod_{\rho \in Gal(L/F)} \rho.l$, dove $\rho.l = x - (u_1 r_{\rho\sigma(1)} + ... + u_n r_{\rho\sigma(n)})$. Si verifica facilmente che $(\sigma^{-1}\varphi\sigma) \times (\rho.l) = (\rho\varphi^{-1}).l$. Quindi:

$$(\sigma^{-1}\varphi\sigma) \times \bar{l} = \prod_{\rho \in Gal(L/F)} (\rho\varphi^{-1}).l = \bar{l}$$

Pertanto $H = \sigma^{-1}Gal(L/F)\sigma$.

□

Osservazione 4.12. Questo approccio fornisce un algoritmo per calcolare il gruppo di Galois di un polinomio, infatti è possibile calcolare $s(\underline{u}, x)$ senza conoscere le radici di f.

Per vederlo iniziamo col considerare le radici come delle variabili:

$$\begin{aligned} S(\underline{u}, \underline{x}, y) &= \prod_{\sigma \in S_n} (y - (u_1 x_{\sigma(1)} + ... + u_n x_{\sigma(n)})) \\ &= \prod_{\sigma \in S_n} (x - (u_{\sigma(1)} x_1 + ... + u_{\sigma(n)} x_n)) \end{aligned}$$

Abbiamo $S(\underline{u}, \underline{x}, y) \in F[\underline{u}, \underline{x}, y]$ con due azioni di S_n (permutazioni degli u_i e permutazioni degli x_i).

Sviluppando $S(\underline{u}, \underline{x}, y) = \sum c_j y^j$, con $c_j = \sum_I g_I x_1^{i_1} ... x_n^{i_n}$, $I = (i_1, ..., i_n)$, $g_I \in F[u_1, ..., u_n]$. I polinomi g_I sono simmetrici negli u_i perché una permutazione degli u_i non cambia $S(\underline{u}, \underline{x}, y)$, quindi, per il teorema delle funzioni simmetriche, $g_I = h_I(e_1, ..., e_n)$ $(e_i = e_i(\underline{u}))$. Pertanto:

$$S(\underline{u}, \underline{x}, y) = \sum (\sum_I h_I(e_1, ..., e_n) x_1^{i_1} ... x_n^{i_n}) y^j$$

Adesso sia $f(y) = y^n - a_1 y^{n-1} + ... + (-1)^n a_n \in F[y]$, con radici r_i. Abbiamo $a_i = e_i(r_1, ..., r_n)$. Per quanto visto prima:

$$s(\underline{x}, y) = S(\underline{r}, \underline{x}, y) = \sum (\sum_I h_I(a_1, ..., a_n) x_1^{i_1} ... x_n^{i_n}) y^j$$

proprio perché $a_i = e_i(\underline{r})$.

Per chiarire la situazione facciamo un esempio banale, ossia $n = 2$ (perché altrimenti *les calculs sont impraticables!*).

Il polinomio generico è:

$$S(\underline{u}, \underline{x}, y) = (y - u_1 x_1 - u_2 x_2)(y - u_1 x_2 - u_2 x_1)$$

Abbiamo $S(\underline{u}, \underline{x}, y) = y^2 + c_1 y + c_0$ con $c_1 = -(x_1 + x_2)(u_1 + u_2) = -e_1(x_1 + x_2)$ e $c_0 = (x_1^2 + x_2^2) u_1 u_2 + (u_1^2 + u_2^2) x_1 x_2$, cioè $c_0 = e_2(x_1^2 + x_2^2) + (e_1^2 - 2e_2) x_1 x_2$.

Se, per esempio, consideriamo $f(y) = y^2 + y + 1$, abbiamo $a_1 = -1 = e_1$, $a_2 = e_2 = 1$ e il polinomio associato $s(\underline{x}, y) = y^2 - (x_1 + x_2) y + x_1^2 + x_2^2 - x_1 x_2$.

Osserviamo che $s(\underline{x}, y) \in \mathbb{Q}[\underline{x}, y]$ è irriducibile (il discriminante vale $-3(x_1 - x_2)^2 < 0$), quindi $Gal_{\mathbb{Q}}(f)$ ha ordine due (come sapevamo già!).

Vediamo adesso un algoritmo per calcolare il gruppo di Galois di un polinomio $f(y) \in \mathbb{Z}[y]$.

- Calcolare il polinomio associato $s(\underline{x}, y)$ (come abbiamo visto non c'è bisogno di conoscere le radici di f)

- Esiste un algoritmo per fattorizzare $s(\underline{x}, y) \in \mathbb{Z}[\underline{x}, y]$ (vedere Esercizio 78 nel caso di una variabile)
- Trovato un fattore irriducibile qualsiasi, h_1, abbiamo già l'ordine di $Gal_{\mathbb{Q}}(f)$: è il grado di h_1. Per avere il gruppo basta applicare ogni $\sigma \in S_n$ e vedere quali lasciano fisso h_1 (cf Teorema 4.11)

Questo algoritmo è interessante da un punto di vista teorico ma, in casi concreti *les calculs sont impraticables* (anche con un computer!).

4.2.3 Dimostrazione del teorema di Dedekind.

Dimostriamo adesso il Teorema 4.9.

Abbiamo $f(x) = x^n - a_{n-1}x^{n-1} + ... + (-1)^n a_0 \in \mathbb{Z}[x]$, irriducibile su $\mathbb{Z}$. Consideriamo l'applicazione naturale (*riduzione mod. p*): $\mathbb{Z} \to \mathbb{F}_p : n \to \overline{n}$. Per ipotesi il polinomio $\overline{f}(x) = x^n - \overline{a}_{n-1}x^{n-1} + ... + \overline{a}_0 \in \mathbb{F}_p[x]$ ha radici distinte in $\mathbb{F}_p$.

Sia $\overline{f} = \overline{f}_1 ... \overline{f}_r$ la fattorizzazione in fattori irriducibili in $\mathbb{F}_p[x]$.

Sia $L = \mathbb{Q}(r_1, ..., r_n)$ il campo di spezzamento di f su $\mathbb{Q}$. Sia

$$s(\underline{u}, x) = \prod_{\sigma \in S_n} (x - (u_1 r_{\sigma(1)} + ... + u_n r_{\sigma(n)})) \in \mathbb{Z}[\underline{u}, x] \tag{4.5}$$

e:

$$\overline{s}(\underline{u}, x) = \prod_{\sigma \in S_n} (x - (u_1 \overline{r}_{\sigma(1)} + ... + u_n \overline{r}_{\sigma(n)})) \in \mathbb{F}_p[\underline{u}, x] \tag{4.6}$$

Osserviamo che $\overline{s}(\underline{u}, x)$ è il polinomio associato a $\overline{f}$ e che $\overline{s}(\underline{u}, x)$ si ottiene da $s(\underline{u}, x)$ per riduzione mod. p dei coefficienti.

Attenzione: Non è così ovvio come potrebbe sembrare, infatti $\overline{r}_i$ NON è la riduzione mod. p di r_i, infatti in generale $r_i \notin \mathbb{Z}$!! (Le notazioni non sono forse il massimo...)

L'asserzione segue dal fatto che i coefficienti di $\overline{f}$ si ottengono da quelli di f per riduzione modulo p e perché i coefficienti di f, $\overline{f}$ sono funzioni elementari delle radici (Cf Osservazione 4.12).

Sia h un fattore irriducibile di $s(\underline{u}, x)$ in $\mathbb{Q}[\underline{u}, x]$. Sappiamo (Teorema 4.11) che $Gal_{\mathbb{Q}}(f)$ è un coniugato di $G = \{\tau \in S_n \mid \tau \times h = h\}$.

Osserviamo che possiamo supporre $h \in \mathbb{Z}[\underline{u}, x]$ (perché $\mathbb{Z}[\underline{u}, x]$ e $\mathbb{Q}[\underline{u}, x]$ sono dei domini a fattorizzazione unica (U.F.D.)). Possiamo quindi considerare $\overline{h} \in \mathbb{F}_p[\underline{u}, x]$.

Il polinomio $\overline{h}$ non è necessariamente irriducibile. Sia $\overline{g}$ un fattore irriducibile di $\overline{h}$. Per il Teorema 4.11, $Gal_{\mathbb{F}_p}(\overline{f})$ è un coniugato di $\overline{G} = \{\sigma \in S_n \mid \sigma \times \overline{g} = \overline{g}\}$ (per ipotesi le radici di $\overline{f}$ sono distinte).

Lemma 4.13. *Con le notazioni precedenti* $\overline{G} \subset G$.

Dimostrazione. Supponiamo $\sigma \times \overline{g} = \overline{g}$, ma $\sigma \times h = h_1 \neq h$.

Abbiamo $\sigma \times s(\underline{u}, x) = s(\underline{u}, x)$. Infatti:

$$\sigma \times s(\underline{u}, x) = \prod_{\theta \in S_n} (x - (u_{\sigma(1)} r_{\theta(1)} + ... + u_{\sigma(n)} r_{\theta(n)}))$$

Se $\sigma(i) = j$, $u_{\sigma(i)} r_{\theta(i)} = u_j r_{\theta\sigma^{-1}(j)}$ quindi:

$$\sigma \times s(\underline{u}, x) = \prod_{\theta \in S_n} (x - (u_1 r_{\theta\sigma^{-1}(1)} + ... + u_n r_{\theta\sigma^{-1}(n)})) = s(\underline{u}, x)$$

Adesso siccome $h \mid s(\underline{u}, x)$ segue che $h_1 = \sigma \times h \mid \sigma \times s(\underline{u}, x) = s(\underline{u}, x)$, anzi h_1 è un fattore irriducibile di $s(\underline{u}, x)$. Abbiamo quindi $s(\underline{u}, x) = h.h_1.q$. Riducendo modulo p: $\overline{s}(\underline{u}, x) = \overline{h}.\overline{h}_1.\overline{q}$.

D'altra parte $\sigma \times h = h_1$ implica $\sigma \times \overline{h} = \overline{h}_1$. Siccome $\overline{g} \mid \overline{h}$, $\sigma \times \overline{g} = \overline{g} \mid \sigma \times \overline{h} = \overline{h}_1$. In conclusione $\overline{g} \mid \overline{h}$ e $\overline{g} \mid \overline{h}_1$, pertanto $\overline{g}^2 \mid \overline{s}(\underline{u}, x)$. Ma questo non è possibile perché (4.6) mostra che $\overline{s}(\underline{u}, x) \in K[\underline{u}, x]$, dove K è il campo di spezzamento di $\overline{f}$, ha fattori irriducibili tutti distinti (perché per ipotesi le radici $\overline{r}_i$ sono distinte). □

A questo punto abbiamo mostrato che $Gal_{\mathbb{Q}}(f)$ contiene un coniugato di $Gal_{\mathbb{F}_p}(\overline{f})$. Per concludere bisogna usare risultati della teoria di Galois in caratteristica p (uno dei possibili seminari per l'esame!).

Sia $g(x) \in \mathbb{F}_p[x]$ un polinomio irriducibile di grado d. Il campo di spezzamento di g è $\mathbb{F}_{p^d}$ e $Gal(\mathbb{F}_{p^d}/\mathbb{F}_p)$ è ciclico di ordine d, generato dal morfismo di Frobenius, $\psi(x) = x^p$. Se α è una radice di g, le altre radici sono $\psi(\alpha), \psi^2(\alpha)$,...,$\psi^d(\alpha) = \alpha^{p^d} = \alpha$. Quindi l'azione di $Gal(\mathbb{F}_{p^d}/\mathbb{F}_p) = \langle \psi \rangle$ è quella di un d-ciclo. Applicando questo fatto ad ogni $\overline{f}_i$ si conclude la dimostrazione del Teorema 4.9.

Esercizi.

Esercizio 74 *Sia* $f(x) = x^5 + 20x - 16 \in \mathbb{Z}[x]$.

1. *Osservare che* $\overline{f}(x) \equiv f(x) \pmod 2$ *non è separabile*
2. *Abbiamo* $f(x) \equiv \overline{f}(x) = x^5 - x - 1 \pmod 3$. *Mostrare che* $\overline{f}(x)$ *è irriducibile. Dedurne che* $f(x) \in \mathbb{Q}[x]$ *è irriducibile e che* $G := Gal_{\mathbb{Q}}(f) \leq S_5$ *contiene un* 5*-ciclo.*
3. *Sia* $\overline{f}(x) \equiv f(x) \pmod 7$. *Mostrare che* $\overline{f}(2) = \overline{f}(3) = 0$ *(per favore non usate la vostra calcolatrice tascabile, ma il piccolo teorema di Fermat:* $x^p \equiv x \pmod p$*).*
4. *Concludere che* $\overline{f}(x) = (x-2)(x-3)g(x) \pmod 7$, *con* $g(x)$ *irriducibile.*
5. *Concludere che* $G := Gal_{\mathbb{Q}}(f)$ *contiene un* 5*-ciclo,* σ, *e un* 3*-ciclo* ρ.
6. *Considerando* $f'(x) \in \mathbb{Q}[x]$, *concludere che* G *contiene un elemento di ordine due.*
7. *Si prenderà per buono che* $disc(f) = 2^{16}.5^6$ *(Se avete tempo da perdere potete provare a dimostrarlo!).*
8. *A questo punto sapppiamo che* $G \subset \mathcal{A}_5$ *(perché?) e che* G *contiene un elemento di ordine due,* τ, *un elemento di ordine* 3, ρ, *e uno di ordine cinque,* σ. *Concludere che* $\#(G) = 30$ *o* 60.
9. *Concludere che* $Gal_{\mathbb{Q}}(f) = \mathcal{A}_5$ *(si tratta di trovare un elemento di ordine due diverso da* τ*).*

Esercizio 75 *Sia* p *un numero primo e* $f(x) = x^p - x - \delta \in \mathbb{F}_p[x]$. *Sia* α *una radice di* f *(in qualche estensione di* $\mathbb{F}_p$*) e sia* $L := \mathbb{F}_p(\alpha)$.

1. *Mostrare che* L *è il campo di spezzamento di* f *(per* $a \in \mathbb{F}_p$, *calcolare* $f(\alpha + a)$*)*
2. *Osservare che l'estensione* $L/\mathbb{F}_p$ *è separabile (e normale). Sia* $G = Gal(L/\mathbb{F}_p) = Gal_{\mathbb{F}_p}(f)$. *Mostrare che* $G \simeq \mathbb{Z}_p$ *(se* $\sigma \in G$, $\sigma(\alpha) = \alpha + j$, $j \in \mathbb{F}_p$*)*
3. *Concludere che se* f *non ha radici in* $\mathbb{F}_p$, *allora* $f(x)$ *è irriducibile in* $\mathbb{F}_p[x]$.

Esercizio 76 *Sia* $f(x) = x^5 - x - 1 \in \mathbb{Q}[x]$ *e sia* $G = Gal_{\mathbb{Q}}(f)$.

1. *Mostrare che* f *è irriducibile e che* G *contiene un* 5*-ciclo (ridurre* $\pmod 5$ *e usare l'Esercizio 75)*
2. *Osservare che* $f(x) \equiv (x^2 + x + 1)(x^3 + x^2 + 1) \pmod 2$. *Concludere che* G *contiene* $\sigma = \tau\rho$ *dove* τ *è una trasposizione e dove* ρ *è un* 3*-ciclo*
3. *Mostrare che* $\tau \in G$
4. *Concludere che* $G \simeq S_5$ *(usare l'Esercizio* 4.1 *del Capitolo III della prima parte).*

Esercizio 77 (Polinomi di interpolazione di Lagrange)
Siano $c_1, ..., c_t$ *degli elementi di* k *due a due distinti (*$c_i \neq c_j$ *se* $i \neq j$*). Si pone*

$$P_i(X) = \frac{\Pi_{j\neq i}(X - c_j)}{\Pi_{j\neq i}(c_i - c_j)}, \ \ 1 \leq i \leq t.$$

I polinomi P_i hanno grado al più $t-1$ e verificano: $P_i(c_j) = \delta_{ij}$.

I polinomi P_i si chiamano i polinomi di interpolazione di Lagrange rispetto agli elementi $c_1, ..., c_t$ di k.

Mostrare che:

1. *I polinomi $P_1, ..., P_t$ sono una base dello spazio vettoriale $E = k[X]_{\leq(t-1)}$ dei polinomi di grado al più $(t-1)$.*
2. *Se P è un polinomio di grado al più $(t-1)$, allora: $P = P(c_1).P_1 + ... + P(c_t).P_t$.*
3. *In particolare:*
   - $1 = P_1 + ... + P_t$
   - $X = c_1P_1 + ... + c_tP_t$
   - $X^k = c_1^k.P_1 + ... + c_t^k.P_t \quad (k \leq t-1)$.

Esercizio 78 *Scopo dell'esercizio è di mostrare che esiste un algoritmo per determinare se un polinomio $f(x) \in \mathbb{Z}[x]$ è o meno irriducibile.*

1. *Sia $\deg(f) = n$, se f non è irriducibile, ammette un fattore di grado $\leq r$ dove r è il massimo intero tale che $2r \leq n$*
2. *Per $0 \leq j \leq r$, si pone: $f(j) = c_j$. Se $h \mid f$, allora $h(j) \mid c_j, \forall j$. Se $c_i = 0$ per un qualche i allora $x - i \mid f$*
3. *Ogni c_j ha un numero finito di divisori ed esiste un algoritmo per determinarli (come?)*
4. *Sia $(d_0, d_1, ..., d_r)$ tale che $d_i \mid c_i, \forall i$. Esiste un unico polinomio $g(x) \in \mathbb{Q}[x]$ con $\deg(g) \leq r$ tale che $g(j) = d_j, 0 \leq j \leq r$ (usare l'Esercizio 77)*
5. *Concludere che si può (teoricamente) determinare in un tempo finito se $f(x)$ è o meno irriducibile e una sua fattorizzazione in fattori irriducibili.*

4.3 Realizzazioni del gruppo simmetrico.

4.3.1 Il teorema di irriducibilità di Hilbert.

I polinomi simmetrici elementari $e_1 = e_1(x_1, ..., x_n) = x_1 + ... + x_n$, ..., $e_n = e_n(x_1, ..., x_n) = x_1...x_n$ sono, in particolare delle funzioni razionali, cioè $e_1, ..., e_n \in \mathbb{Q}(x_1, ..., x_n) =: L$. Possiamo quindi considerare il campo delle funzioni razionali simmetriche: $K := \mathbb{Q}(e_1, ..., e_n) \subset \mathbb{Q}(x_1, ..., x_n) = L$.

Il campo L è il campo di spezzamento del polinomio $P(T) = T^n - e_1T^{n-1} + ... + (-1)^n e_n \in K[T]$ perché $P(T) = (T - x_1)...(T - x_n)$. Segue che l'estensione L/K è algebrica finita e normale.

Il gruppo S_n agisce su L per permutazioni delle variabili x_i, quindi $S_n \leq Aut(L)$. Se $\varphi(x_1, ..., x_n) \in L$ è una funzione razionale, allora φ è simmetrica se e solo se $\sigma.\varphi = \varphi, \forall \sigma \in S_n$. Quindi K è il campo fisso di $S_n \leq Aut(L)$. Quindi $Gal(L/K) = S_n$.

Il polinomio

$$P(\underline{x}, T) = T^n - e_1(x_1, ..., x_n)T^{n-1} + ... + (-1)^n e_n(x_1, ..., x_n) \in \mathbb{Q}[\underline{x}, T] \quad (4.7)$$

Osservare che i coefficienti di $P(\underline{x}, T)$ valgono tutti ± 1. Il polinomio $P(\underline{x}, T)$ è detto il polinomio *generico*.

Infatti se specializziamo le variabili x_i (i.e. diamo dei valori): $x_1 = a_1$, ..., $x_n = a_n$, otteniamo il polinomio $(T - a_1)...(T - a_n)$. Prendendo gli a_i in $\overline{\mathbb{Q}}$, otteniamo tutti i polinomi monici (e quindi tutti i polinomi a meno di una costante) a coefficienti in $\overline{\mathbb{Q}}$, in particolare tutti i polinomi a coefficienti razionali.

Se il polinomio ottenuto specializzando gli x_i in a_i è a coefficienti in $\mathbb{Q}$: $p(T) := P(\underline{a}, T) \in \mathbb{Q}[T]$, allora $\mathbb{Q}(e_i(\underline{a})) = \mathbb{Q}$ e $\mathbb{Q}(a_1, ..., a_n) = L$ è il campo di spezzamento di $p(T)$. Se gli a_i sono *sufficientemente generali* li possiamo pensare come delle variabili e, per quanto abbiamo visto prima, è lecito aspettarsi che si avrà $Gal_{\mathbb{Q}}(p) = S_n$ (in particolare questo implica che $p(T)$ è irriducibile); cioè il gruppo di Galois di un polinomio $p(T) \in \mathbb{Q}[T]$, di grado n, "sufficientemente generale", è S_n.

Questi argomenti non costituiscono una dimostrazione, rimane qualcosa da dimostrare ed è proprio quello che ha fatto Hilbert col suo famoso teorema di irriducibilità (1892):

Teorema 4.14. (Teorema di irriducibilità di Hilbert)
Sia k un'estensione finita di $\mathbb{Q}$ (eventualmente $k = \mathbb{Q}$). Sia $f(T_1, ..., T_n, X) \in k[T_1, ..., T_n, X]$ un polinomio irriducibile su k. Esistono infiniti $(b_1, ..., b_n) \in k^n$ tali che la specializzazione $f(\underline{b}, X)$ sia un polinomio irriducibile a coefficienti in k ($f(\underline{b}, X) \in k[X]$).

Inoltre si possono scegliere i b_i di modo che $Gal_{k(\underline{T})}(f(\underline{T}, X)) \simeq Gal_k(f(\underline{b}, X))$.

La parte difficile è la prima parte sull'irriducibilità. Vediamo come dimostrare che S_n è di Galois su $\mathbb{Q}$ usando solo l'irriducibilità di una generica specializzazione.

Corollario 4.15. *Per ogni $n \geq 2$, S_n è di Galois su $\mathbb{Q}$. Più precisamente per ogni $n \geq 2$ esiste $f(x) \in \mathbb{Q}[x]$, irriducibile, di grado n, con $Gal_{\mathbb{Q}}(f) = S_n$.*

Dimostrazione. Consideriamo come prima l'estensione:

$$L := \mathbb{Q}(x_1, ..., x_n)/\mathbb{Q}(e_1, ..., e_n) =: K$$

L'estensione è normale (L è il campo di spezzamento del polinomio $p(X) = \prod(X - x_i) = X^n - e_1X^{n-1} + ... + (-1)^n e_n$), quindi $L = K(x_1, ..., x_n)$. Sappiamo (risolvente di Galois) che per $(a_1, ..., a_n) \in \mathbb{Z}^n$ sufficientemente generale, $\alpha = a_1x_1 + ... + a_nx_n$ è un elemento primitivo di L/K. Sia $m(X) \in K[X]$ il suo polinomio minimo. Allora

$$m(X) = \prod_{\sigma \in S_n} (X - (a_1x_{\sigma(1)} + ... + a_nx_{\sigma(n)})) \tag{4.8}$$

Infatti $m(X)$ ha grado $[L : K] = \#(Gal(L/K)) = n!$. Osserviamo che i coefficienti di m sono dei polinomi (e non delle funzioni razionali) simmetrici negli x_i, cioè $m(X) \in \mathbb{Q}[\overline{e_1, ..., e_n}][X]$ (invece di $m(X) \in \mathbb{Q}(e_1, ..., e_n)[X]$).

Quindi $m(X) \in \mathbb{Q}[e_1, ..., e_n][X]$, cioè $m(e_1, ..., e_n, X) \in \mathbb{Q}[e_1, ..., e_n, X]$.

Il polinomio $m(T_1, ..., T_n, X) \in \mathbb{Q}[T_1, ..., T - n, X]$ è irriducibile su $\mathbb{Q}$.

Infatti se $m(\underline{T}, X) = g(\underline{T}, X)h(\underline{T}, X)$, allora questa fattorizzazione dovrebbe valere in $\mathbb{Q}(\underline{e})[X]$, ma m è irriducibile su $\mathbb{Q}(\underline{e})$ (è il polinomio minimo di α). Quindi uno dei fattori, diciamo g, ha grado zero in X. Siccome m è monico in X, $g \in \mathbb{Q}$ è una costante.

Per il teorema di Hilbert se $(b_1, ..., b_n) \in \mathbb{Q}^n$ è sufficientemente generale, $\tilde{m}(X) = m(\underline{b}, X) \in \mathbb{Q}[X]$ è irriducibile (di grado $n!$).

Sia $f(x) = x^n - b_1x^{n-1} + ... + (-1)^n b_n \in \mathbb{Q}[x]$ e siano $r_1, ..., r_n$ le sue radici in Ω. Abbiamo $b_i = e_i(r_1, ..., r_n)$.

Quindi

$$m(e_1(r_1, ..., r_n), ..., e_n(r_1, ..., r_n), X) = m(b_1, ..., b_n, X)$$
$$= \tilde{m}(X) = \prod_{\sigma \in S_n} (X - (a_1r_{\sigma(1)} + ... + a_nr_{\sigma(n)}))$$

(Abbiamo fatto: $x_i \to r_i$, $e_i = e_i(x_1, ..., x_n) \to e_i(r_1, ..., r_n) = b_i$, $a_1x_1 + ... + a_nx_n \to a_1r_1 + ... + a_nr_n$.)

Segue che $\tilde{\alpha} := a_1r_1 + ... + a_nr_n \in \mathbb{Q}(r_1, ..., r_n)$ è radice del polinomio irriducibile $\tilde{m}(X)$, di grado $n!$. Questo implica $[\mathbb{Q}(r_1, ..., r_n) : \mathbb{Q}] \geq n!$. Segue che $Gal_{\mathbb{Q}}(f) = S_n$ e questo, a sua volta, implica che $f(x)$ è irriducibile.

□

Osservazione 4.16. La dimostrazione di Hilbert non è effettiva, cioè non fornisce un polinomio $f(x) \in \mathbb{Q}[x]$ con $Gal_{\mathbb{Q}}(f) = S_n$.

Con lo stesso procedimento Hilbert ha mostrato che $\mathcal{A}_n$ è di Galois su $\mathbb{Q}$.

Il teorema di irriducibilità di Hilbert è tuttora alla base di alcuni degli approcci moderni più promettenti per affrontare il problema inverso di Galois.

4.3.2 Realizzazioni di S_n con il teorema di Dedekind.

Iniziamo con un lemma:

Lemma 4.17. *Sia $G \leq S_n$ un sotto gruppo transitivo. Se G contiene una trasposizione e un ciclo di lunghezza $(n-1)$, allora $G = S_n$.*

Dimostrazione. Cf Esercizio 79. □

Teorema 4.18. *Per ogni $n \geq 2$, S_n è di Galois su $\mathbb{Q}$.*

Dimostrazione. Possiamo assumere $n \geq 4$. Siano $f_1(x), f_2(x), f_3(x) \in \mathbb{Q}[x]$, monici, di grado n tali che:

- $\overline{f}_1(x) \in \mathbb{Z}_2[x]$ è irriducibile
- $\overline{f}_2(x) \in \mathbb{Z}_3[x]$ spezza come un prodotto di un fattore lineare e di un fattore irriducibile di grado $n-1$
- $\overline{f}_3(x) \in \mathbb{Z}_5[x]$ spezza come un prodotto di un fattore irriducibile di grado due e uno o due fattori irriducibili (distinti) di grado dispari

Sia:

$$f(x) = -15f_1(x) + 10f_2(x) + 6f_3(x) \in \mathbb{Z}[x]$$

Il polinomio $f(x)$ è monico di grado n. Inoltre $f(x)$ è irriducibile perché $\overline{f}_2(x)$ lo è. Quindi se $G = Gal_{\mathbb{Q}}(f)$, $G \leq S_n$ è transitivo. Per il teorema di Dedekind (Teorema 4.9), G contiene un $(n-1)$-ciclo (considerare $\overline{f}_2(x) \in \mathbb{Z}_3[x]$). Finalmente, considerando $\overline{f}_3(x) \in \mathbb{Z}_5[x]$, vediamo che G contiene ρ con $\rho = \tau\sigma$ o $\rho = \tau\sigma\alpha$, σ, α cicli di lunghezza dispari. Quindi $\tau \in G$ e si conclude con il Lemma 4.17. □

Osservazione 4.19. Anche questa dimostrazione non è effettiva. Inoltre, per essere perfetti, bisognerebbe giustificare il fatto che è sempre possibile trovare dei polinomi $f_i(x)$ soddisfacenti le richieste mod. $2, 3, 5$.

Per n dato, questo metodo permette però di trovare (specie con l'aiuto di un computer) dei polinomi con gruppo di Galois S_n.

Comunque sia abbiamo visto due (anzi tre tenendo conto del Teorema 4.6) modi per realizzare S_n su $\mathbb{Q}$. Siccome ogni gruppo finito può essere visto (in tanti modi) come un sotto gruppo di S_n, ci sono ancora speranze per il problema inverso!

Esercizi.

Esercizio 79 *Sia $G \leq S_n$.*

Mostrare che se G contiene tutte le trasposizioni (ik), $1 < k \leq n$, $k \neq i$, allora $G = S_n$.

Si tratta di mostrare che se G è transitivo, contiene un $(n-1)$-ciclo, ρ, e una trasposizione, τ, allora $G = S_n$.

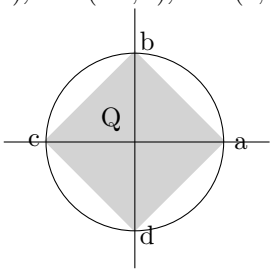
Possiamo assumere $\rho = (12...(n-1))$ e $\tau = (xy)$.

1. *Mostrare che G contiene una trasposizione che scambia n: $(kn) \in G, k < n$ (usare che G è transitivo)*
2. *Mostrare che le $\varphi_i = \rho^i(kn)\rho^{-i}$, $1 \leq i < n$ sono tutte le trasposizioni (an), $1 \leq a < n$ (per questo osservare che φ_i è una trasposizione e calcolare $\varphi_i(n)$)*
3. *Concludere che $G = S_n$.*

Esercizio 80 *Siano $f_1(x) = x^6 + x + 1$, $f_2(x) = (x+1)(x^5 + 2x + 1)$, $f_3(x) = (x+1)(x^2+x+1)(x^3+x+1)$. Finalmente sia $f(x) = 15f_1(x) + 10f_2(x) + 6f_3(x)$.*

1. *Mostrare che f è irriducibile su $\mathbb{Q}$ (considerare $f_1(x) \pmod 2$)*
2. *Mostrare che $Gal_{\mathbb{Q}}(f)$ contiene un 5-ciclo (considerare $f_2(x) \pmod 3$)*
3. *Concludere che $Gal_{\mathbb{Q}}(f) = S_6$ (considerare $f_3(x) \pmod 5$).*

Esercizio 81 *Sia nel piano il quadrato Q di vertici i punti $a = (1, 0)$, $b = (0, 1)$, $c = (-1, 0)$, $d = (0, -1)$.*



1. *Dimostrare che se $p \in Q$, $p \notin \{a, b, c, d\}$, allora $d(O, p) < 1$ (O è l'origine)*
2. *Si ricorda che un'isometria vettoriale del piano e una rotazione di centro l'origine (isometrie positive, $\det = 1$), oppure una riflessione ortogonale rispetto ad una retta passante per l'origine (isometrie negative, $\det = -1$). Sia $D_4 = \{g \mid g$ è un'isometria vettoriale del piano tale che $g(Q) = Q\}$. Mostrare che D_4 è un gruppo.*
3. *Mostrare che se $g \in D_4$ allora g manda un vertice di Q su un vertice (quindi g induce una permutazione di $\{a, b, c, d\}$); inoltre vertici adiacenti vanno mandati in vertici adiacenti.*
4. *Sia $\rho \in D_4$ una rotazione, mostrare che $\rho = r^i$ $(1 \leq i \leq 4)$ dove r è la rotazione di angolo $\pi/2$.*

5. *Mostrare che D_4 ha otto elementi, quattro rotazioni e quattro simmetrie ortogonali (di cui si determineranno gli assi).*
6. *Concludere che $D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$ dove s è una simmetria. In particolare D_4 è un gruppo di ordine 8, non abeliano con 4 elementi di ordine due (cf Esercizio 73).*
7. *Osservare che $D_4 \leq Sym\{a, b, c, d\} \simeq S_4$ è transitivo.*

Nota: *Più generalmente se indichiamo con D_n il gruppo delle simmetrie di un poligono regolare con n lati, allora D_n è generato da due elementi r, s, con le relazioni $r^n = 1$, $s^2 = 1$, $srs = r^{-1}$; D_n ha $2n$ elementi ed ogni elemento si scrive r^k o sr^k, $0 \leq k \leq n-1$.*

Esercizio 82 *Le possibili strutture cicliche (decomposizioni in cicli disgiunti) in S_4 sono: (ab), $(ab)(cd)$, (abc), $(abcd)$.*

Mostrare che ci sono: 6 trasposizioni, 3 doppie trasposizioni, 8 tricicli e 6 quattro cicli ($6 + 3 + 8 + 6 + 1 = 24$).

Esercizio 83 *Sia $G \leq S_4$ un sotto gruppo transitivo.*

1. *Mostrare che $\#(G) \in \{4, 8, 12, 24\}$*
2. *Nel seguito si assume $\#(G) = 8$. Mostrare che G contiene almeno due trasposizioni, τ_1, τ_2 (usare l'equazione delle classi $\#(G) = \#(G_x).\#(O(x))$). Mostrare che τ_1 e τ_2 sono disgiunte.*
3. *Possiamo quindi assumere che $\tau_1 = (12)$ e $\tau_2 = (34)$ sono in G. Mostrare che G contiene un 4-ciclo, ρ (usare l'Esercizio 73 e l'Esercizio 5.2 del Cap. III della prima parte)*
4. *Modulo gli inversi ci sono tre 4-cicli: $\rho_1 = (1234)$, $\rho_2 = (1243)$, $\rho_3 = (1324)$. Se $\rho^2 \neq \tau_1\tau_2$, allora $\rho = \rho_1$ o $\rho = \rho_2$ (considerare ρ_i^2). Ma questo non è possibile (considerare $\tau_1\rho$). In conclusione $\rho^2 = \tau_1\tau_2$ e $\rho = (1324)$*
5. *Concludere che $G = \{1, \tau_1, \tau_2, \rho, \rho^2, \rho^3, \tau_1\rho, \rho\tau_1\}$ e che $G \simeq D_4$ (cf Esercizio 81).*

Nota: *La dimostrazione può essere sensibilmente semplificata se si sa che ci sono solo due gruppi di ordine 8 non abeliani: $\mathbb{H}_8$ e D_4; $\mathbb{H}_8$ ha un unico elemento di ordine due mentre D_4 ne ha quattro.*

Esercizio 84 *Sia $G \leq S_4$ un sotto gruppo transitivo.*

1. *Se $\#(G) = 4$, dalla classificazione dei gruppi di ordine quattro $G \simeq \mathbb{Z}_4$ o $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. Mostrare che entrambi i casi sono possibili*
2. *Se $\#(G) = 12$, mostrare che $G \simeq \mathcal{A}_4$*

In conclusione G è isomorfo ad uno dei seguenti gruppi: $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, D_4, $\mathcal{A}_4$, S_4.

4.4 Il problema inverso per i gruppi abeliani.

Il risultato principale di questa sezione è il seguente:

Teorema 4.20. *Se G è un gruppo abeliano finito esiste un'estensione normale $L/\mathbb{Q}$ tale che $Gal(L/\mathbb{Q}) \simeq G$.*

La dimostrazione usa vari ingredienti:

Teorema 4.21. (Classificazione dei gruppi abeliani)
Ogni gruppo abeliano, G, è isomorfo a un prodotto diretto di gruppi ciclici:

$$G \simeq \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_s}$$

Avremo anche bisogno del teorema della progressione aritmetica di Dirichlet:

Teorema 4.22. (Dirichlet)
Siano a, b due interi primi tra di loro, allora esistono infiniti primi p, tali che: $p = a + nb$ con $n \in \mathbb{N}$ (cioè: $p \equiv a \ (mod\ b)$).

La dimostrazione di questo teorema è piuttosto difficile e usa strumenti della teoria analitica dei numeri.

Finalmente ricordiamo:

Teorema 4.23. (Teorema cinese del resto)
Sia $n = \prod_{i=1}^{s} n_i$ con $(n_i, n_j) = 1$ se $i \neq j$. Allora dati $a_1, ..., a_s \in \mathbb{Z}$, $\exists! x \in \mathbb{Z}_n$ tale che $x \equiv a_i (mod\ \ n_i)$, $\forall i$. In particolare:

$$(\mathbb{Z}_n)^* \simeq (\mathbb{Z}_{n_1})^* \times ... \times (\mathbb{Z}_{n_s})^*$$

Nella prima parte (Cap. 3, Proposizione 3.13) abbiamo dimostrato:

Proposizione 4.24. *Sia ζ una radice primitiva N-esima dell'unità, allora:*

$$Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq (\mathbb{Z}_N)^*$$

dove $(\mathbb{Z}_N)^* = U_N$ indica il gruppo moltiplicativo degli elementi invertibili di $\mathbb{Z}_N$.

Osservazione 4.25. Se $\mathbb{F}_p = \mathbb{Z}_p$ il gruppo moltiplicativo $\mathbb{F}_p^\times = (\mathbb{Z}_p)^*$ è isomorfo al gruppo additivo $\mathbb{Z}_{p-1}$:

$$(\mathbb{F}_p^*, \cdot) \simeq (\mathbb{Z}_{p-1}, +)$$

Con tutto questo armamentario siamo pronti per la dimostrazione del teorema.

Lemma 4.26. *Sia G un gruppo abeliano finito allora esiste N e un morfismo suriettivo:*

$$(\mathbb{Z}_N)^* \to G \to 1$$

Dimostrazione. (a) Iniziamo con il caso $G = \mathbb{Z}_n$. Per il Teorema di Dirichlet (4.22), esiste un numero primo p tale che $p \equiv 1$ $(mod\ n)$ (applicare il Teorema con $a = 1, b = n$). Quindi $p - 1 \equiv 0$ $(mod\ n)$ cioè $n \mid p - 1$. Segue che $(p-1)\mathbb{Z}$ è un sottogruppo (normale) di $n\mathbb{Z}$. Quindi:

$$\frac{\mathbb{Z}/(p-1)\mathbb{Z}}{n\mathbb{Z}/(p-1)\mathbb{Z}} \simeq \mathbb{Z}/n\mathbb{Z} =: \mathbb{Z}_n$$

Quindi $\mathbb{Z}_{p-1}$ surietta $\mathbb{Z}_n$. Pertanto (Osservazione 4.25): $(\mathbb{Z}_p)^* \to \mathbb{Z}_n \to 1$.

(b) Sia adesso G un gruppo abeliano finito qualsiasi. Per il Teorema 4.21 $G \simeq \prod \mathbb{Z}_{n_i}$. Per il passo (a): $\forall n_i, \exists p_i$, p_i primo tale che $(\mathbb{Z}_{p_i})^* \to \mathbb{Z}_{n_i} \to 1$. Inoltre possiamo assumere $p_i \neq p_j$ perché nel Teorema 4.22 ci sono infiniti primi tali che: $p \equiv 1$ $(mod\ n)$.

Sia $N = \prod p_i$. Dal Teorema cinese del resto (4.23) $(\mathbb{Z}_N)^* \simeq \prod (\mathbb{Z}_{p_i})^*$. Abbiamo quindi:

$$(\mathbb{Z}_N)^* \simeq \prod (\mathbb{Z}_{p_i})^* \to \prod \mathbb{Z}_{n_i} \simeq G \to 1$$

□

Finalmente:

Dimostrazione (del Teorema 4.20).
Per il Lemma 4.26 esiste $\varphi : (\mathbb{Z}_N)^* \to G \to 1$. Sia ζ una radice primitiva N-esima dell'unità. Per la Proposizione 4.24: $Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq (\mathbb{Z}_N)^*$. Sia $H = Ker(\varphi)$; H è un sotto gruppo normale di $(\mathbb{Z}_N)^*$. Sia $K := \mathbb{Q}(\zeta)^H$, per la corrispondenza di Galois, $H = Gal(\mathbb{Q}(\zeta)/K)$, $K/\mathbb{Q}$ è normale e $Gal(K/\mathbb{Q}) \simeq (\mathbb{Z}_N)^*/H \simeq G$. □

Ricordiamo che un'estensione finita, normale $L/\mathbb{Q}$ si dice *abeliana* se $Gal(L/\mathbb{Q})$ è abeliano. Riguardo alle estensioni abeliane abbiamo:

Teorema 4.27. (Kronecker-Weber)
Ogni estensione abeliana è contenuta in un'estensione ciclotomica.

Questo teorema, la cui dimostrazione usa risultati avanzati di teoria algebrica dei numeri, segna l'inizio della *classfield theory* (teoria del campo di classe, théorie du corps de classe). Combinando il Teorema di Kronecker-Weber col Teorema 4.20 abbiamo:

Corollario 4.28. *Ogni gruppo abeliano finito è il gruppo di Galois di un'estensione normale contenuta in un'estensione ciclotomica.*

Le considerazioni precedenti sono utili anche per risolvere il problema inverso effettivo. Per esempio se $n = (p-1)/2$, p un numero primo dispari, abbiamo $(\mathbb{Z}_p)^* \to \mathbb{Z}_n \to 1$, il nucleo è $\mathbb{Z}_2$. Se ζ è una radice primitiva p-esima dell'unità abbiamo quindi: $\mathbb{Q} \subset L \subset \mathbb{Q}(\zeta)$ con $Gal(L/\mathbb{Q}) = \mathbb{Z}_n$. Il polinomio minimo di ζ è il polinomio ciclotomico $\Phi_p(x) = x^{p-1} + ... + x + 1 = \prod_{i=1}^{n-1}(x - \zeta^i)$, un attimo di riflessione ci fa indovinare che $L = \mathbb{Q}(\zeta + \overline{\zeta})$, dopodiché è tutto un divertimento trovare il polinomio minimo di $\zeta + \overline{\zeta}$, cioè un polinomio irriducibile su $\mathbb{Q}$ con gruppo di Galois $\mathbb{Z}_n$ e questo risolve il problema inverso effettivo per $\mathbb{Z}_n$ dove $n = (p-1)/2$ (vedere Esercizio 88).

Per quanto riguarda i gradi delle realizzazioni, la situazione è assai semplice:

Proposizione 4.29. *Sia G un gruppo abeliano di ordine n. Se $f(x) \in \mathbb{Q}[x]$ è un polinomio irriducibile con $Gal_{\mathbb{Q}}(f) = G$, allora* $\deg(f) = n$*; cioè ogni rappresentazione di G è massimale.*

Dimostrazione. Esercizio 71. □

—— .. ——

Esercizi.

Esercizio 85 *Sia K un campo quadratico (i.e. $[K:\mathbb{Q}]=2$).*

1. *Sia $\alpha \in K \setminus \mathbb{Q}$, mostrare che α è radice di un polinomio della forma $ax^2+bx+c \in \mathbb{Z}[x]$; inoltre questo polinomio è univocamente determinato se si richiede $(a,b,c)=1, a>0$*
2. *Concludere che $K=\mathbb{Q}(\sqrt{d})$ per un qualche $d \in \mathbb{Z}$ senza fattori quadrati, cioè $d=\pm 2^e p_1 p_2 ... p_r$ dove $0 \le e \le 1$ e dove i p_i sono dei numeri primi dispari distinti (osservare che $\sqrt{\frac{a}{b}} = \pm\sqrt{ab}/b$ e $\sqrt{a^2 b} = \pm a\sqrt{b}$).*
3. *Mostrare che se $\mathbb{Q}(\sqrt{d}) \neq \mathbb{Q}(\sqrt{t})$ e se d,t sono senza fattori quadrati, allora $\mathbb{Q}(\sqrt{d}) \cap \mathbb{Q}(\sqrt{t}) = \mathbb{Q}$ (quindi l'intero d è univocamente determinato da K).*

Esercizio 86 *Sia p un numero primo dispari e $\Phi_p(x) = x^{p-1} + ... + x + 1$ il p-esimo polinomio ciclotomico. Abbiamo:*

$$\frac{x^p-1}{x-1} = \Phi_p(x) = \prod_{i=1}^{p-1}(x-\xi^i) \tag{4.9}$$

Scopo dell'esercizio è di calcolare il discriminante di $\Phi_p(x)$ e di mostrare:

$$D(\xi) := \prod_{1\le i<j\le p-1}(\xi^i-\xi^j)^2 = (-1)^{(p-1)/2}p^{p-2}$$

1. *Calcolando le derivate in (4.9) per $x=\xi^j$, mostrare che*

$$\frac{-p\xi^{p-j}}{1-\xi^j} = \prod_{\substack{1\le i\le p-1\\ i\neq j}}(\xi^j-\xi^i)$$

2. *Dalla relazione (4.9) per $x=0$ viene $\prod_{i=1}^{p-1}\xi^i = \xi\xi^2...\xi^{p-1} = (-1)^{p-1}$; mentre per $x=1$ viene: $\prod_{i=1}^{p-1}(1-\xi^i)=p$*
3. *Concludere che:*

$$p^{p-2} = \prod_{j=1}^{p-1}\prod_{\substack{i=1\\ i\neq j}}^{p-1}(\xi^j-\xi^i)$$

Ci sono $(p-1)(p-2)$ fattori in questo prodotto; per metà dei fattori $i>j$ mentre per l'altra metà $i<j$, pertanto:

$$p^{p-2} = (-1)^{(p-1)(p-2)/2}\prod_{1\le i<j\le p-1}(\xi^i-\xi^j)^2$$

Dedurne la formula cercata.

Esercizio 87 (Il teorema di Kronecker-Weber per i campi quadratici)
Sia $K/\mathbb{Q}$ un campo quadratico. Abbiamo $K = \mathbb{Q}(\sqrt{d})$ dove $d = \pm 2^r p_1 ... p_m$ (cf Esercizio 85).

1. *Osservare che $K \subset \mathbb{Q}(i, \sqrt{2}, \sqrt{p_1}, ..., \sqrt{p_m})$*
2. *Osservare che i è una radice primitiva quarta dell'unità e che $(\xi_8 + \xi_8^{-1})^2 = 2$ dove ξ_8 è una radice primitiva ottava dell'unità. Concludere che $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\xi_8)$*
3. *Sia p un numero primo dispari. Mostrare che se $p \equiv 1 \pmod 4$, allora $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\xi_p)$, dove ξ_p è una radice primitiva p-esima dell'unità. Mentre se $p \equiv 3 \pmod 4$, $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(i, \xi_p)$ (usare l'Esercizio 86 e un esercizio della prima parte).*
4. *Concludere che*
$$K \subset \mathbb{Q}(\xi_8, \xi_{p_1}, ..., \xi_{p_m}) \subset \mathbb{Q}(\xi_t)$$
dove $t = 8p_1 ... p_m$ e dove ξ_t è una radice primitiva t-esima dell'unità.

Esercizio 88 *Sia p un numero primo dispari. Le radici di $\Phi_p(x)$ sono le radici primitive e sono: $\{\zeta, \zeta^2, ..., \zeta^{p-1}\}$ dove $\zeta = e^{\frac{2i\Pi}{p}}$. Le radici sono due a due coniugate: $\zeta^i . \zeta^{p-i} = 1$ implica $\zeta^{p-i} = (\zeta^i)^{-1} = \overline{\zeta^i} = \overline{\zeta}^i$. Quindi possiamo scrivere le $p-1$ radici primitive anche in questo modo (con $k = \frac{p-1}{2}$):*

$$\begin{array}{c} \zeta \ ; \ \overline{\zeta} = \zeta^{p-1} \\ \zeta^2 \ ; \ \overline{\zeta}^2 = \zeta^{p-2} \\ \vdots \qquad \vdots \\ \zeta^k \ ; \ \overline{\zeta}^k = \zeta^{k+1} \end{array}$$

Il coniugo ($z \to \overline{z}$) induce un $\mathbb{Q}$ automorfismo non banale, c, su $L = \mathbb{Q}(\zeta)$. Quindi $c \in G := Gal(L/\mathbb{Q}) \simeq \mathbb{Z}_{p-1}$.

1. *Sia $H = \{1, c\} \leq G$ e sia $K = L^H$. Si pone $k = (p-1)/2$ e $\theta_i = \zeta^i + \overline{\zeta}^i$, $1 \leq i \leq k$. Usando il fatto che ogni $\alpha \in L$ si scrive in modo unico come combinazione lineare a coefficienti in $\mathbb{Q}$ di $1, \zeta, ..., \zeta^k, ..., \overline{\zeta}^2$, mostrare che $K = \mathbb{Q}(\theta_2, ..., \theta_k)$*
2. *Mostrare che $\mathbb{Q}(\theta_2, ..., \theta_k) = \mathbb{Q}(\theta)$ ($\theta = \theta_1$)*
3. *Mostrare che $\mathbb{Q}(\theta)/\mathbb{Q}$ è normale con $Gal(\mathbb{Q}(\theta)/\mathbb{Q}) = \mathbb{Z}_k$*
4. *Mostrare che il polinomio minimo di θ è:*
$$P_k(x) = (x - \theta)(x - \theta_2)...(x - \theta_k)$$
5. *Calcolare $P_2(x)$.*
6. *Sia $P_k(x) = x^k + b_1 x^{k-1} + ... + b_k$. Confrontando le funzioni simmetriche elementari delle radici di $\Phi_p(x)$ con quelle delle radici di $P_k(x)$, mostrare che $b_1 = 1, \forall k$.*

Nota: *Con il procedimento suggerito è possibile stabilire una formula induttiva per calcolare i coefficienti di* $P_k(x)$. *Inoltre si può mostrare che* $P_k(x) \in \mathbb{Z}[x]$ *(infatti* ζ *è intero su* $\mathbb{Q}$ *perché radice di* $\Phi_p(x) \in \mathbb{Z}[x]$, *monico, irriducibile. Per lo stesso motivo anche* $\overline{\zeta}$ *è intero. Quindi* $\theta = \zeta + \overline{\zeta}$ *è intero, pertanto il suo polinomio minimo è a coefficienti interi).*

5

La classificazione dei gruppi finiti non è finita!

5.1 Il teorema di Jordan-Hölder.

Il teorema fondamentale dell'aritmetica dice che ogni intero n si scrive, in modo essenzialmente unico, come un prodotto di numeri primi. I numeri primi sono quindi gli atomi, i mattoni con i quali costruire tutti i numeri.

Cerchiamo un'analogia per i gruppi finiti. L'analogo della nozione di divisore ($d \mid n$) è quella di sotto gruppo *normale*, infatti se $H \leq G$, vogliamo che il quoziente G/H sia un gruppo (nello stesso modo in cui n/d è un intero).

Quindi l'analogo di un numero primo sarebbe un gruppo, G, i cui unici sotto gruppi normali sono quelli banali ($\{1\}$ e G).

Definizione 5.1. *Un gruppo G è* semplice *se i suoi unici sotto gruppi normali sono $\{1\}$ e G.*

Sia G un gruppo e sia $N \lhd G$ un sottogruppo normale massimale (cioè se $N \leq H \lhd G$, allora $H = N$ o $H = G$), allora G/N è semplice. Adesso si può ripetere il procedimento con N al posto di G, andando avanti così, alla fine avremo "smontato" (fattorizzato) G in gruppi semplici. Infatti l'analogo del teorema fondamentale dell'aritmetica é:

Teorema 5.2. (Jordan-Hölder)
Se G è un gruppo finito esiste una filtrazione

$$\{1\} = G_r \leq G_{r-1} \leq ... \leq G_1 \leq G_0 = G \tag{5.1}$$

tale che: $G_{i+1} \lhd G_i$ e G_i/G_{i+1} è semplice, $\forall i, 0 \leq i \leq r-1$.

Inoltre la famiglia di gruppi semplici così ottenuta ($S_i = G_{i-1}/G_i$) è unica modulo permutazioni.

Una filtrazione tipo (5.1) si chiama anche una *serie di composizione.*

Con questo teorema i gruppi semplici fanno la parte dei numeri primi. L'analogia tuttavia non è del tutto perfetta perché i G_i non sono "divisori" di G (i G_i non sono necessariamente sotto gruppi normali di G...).

Osserviamo che il teorema di Jordan-Hölder non è vero per i gruppi infiniti.

D'ora in poi, tranne menzione espressa del contrario, tutti i gruppi considerati sono **finiti**.

Supponiamo di conoscere tutti i gruppi semplici, è possibile con questa informazione ricostruire (i.e. classificare) tutti i gruppi?

Questo torna, grosso modo, a potere costruire tutte le serie di composizione (5.1) possibili conoscendo gli $S_i = G_{i-1}/G_i$. Il primo passo è facile: $G_r = \{1\}$, quindi $G_{r-1} = G_{r-1}/G_r = S_r$. Poi conoscendo $S_{r-1} = G_{r-2}/G_{r-1}$ e $G_{r-1} = S_r$, bisogna determinare G_{r-2}.

Il problema si può riassumere così: dati due gruppi H, K, con K semplice, trovare tutti i gruppi G tali che: $H \lhd G$, $G/H \simeq K$. Più generalmente questo significa che abbiamo un morfismo iniettivo: $i : H \to G$, un morfismo suriettivo $p : G \to K$, tali che $Ker(p) \simeq Im(i) \simeq H$.

Definizione 5.3. *Un complesso di gruppi è una successione:*

$$... \to G_n \stackrel{d_n}{\to} G_{n+1} \stackrel{d_{n+1}}{\to} G_{n+2} \stackrel{d_{n+2}}{\to} G_{n+3} \stackrel{d_{n+3}}{\to} ...$$

dove i G_i sono dei gruppi, i d_i dei morfismi tali che $d_{i+1} \circ d_i = 0, \forall i$, cioè $Im(d_i) \subset Ker(d_{i+1})$, $\forall i$.

Il complesso è esatto *in G_{n+1} se $Im(d_n) = Ker(d_{n+1})$.*

Definizione 5.4. *Una successione esatta (corta) di gruppi è un complesso*

$$1 \to H \stackrel{i}{\to} G \stackrel{p}{\to} K \to 1$$

esatto in H, G, K (1 indica il gruppo banale $\{1\}$).

Questo significa che: (i) i è iniettivo, (ii) $Im(i) \simeq Ker(p)$ e (iii) p è suriettivo. Segue che $G/i(H) \simeq K$, quindi $H \simeq i(H) \lhd G$ e, con un piccolo abuso, $G/H \simeq K$.

In questa situazione si dice che G è *un'estensione di H per K*.

Il nostro problema può essere riformulato nel modo seguente:

Problema 5.5. *(Problema delle estensioni)*
Dati due gruppi H, K con K semplice, classificare tutte le estensioni di H per K.

Più generalmente dati due gruppi qualsiasi, classificare le loro estensioni.

In teoria il problema ammette una risposta positiva: dati due gruppi è possibile determinare in modo sistematico tutte le loro estensioni (si tratta di fare tutte le possibili "tabelle" partendo da quelle dei due gruppi dati, Schreier). Purtroppo questo approccio, poco economico, non è di grande aiuto, sia dal punto di vista pratico che da quello teorico.

Comunque sia la strategia per classificare i gruppi finiti potrebbe essere:

- Classificare tutti i gruppi semplici
- Risovere in modo utile il problema dell'estensione (Problema 5.5).

Questa è, effettivamente, la strategia seguita dagli esperti nel campo.

—— .. ——

Esercizi.

Esercizio 89 *Sia G un gruppo di ordine 8 mostrare che la serie di composizione di Jordan-Hölder è della forma seguente:*

$$\{1\} = G_3 \lhd G_2 \lhd G_1 \lhd G_0 = G$$

con $G_i/G_{i-1} \simeq \mathbb{Z}_2$, $\forall i, 0 \leq i \leq 2$.

Questo esempio mostra che la sola conoscenza dei gruppi semplici e il teorema di Jordan-Hölder non sono sufficienti per concludere la classificazione.

Esercizio 90 *Una successione esatta di gruppi*

$$1 \to N \xrightarrow{f} G \xrightarrow{p} H \to 1$$

è spezzata *se esiste un diagramma commutativo:*

$$\begin{array}{ccccccccc} 1 \to & N & \xrightarrow{f} & G & \xrightarrow{p} & H & \to 1 \\ & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & \\ 1 \to & N & \xrightarrow{i} & N \times H & \xrightarrow{\pi} & H & \to 1 \end{array}$$

dove α, β e γ sono degli isomorfismi. In particolare $G \simeq N \times H$.

1. *Mostrare che la successione esatta*

$$1 \to N \xrightarrow{f} G \xrightarrow{p} H \to 1$$

   è spezzata se e solo se esiste $r : G \to N$ tale che $r \circ f = Id_N$ (si dice che r è una retrazione di f)
2. *Mostrare che se la successione è spezzata, allora esiste $s : H \to G$ tale che $p \circ s = Id_H$ (si dice che s è una sezione di p)*

Esercizio 91 *Sia $\rho = (123) \in S_3$ e sia $N = \langle \rho \rangle$.*

1. *Mostrare che $N \lhd S_3$*
2. *Sia (E) la successione esatta:*

$$1 \to N \xrightarrow{i} S_3 \xrightarrow{p} H \to 1$$

   dove i è l'inclusione e dove $S_3 \xrightarrow{p} H = S_3/N$ è la proiezione canonica.
   Mostrare che esiste una sezione di p cioè: $s : H \to S_3$ tale che $p \circ s = Id_H$
3. *Mostrare che (E) non è spezzata.*

Nota: *Si può mostrare che nella categoria* **Ab** *dei gruppi abeliani una successione esatta è spezzata se e solo se ammette una sezione (questo è vero più generalmente in ogni categoria abeliana, quindi in Mod_A, A anello commutativo).*

5.2 Gruppi semplici.

Iniziamo col fare qualche esempio di gruppi semplici.

5.2.1 Gruppi semplici abeliani

La classificazione dei gruppi semplici abeliani è semplice!

Proposizione 5.6. *Un gruppo abeliano, G, è semplice se e solo se $G \simeq \mathbb{Z}_p$ per qualche numero primo p.*

Dimostrazione. Esercizio 92. □

Nel caso non abeliano la questione non è così facile. Iniziamo col fare qualche esempio.

5.2.2 I gruppi alterni $\mathcal{A}_n$.

Abbiamo già visto che $\mathcal{A}_n$ non è risolubile se $n \geq 5$; in realtà vale qualcosa di più:

Teorema 5.7. *Per $n \geq 5$, $\mathcal{A}_n$ è semplice.*

Ci servono un paio di lemma:

Lemma 5.8. *Per $n \geq 3$ gli $n-2$ tre-cicli $\rho_k = (12k)$, $3 \leq k \leq n$ generano $\mathcal{A}_n$. (Cioè ogni $\sigma \in \mathcal{A}_n$ si scrive come un prodotto $h_1 ... h_i$ dove $h_i = \rho_{i_k}$ o $h_i = \rho_{i_k}^{-1}$, per ogni i).*

Dimostrazione. Abbiamo già visto (**??**) che ogni elemento di $\mathcal{A}_n$ si scrive come un prodotto di tre-cicli.

Per concludere basta usare le seguenti uguaglianze:

$(ijk) = (12i)(2jk)(12i)^{-1}$, $(2jk) = (12j)(12k)(12j)^{-1}$, $(1jk) = (12k)^{-1}(12j)(12k)$ □

Lemma 5.9. *Sia $H \lhd \mathcal{A}_n$ un sottogruppo normale, $n \geq 3$. Se H contiene un tre-ciclo allora $H = \mathcal{A}_n$.*

Dimostrazione. Dopo avere riordinato gli indici possiamo assumere $\rho = (123) \in H$. Quindi $\rho^{-1} = (132) \in H$ (perché H è un sottogruppo). Sia $\tau = (13)(3k)$. Siccome $H \lhd \mathcal{A}_n$ è un sottogruppo normale, $\tau^{-1}\rho^{-1}\tau = (12k) \in H$. Quindi H contiene tutti i ρ_k, ed essendo un sottogruppo, anche tutti gli inversi ρ_k^{-1}. Per il Lemma 5.8, $H \supset \mathcal{A}_n$, cioè $H = \mathcal{A}_n$. □

Lemma 5.10. *Sia $H \lhd \mathcal{A}_n$ un sottogruppo normale, $n \geq 5$. Se H contiene un prodotto di due trasposizioni, allora $H = \mathcal{A}_n$.*

Dimostrazione. Se le trasposizioni non sono disgiunte: $(ab)(bc) = (bca)$ e si conclude con il Lemma 5.9.
Sia $\alpha \in H$ prodotto di due trasposizioni disgiunte: $\alpha = (ab)(cd)$. Se $n \geq 5$, possiamo considerare $\tau = (abe)$. Siccome $H \lhd \mathcal{A}_n$: $\tau^{-1}\alpha\tau = (ae)(cd) \in H$. Quindi anche $\alpha^{-1}\tau^{-1}\alpha\tau \in H$. Ma $\alpha^{-1}\tau^{-1}\alpha\tau = (aeb)$. Quindi $(aeb) \in H$ e si conclude con il Lemma 5.9. □

Possiamo finalmente dimostrare il teorema:

Dimostrazione (del Teorema 5.7).

Sia $H \lhd \mathcal{A}_n$, con $\alpha \in H$, $\alpha \neq 1$. Per dimostrare il teorema dobbiamo mostrare che $H = \mathcal{A}_n$.

Sia $\alpha = \gamma_1\gamma_2...\gamma_t$ la decomposizione in cicli disgiunti ordinata in modo tale che $l(\gamma_1) \geq l(\gamma_2) \geq ... \geq l(\gamma_t)$.

(a) Supponiamo $l(\gamma_1) > 3$.

Quindi $\gamma_1 = (a_1...a_m)$ con $m > 3$. Sia $\rho = (a_1\, a_2\, a_3)$. Siccome $\rho \in \mathcal{A}_n$ e siccome $H \lhd \mathcal{A}_n$ è normale: $\rho^{-1}\alpha\rho \in H$, e quindi anche $\alpha^{-1}(\rho^{-1}\alpha\rho) \in H$. Abbiamo $\rho^{-1}\alpha\rho = (a_3\, a_1\, a_2\, a_4 \dots a_m)\gamma_2...\gamma_t$.

$$\alpha^{-1}\rho^{-1}\alpha\rho = \gamma_t^{-1}...\gamma_2^{-1}\gamma_1^{-1}(a_3\, a_1\, a_2\, a_4 \dots a_m)\gamma_2...\gamma_t$$

Siccome i cicli disgiunti commutano

$$\alpha^{-1}\rho^{-1}\alpha\rho = \gamma_1^{-1}(a_3\, a_1\, a_2\, a_4 \dots a_m)$$

$$\alpha^{-1}\rho^{-1}\alpha\rho = (a_m \dots a_1)(a_3\, a_1\, a_2\, a_4 \dots a_m)$$

$$\alpha^{-1}\rho^{-1}\alpha\rho = (a_2\, a_3\, a_m)$$

Si conclude con il Lemma 5.9.

(b) Supponiamo $l(\gamma_1) = l(\gamma_2) = 3$.

Quindi $\gamma_1 = (a_1\, a_2\, a_3)$, $\gamma_2 = (a_4\, a_5\, a_6)$. Sia $\rho = (a_2\, a_3\, a_4)$. Abbiamo:

$$\rho^{-1}\alpha\rho = \rho^{-1}(\gamma_1 \dots \gamma_t)\rho$$

Siccome ρ è disgiunto da $\gamma_3, ..., \gamma_t$:

$$\rho^{-1}\alpha\rho = \rho^{-1}(\gamma_1\, \gamma_2)\rho\, \gamma_3...\gamma_t$$

$$= \rho^{-1}(\gamma_1\, \rho\, \rho^{-1}\, \gamma_2)\rho\, \gamma_3...\gamma_t$$

$$= (\rho^{-1}\, \gamma_1\, \rho)\, (\rho^{-1}\, \gamma_2\, \rho)\, \gamma_3...\gamma_t$$

Adesso, come prima, $\alpha^{-1}\rho^{-1}\alpha\rho \in H$, abbiamo:

$$\alpha^{-1}\rho^{-1}\alpha\rho = (\gamma_t^{-1}...\gamma_2^{-1}\gamma_1^{-1})(\rho^{-1}\, \gamma_1\, \rho)\, (\rho^{-1}\, \gamma_2\, \rho)\, \gamma_3...\gamma_t$$

I cicli $\gamma_3, ..., \gamma_t$ sono disgiunti da ρ, γ_1, γ_2, quindi:

$$\alpha^{-1}\rho^{-1}\alpha\rho = (\gamma_2^{-1}\gamma_1^{-1})(\rho^{-1}\, \gamma_1\, \rho)\, (\rho^{-1}\, \gamma_2\, \rho)$$

$$= (a_1\, a_6\, a_2\, a_3\, a_4)$$

Quindi H contiene un ciclo di lunghezza > 3 e concludiamo con (a).

(c) Supponiamo $l(\gamma_1) = 3$ e $\gamma_2, ..., \gamma_t$ delle trasposizioni.

Quindi $\alpha = (a_1\, a_2\, a_3)\gamma_2...\gamma_t$. Abbiamo:

$$\alpha^2 = (a_1\, a_2\, a_3)\gamma_2...\gamma_t\,(a_1\, a_2\, a_3)\gamma_2...\gamma_t$$

Siccome i cicli sono disgiunti, commutano:

$$\alpha^2 = (a_1\, a_2\, a_3)^2\gamma_2^2...\gamma_t^2$$

Se γ_i è una trasposizione: $\gamma_i^2 = Id$, quindi:

$$\alpha^2 = (a_1\, a_2\, a_3)^2 = (a_1\, a_3\, a_2)$$

e si conclude con il Lemma 5.9.

(d) L'ultima possibilità è che α sia il prodotto di un numero pari di trasposizioni disgiunte:

$$\alpha = (a_1\, a_2)(a_3\, a_4)\gamma_3...\gamma_t$$

Sia $\rho = (a_2\, a_3\, a_4)$, abbiamo:

$$\rho^{-1}\alpha\rho = (a_4\, a_3\, a_2)(a_1\, a_2)(a_3\, a_4)\gamma_3...\gamma_t(a_2\, a_3\, a_4)$$

$$= (a_4\, a_3\, a_2)(a_1\, a_2)(a_3\, a_4)(a_2\, a_3\, a_4)\gamma_3...\gamma_t$$

Quindi:

$$\alpha^{-1}\rho^{-1}\alpha\rho = \gamma_t^{-1}...\gamma_3^{-1}(a_3\, a_4)(a_1\, a_2)(a_4\, a_3\, a_2)(a_1\, a_2)(a_3\, a_4)(a_2\, a_3\, a_4)\gamma_3...\gamma_t$$

$$= (a_3\, a_4)(a_1\, a_2)(a_4\, a_3\, a_2)(a_1\, a_2)(a_3\, a_4)(a_2\, a_3\, a_4)$$

$$= (a_1\, a_4)(a_2\, a_3)$$

e si conclude con il Lemma 5.10. □

Si può mostrare (cf Esercizio 113, Esercizio 114) che $\mathcal{A}_5$ è il più piccolo gruppo semplice, non abeliano (cioè ogni gruppo non abeliano di ordine < 60 non è semplice).

5.2.3 I gruppi di tipo Lie.

Sia k un campo qualsiasi e sia E un k-spazio vettoriale di dimensione n. Si nota con $Gl(E)$ il *gruppo lineare* di E: $Gl(E) = \{f \in End(E) \mid \det(f) \neq 0\}$. Il gruppo *speciale lineare*, $Sl(E)$ è definito da $Sl(E) = \{f \in Gl(E) \mid \det(f) = 1\}$. Ovviamente $Sl(E) \lhd Gl(E)$ perché $Sl(E) = Ker(\det)$ dove $\det : Gl(E) \to k^*$.

Prendendo una base di E, i gruppi $Gl(E), Sl(E)$ possono essere visti come gruppi di matrici: $Gl(n,k), Sl(n.k) \leq (M_n(k), .)$.

Si ricorda che se G è un gruppo, il *centro* di G, $Z(G)$ è definito da: $Z(G) = \{h \in G \mid hg = gh, \forall g \in G\}$. Abbiamo $Z(G) \lhd G$ e quindi possiamo considerare il gruppo $G/Z(G)$.

Un classico esercizio di algebra lineare mostra che $Z(Gl(E)) \simeq k^*$ (e quindi $Z(Sl(E)) \simeq \mu_n$).

Il gruppo *lineare proiettivo* è $PGl(E) := Gl(E)/Z(Gl(E))$, cioè $PGl(E) = Gl(E)/k^*$ e il gruppo *speciale lineare proiettivo* è $PSl(E) = Sl(E)/Z(Sl(E))$.

Il gruppo $PGl(E)$ è il gruppo degli automorfismi lineari dello spazio proiettivo $\mathbb{P}(E)$ (osservare che $f(\lambda v) = (\lambda f)(v)$). Dal punto di vista matriciale un elemento di $PGl(n,k)$ è una matrice invertibile, definita a meno di una costante non nulla. Invece un elemento di $PSl(n,k)$ è una matrice con determinante uguale a uno, definita a meno della moltiplicazione per una radice n-esima dell'unità.

Considerazioni di algebra lineare permettono di dimostrare:

Teorema 5.11. *Il gruppo $PSl(n,k)$ è semplice tranne che nei due casi seguenti: $n = 2$, $k = \mathbb{F}_2$; $n = 2$, $k = \mathbb{F}_3$.*

Il caso $n \geq 3$ è l'oggetto degli Esercizi 97–104.

Ovviamente se k è infinito tutti i gruppi $Gl(E), Sl(E), PGl(E), PSl(E)$ sono infiniti, ma se k è un campo finito, i gruppi in questione sono finiti. Otteniamo così una nuova famiglia infinita di gruppi (finiti) semplici: $PSl(n, \mathbb{F}_p)$, $n \geq 3$, p un numero primo.

I gruppi $Gl(E), Sl(E)$ sono gruppi *classici* (terminologia introdotta da Herman Weyl [20]), altri gruppi classici sono il gruppo delle matrici ortogonali o più generalmente i gruppi che preservono una forma (bilineare simmetrica, anti-simmetrica (gruppi simpletici), sesquilineari hermitiane ecc...).

Esiste un procedimento uniforme che permette di associare ad ogni gruppo classico, G, un gruppo (quasi sempre) semplice: se G' è il sotto gruppo dei commutatori ($G' = \{xyx^{-1}y^{-1}\}$), allora $G'/Z(G')$ è, in generale, semplice. Ci sono eccezioni (in dimensione bassa, o in caratteristica positiva per valori bassi di p, ...), ma in generale funziona!

I gruppi classici sono esempi di gruppi di Lie. Nel 1955 Claude Chevalley ([4]) ha introdotto un metodo per costruire famiglie infinite di gruppi semplici (*gruppi di Chevalley*) associati ad algebre di Lie. Considerando campi finiti si ottengono famiglie infinite di gruppi (finiti) semplici. Questi gruppi vengono chiamati "di tipo Lie".

Esercizi.

Esercizio 92 *Dimostrare, senza usare la classificazione, che ogni gruppo finito abeliano semplice è della forma* $\mathbb{Z}_p$.

Esercizio 93 *Sia* G *un gruppo di ordine* n *e sia* k *un campo qualsiasi. Mostrare che* G *è isomorfo a un sotto gruppo di* $Gl(n,k)$ *(se* $\sigma \in S_n$*, considerare la matrice di permutazione* $I(\sigma)$ *ottenuta permutando le colonne della matrice identità* I_n *e usare il teorema di Cayley).*

Esercizio 94 *Sia* G *un gruppo finito di ordine* n*. Si assume che per ogni divisore* d *di* n*, l'insieme* $\{x \in G \mid x^d = 1\}$ *ha al più* d *elementi.*

1. *Mostrare che se* $d \mid n$*, allora* G *ha* 0 *o* $\varphi(d)$ *elementi di ordine* d
2. *Concludere che* G *è ciclico (mostrare che esiste un elemento di ordine* n*, usare l'Esercizio 51)*
3. *Concludere che se* k *è un campo qualsiasi e se* G *è un sotto gruppo* finito *del gruppo moltiplicativo* k^**, allora* G *è ciclico. In particolare* $\mathbb{F}_q^\times \simeq \mathbb{Z}_{q-1}$ *(*$q = p^n$*,* p *primo) e ogni* $x \in \mathbb{F}_q^\times$ *verifica* $x^{q-1} = 1$.

Esercizio 95 *Sia* $q = p^n$ *dove* p *è un numero primo.*

1. *Mostrare che* $\#(Gl(n,\mathbb{F}_q)) = (q^n - 1)(q^n - q)...(q^n - q^{n-1}))$ *(considerare i vettori colona* $C_1, ..., C_n$*:* C_1 *può essere un vettore qualsiasi, tranne il vettore nullo;* C_2 *è un vettore qualsiasi tale che* $C_2 \notin \langle C_1 \rangle$*, ecc...)*
2. *Dedurne che* $\#(Sl(n,\mathbb{F}_q)) = (q^n - 1)(q^n - q)...(q^n - q^{n-2})q^{n-1} =: N$ *(usare la successione esatta:* $1 \to Sl(n,\mathbb{F}_q) \to Gl(n,\mathbb{F}_q) \overset{\det}{\to} \mathbb{F}_q^\times \to 1$*)*
3. *Mostrare che* $\#(PGl(n,\mathbb{F}_q)) = N$ *(usare la definizione di* $PGl(E)$*)*
4. *Sia* $\mu_n = \{x \in \mathbb{F}_q \mid x^n = 1\}$*, l'insieme delle radici* n*-esime dell'unità. Sia* $d = (n, q-1)$*. Mostrare che* $\mu_n = \mu_d$ *(usare l'Esercizio 94). Concludere che* $\#(\mu_n) = d$ *(osservare che* $X^d - 1$ *divide* $X^{q-1} - 1$ *e usare l'Esercizio 94)*
5. *Usando il punto precedente e la definizione di* $PSl(E)$ *mostrare che* $\#(PSl(n,\mathbb{F}_q)) = N/d$*, dove* $d = (n, q-1)$.

Esercizio 96

1. *Mostrare che* $\mathcal{A}_n$ *è l'unico sotto gruppo di indice due di* S_n *(considerare* $H \cap \mathcal{A}_n$*,* H *un altro eventuale sotto gruppo di indice due; se* $n \geq 5$ *usare il fatto che* $\mathcal{A}_n$ *è semplice, se* $n < 5$ *l'avete già fatto! (Esercizio 84))*
2. *Mostrare che* $\mathbb{P}(\mathbb{F}_q^2) = \mathbb{P}^1_{\mathbb{F}_q}$ *(retta proiettiva su* $\mathbb{F}_q$*) ha* $q+1$ *elementi*
3. $PGl(2,k)$ *è il gruppo delle trasformazioni lineari di* $\mathbb{P}^1_k$*: se* $x = \langle v \rangle \in \mathbb{P}^1$ *e* $\varphi = \langle f \rangle \in PGl(2,k)$*,* $\varphi(x) = \langle f(v) \rangle$*. Mostrare che esiste un morfismo iniettivo di gruppi:* $F : PGl(2,\mathbb{F}_q) \to S_{q+1}$
4. *Mostrare che i quattro gruppi* $Gl(2,\mathbb{F}_2)$*,* $Sl(2,\mathbb{F}_2)$*,* $PGl(2,\mathbb{F}_2)$*,* $PSl(2,\mathbb{F}_2)$ *sono tutti isomorfi a* S_3

5. *Mostrare che* $PGl(2,\mathbb{F}_3) \simeq S_4$ *e* $PSl(2,\mathbb{F}_3) \simeq \mathcal{A}_4$.

Esercizio 97 (Transvezioni, dilatazioni)
Sia E *un* k*-spazio vettoriale di dimensione* n *e* $f : E \to E$ *un endomorfismo,* $f \neq Id$*, tale che esista un iperpiano* H *tale che* $f|H = Id_H$.

(i) Sono equivalenti:

1. $\det(f) = \lambda \neq 1$
2. f *è diagonalizzabile*
3. *La retta* $D := Im(Id - f)$ *non è contenuta in* H

In questo caso si dice che f *è una* dilatazione *di iperpiano* H*, retta* D *e rapporto* λ.

(ii) Mostrare che una dilatazione f *è univocamente determinata da* H*,* D*,* λ.

(iii) Sono equivalenti:

1. $\det(f) = 1$
2. f *non è diagonalizzabile*
3. $D := Im(Id - f) \subset H$
4. $\exists w \in H$*,* $w \neq 0$ *e* $\varphi \in E^*$ *con* $Ker(\varphi) = H$ *tali che:* $f(v) = v + \varphi(v).w$*,* $\forall v \in E$
5. *Esiste una base* B *tale* $mat(f; B, B) = \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ \vdots & \ddots & & & \vdots \\ \vdots & & \ddots & & 0 \\ \vdots & & & \ddots & 1 \\ 0 & \cdots & \cdots & \cdots & 1 \end{pmatrix}$.

In questo caso si dice che f *è una* transvezione *(*transvection *in inglese e francese) di iperpiano* H *e retta* D.

(iv) Sia $n = 2$ *e* $B = (e_1, e_2)$ *una base di* E*. Determinare tutte le transvezioni con* $H = D = \langle e_1 \rangle$*. Concludere che una transvezione non è univocamente determinata da* H *e* D.

(v) Sia $\varphi \in E^*$*,* $\varphi \neq 0$ *e sia* $w \in Ker(\varphi)$*,* $w \neq 0$*, osservare che* φ *e* w *determinano una transvezione* $f = \tau(\varphi, w)$ *tramite* $f(v) = v + \varphi(v).w, \forall v \in E$*;* $\tau(\varphi, w)$ *è una transvezione di iperpiano* $H = Ker(\varphi)$*, retta* $D = \langle w \rangle$*. Viceversa se* $f = \tau(\varphi, w)$ *è una transvezione,* f non *determina* (φ, w).

Esercizio 98 (Transvezioni: inversi, prodotti)
Sia E *un* k*-spazio vettoriale.*

1. *Mostrare che se* $f \in End(E)$ *è una transvezione, allora anche* f^{-1} *è una transvezione (con lo stesso iperpiano e la stessa retta).*
2. *Mostrare che se* f, g *sono due transvezioni di iperpiano* H*, allora* $f \circ g = Id$ *oppure* $f \circ g$ *è una transvezione di iperpiano* H.
3. *Mostrare che, in generale, il prodotto di due transvezioni* non *è una transvezione.*

Esercizio 99 (Centro di $Gl(E), Sl(E)$)
Scopo di questo esercizio è di determinare il centro di $Gl(E)$ e di $Sl(E) = \{g \in Gl(E) \mid \det(g) = 1\}$. (Vedere Esercizio 100 per una dimostrazione alternativa).

Sia E un k-spazio vettoriale di dimensione n.

1. *Sia $f \in End(E)$ tale che: $\forall v \in E$, v e $f(v)$ siano dipendenti. Mostrare che f è un'omotetia (cioè $f = \lambda.Id$ per qualche $\lambda \in k$).*
2. *Sia $f = \tau(\varphi, w)$ una transvezione (cf Esercizio 97) e $g \in Gl(E)$ un automorfismo di E. Mostrare che gfg^{-1} è una transvezione di iperpiano $g(H)$, retta $g(D)$ ($H = Ker(\varphi), D = \langle w \rangle$).*
3. *Sia G un gruppo. Mostrare che $Z(G) = \{x \in G \mid xy = yx, \forall y \in G\}$ è un sottogruppo* normale *di G. Il sottogruppo $Z(G)$ si chiama il* centro *di G.*
4. *Mostrare che $Sl(E)$ è un sottogruppo normale di $Gl(E)$ (considerare il determinante).*
5. *Mostrare che se $g \in Gl(E)$ commuta con ogni transvezione, allora g è un'omotetia (usare 1. e 2.). Dedurne che $Z(Gl(E)) \simeq k^*$ e $Z(Sl(E)) \simeq \mu_n = \{z \in k \mid z^n = 1\}$ (gruppo moltiplicativo delle radici n-esime dell'unità).*

Esercizio 100 (Centro di $Gl(E), Sl(E)$, take two)
Una dimostrazione diretta, più semplice (ma meno istruttiva) della determinazione di $Z(Gl(E)), Z(Sl(E))$.

Sia E un k-spazio vettoriale di dimensione n.

1. *Sia $f \in End(E)$ tale che $f \circ g = g \circ f, \forall g \in Sl(E)$. Mostrare che $\forall v \in E, v$ e $f(v)$ sono linearmente dipendenti (se $f(w) = v$ con w, v linearmente indipendenti, considerare g, h, automorfismi opportuni tali che: $g(w) = w + v$, $g(v) = -w$; $h(w) = w + v$, $h(v) = v$).*
2. *Concludere che ogni elemento di $Z(Gl(E))$ (risp. $Z(Sl(E))$) è un'omotetia (cf Esercizio 99 (i)).*

Esercizio 101 *Sia E un k-spazio vettoriale di dimensione n.*

(i) Siano $u, v \in E \setminus \{0\}$.

1. *Se u, v sono linearmente indipendenti, mostrare che esiste una transvezione, f, tale che $f(u) = v$.*
2. *Se u, v sono linearmente dipendenti, mostrare che esistono due transvezioni, f, g, tali che $(f \circ g)(u) = v$.*

(ii) Siano H_1, H_2 due iperpiani distinti di E e sia $v \notin H_1 \cup H_2$. Mostrare che esiste una transvezione, f, tale che $f(v) = v$, $f(H_1) = H_2$.

Esercizio 102 (Generatori di $Sl(E), Gl(E)$)
Sia E un k-spazio vettoriale di dimensione n.

1. *Mostrare che ogni elemento di $Sl(E)$ si scrive come un prodotto di transvezioni (usare l'Esercizio 101).*
2. *Concludere che le dilatazioni e le transvezioni generano $Gl(E)$.*

Esercizio 103 (Transvezioni e coniugo, $n \geq 3$)
Sia E un k-spazio vettoriale di dimensione n e siano $f, g \in Sl(E)$ due transvezioni.

1. *Usare l'Esercizio 97, (iii), (5) e concludere che f e g sono coniugati in $Gl(E)$ (i.e. $\exists u \in Gl(E)$ tale che $ugu^{-1} = f$).*
2. *Sia $\lambda \in k$, $\lambda \neq 0$. Mostrare che se $n \geq 3$, esiste $v \in Gl(E)$ con $\det(v) = 1/\lambda$ tale che $vgv^{-1} = g$ (considerare $mat(g; B, B)$ per una base B opportuna di E, cf Esercizio 97, (iii), (5)).*
3. *Concludere che se $n \geq 3$, due transvezioni f e g sono coniugate in $Sl(E)$ (i.e $\exists u \in Sl(E)$ tale che $ugu^{-1} = f$).*

Esercizio 104 (Semplicità di $PSl(E), dim(E) \geq 3$)
Abbiamo visto (Esercizio 99, 100) che il centro, Z, di $Sl(E)$ è costituito dalle omotetie in $Sl(E)$.

Sia G un sottogruppo di $Sl(E)$ contenente Z. Scopo dell'esercizio è di mostrare, <u>sotto l'ipotesi</u> $\dim(E) \geq 3$, che se G è normale*, allora $G = Sl(E)$.*

1. *Osservare che G essendo normale, se $g \in G$ e $f \in Sl(E)$, allora $gfg^{-1}f^{-1} \in G$.*
2. *L'idea adesso è di usare 1. per mostrare che G contiene <u>una</u> transvezione. Infatti mostrare (usando Esercizio 102 e Esercizio 103: è qui che interviene l'ipotesi $\dim(E) \geq 3$) che se G contiene una transvezione, allora $G = Sl(E)$.*
3. *Sia $g \in G \setminus Z$. Siccome g non è un'omotetia esistono u, v linearmente indipendenti tali che $g(u) = v$. Sia t una transvezione di retta $\langle u \rangle$ e poniamo: $f = gtg^{-1}t^{-1}$. Mostrare:*
   a) *$f \in G$ e $f \neq Id$ (osservare che gtg^{-1} è una transvezione di retta $\langle g(u) = v \rangle$, cf Esercizio 99, (ii))*
   b) *Sia H un iperpiano contenente $\langle u, v \rangle$ (esistono tali iperpiani perchè $\dim(E) \geq 3$). Mostrare che: $\forall x \in E$, $f(x) - x \in H$*
   c) *Concludere che $f(H) = H$.*
4. *Supponiamo che esista una transvezione, h, d'iperpiano H che non commuta con f ($hf \neq fh$). Sia $v := fhf^{-1}h^{-1}$. Mostrare che $v \in G$, $v \neq Id$, v è una transvezione di iperpiano H (considerare fhf^{-1} e h^{-1} e usare l'Esercizio 98).*
5. *Finalmente supponiamo invece che f commuti con ogni transvezione di iperpiano H. Mostrare che f è una transvezione (d'iperpiano H).*
6. *Abbiamo quindi mostrato che ogni sottogruppo normale di $Sl(E)$ contenente Z è uguale a Z o a $Sl(E)$. Concldere che sotto l'ipotesi $\dim(E) \geq 3$, $PSl(E)$ è un gruppo* semplice.

5.3 Il teorema enorme.

Finora abbiamo visto gruppi semplici organizzati in famiglie, ma già nel 1861 si conoscevano altri esempi "isolati" di gruppi semplici.

5.3.1 Rappresentazioni transitive e gruppi di Mathieu.

Abbiamo visto (teorema di Cayley) che ogni gruppo G può essere visto come un sotto gruppo transitivo di S_n, è naturale chiedersi quali siano <u>tutti</u> i modi di realizzare G come un sotto gruppo di S_n.

Definizione 5.12. *Una rappresentazione di permutazione del gruppo G è un morfismo di gruppi: $\varphi : G \to Sym(X)$ dove X è un insieme finito.*

Il grado *della rappresentazione è $\#(X)$. La rappresentazione è* fedele *se φ è iniettivo ed è transitiva se $\varphi(G) \leq Sym(X)$ è transitivo.*

Un modo per costruire delle rappresentazioni di permutazioni è il seguente. Sia $H \leq G$, allora G agisce sull'insieme quoziente G/H. Infatti se $G/H = \{x_1H, ..., x_nH\} = \{\overline{x}_1, ..., \overline{x}_n\}$ $(x_1 = 1)$, allora $\varphi_g : G/H \to G/H : \overline{x}_i \to \overline{gx_i}$ è biiettiva e si verifica facilmente che $\varphi : G \to Sym(G/H)$ è un morfismo di gruppi. Inoltre l'azione indotta su G/H è transitiva. Osserviamo che, in generale, la rappresentazione ottenuta non è fedele (cioè φ non è iniettivo). La rappresentazione del teorema di Cayley è quella corrispondente a $H = \{1\}$.

Viceversa se abbiamo una rappresentazione di permutazione transitiva, φ, allora φ corrisponde (più precisamente è equivalente) ad una rappresentazione data da un sotto gruppo.

Infatti sia $\varphi : G \to Sym(X)$, $X = \{1, ..., n\}$ una rappresentazione transitiva. Sia $H := G_1 = \{g \in G \mid \varphi_g(1) = 1\}$ lo stabilizzatore di 1.

Siccome l'azione è transitiva, per ogni i esiste g_i tale che $\varphi_{g_i}(1) = i$. Mostriamo che $G^i := \{g \in G \mid \varphi_g(1) = i\}$ non è altro che g_iH. Se $h \in H$, allora $\varphi_{g_ih}(1) = \varphi_{g_i}(\varphi_h(1)) = i$, quindi $g_iH \subset G^i$. Se $\varphi_g(1) = i$, allora $\varphi_{g_i^{-1}g}(1) = 1$ e $g_i^{-1}g \in H$ cioè $G^i \subset g_iH$.

Adesso ogni $g \in G$ manda 1 da qualche parte ossia: $g \in g_iH$ per un qualche i. Inoltre chiaramente $g_iH \cap g_jH = \emptyset$ se $i \neq j$. Vediamo così che i $g_iH, 1 \leq i \leq n$ formano una partizione di G che non è altro che quella corrispondente alla relazione d'equivalenza: $tRg \Leftrightarrow t^{-1}g \in H$, il cui insieme quoziente è G/H.

Chiaramente questo approccio può essere utile nel studiare i possibili gradi delle realizzazioni di un dato gruppo.

Definizione 5.13. *Un sotto gruppo $G \leq S_n$ è m-transitivo se dati due m-uple di elementi distinti di $\{1, ..., n\}$, $(x_1, ..., x_m)$, $(y_1, ..., y_m)$, esiste $\sigma \in G$ con $\sigma(x_i) = y_i, \forall i$.*

Un sotto gruppo transitivo è un gruppo 1-transitivo. Chiaramente S_n è m-transitivo per ogni $m \leq n$; $\mathcal{A}_n$ è m-transitivo per ogni $m \leq n-2$. Si conoscono infiniti esempi di gruppi 2 o 3 transitivi.

A parte $S_n, \mathcal{A}_n$ si conoscono solo quattro gruppi che sono 4, 5-transitivi su un insieme finito. Sono i *gruppi di Mathieu* scoperti nel 1861 e nel 1873.

Il gruppo di Mathieu M_{12} è un gruppo di ordine 95 040, 5-transitivo su un insieme di cardinalità 12. Il gruppo M_{24} invece ha ordine 244 823 040 ed è 5-transitivo su un insieme di cardinalità 24. Lo stabilizzatore in M_{12} di un punto qualsiasi (risp. M_{24}) è M_{11}, di ordine 7 920, 4-transitivo su un insieme di cardinalità 11 (risp. M_{23}, di ordine 10 200 960, 4-transitivo su un insieme con 23 elementi). Lo stabilizzatore di un punto in M_{23} è M_{22}, ha ordine 443 520. I cinque gruppi M_{11}, M_{12}, M_{22}, M_{23}, M_{24} sono semplici e non isomorfi a nessun gruppo alterno o gruppo di tipo Lie. Siccome questi gruppi non rientrano in nessuna famiglia infinita di gruppi semplici, sono stati chiamati (da Burnside) *gruppi sporadici.*

5.3.2 Gruppi sporadici.

Fino al 1966 questi erano gli unici gruppi sporadici noti. Nel periodo tra 1955 e 1961, a seguito dei lavori di Chevalley, l'attenzione si era focalizzata sui gruppi di tipo Lie: la caccia ai gruppi di tipo Lie si concluse nel 1961 con 16 famiglie infinite di gruppi di tipo Lie, scoperte da vari matematici. Si pensava che la classificazione dei gruppi semplici fosse completa. Ma nel 1966, Janko scoprì un nuovo gruppo sporadico. A questo punto la caccia ai gruppi sporadici era aperta. Altri 20 gruppi sporadici furono scoperti. Verso la fine degli anni '70 gli esperti pensavano che esistessero 26 gruppi sporadici, ma ne conoscevano solo 24. Finalmente Griess nel 1980 riuscì a costruire (a mano, usando un gruppo di simmetrie in uno spazio di dimensione 196 833) *il mostro*, M, la cui esistenza era stata congetturata nel 1972. Il cardinale di M è dell'ordine di 10^{50}: è il più grande gruppo sporadico noto. L'ultimo gruppo mancante, J_4, fu scoperto anche lui nel 1980 (ma con l'uso del computer). Per quanto ne so non esistono pubblicazioni con dimostrazioni complete dell'esistenza di questi gruppi (M, J_4).

Finalmente inizio anni '80 vari esperti (Ashbacher, Conway, Gorenstein tra altri) annunciarono che la classificazione dei gruppi semplici era completa, il risultato finale si può enunciare nel modo seguente:

Teorema 5.14. (Il teorema enorme)
Ogni gruppo semplice finito è isomorfo ad uno dei seguenti gruppi:

1. *un gruppo ciclico di ordine un numero primo ($\mathbb{Z}_p$)*
2. *un gruppo alterno $\mathcal{A}_n$, $n \geq 5$*
3. *un gruppo appartenente ad una delle* 16 *famiglie infinite di gruppi di tipo Lie*
4. *uno dei* 26 *gruppi sporadici.*

Per un enunciato più preciso il lettore interessato può consultare [11] (e anche [10]). Questo "teorema" è straordinario, enorme, per almeno due motivi:

- non esiste nessuna dimostrazione scritta, completa del teorema!
- è l'opera di un numero imprecisato di matematici.

Si stima che al momento sia reperibile, nelle riviste, un buon 80% della dimostrazione e che una dimostrazione completa necessiterebbe almeno 5.000 pagine di rivista! Tant'è che alcuni matematici mettono in dubbio la sua veracità. Per esempio J.P. Serre, sicuramente uno dei più autorevoli matematici viventi, ha più volte lamentato l'assenza di una dimostrazione completa.

Osserviamo che nell'ambito della teoria dei gruppi finiti le dimostrazioni possono essere molto lunghe. Per esempio nel 1963, Feit e Thompson ([7]) hanno dimostrato:

Teorema 5.15. (Feit-Thompson (1963))
Ogni gruppo finito di ordine dispari è risolubile.

La dimostrazione di questo risultato spettacolare e fondamentale (un gruppo semplice non abeliano non è risolubile, quindi ha ordine pari) occupa 255 pagine di una rivista!

Osserviamo che questo risultato, insieme a quello di Shafarevich (Teorema 4.4) risolve "metà" del problema inverso:

Corollario 5.16. *Ogni gruppo finito di ordine dispari è di Galois su* $\mathbb{Q}$.

In conclusione la classificazione dei gruppi finiti è ancora lontana: ammesso (e non concesso) che la classificazione dei gruppi semplici sia finita, rimane ancora da risolvere, in modo utile, il problema delle estensioni.

Esercizi.

Esercizio 105 *Sia G un gruppo di ordine n e sia $H \leq G$. Finalmente sia $\varphi : G \to Sym(G/H)$ la rappresentazione transitiva di permutazione associata ad H. Mostrare che $Ker(\varphi) = H_G$, dove*

$$H_G = \bigcap_{g \in G} gHg^{-1}$$

Il sotto gruppo H_G è il normal core *di H in G.*
Mostrare che $H_G \leq G$ è il più grande sotto gruppo normale in G di H.

In particolare se G è di Galois su $\mathbb{Q}$, allora G ammette solo realizzazioni massimali $\Leftrightarrow$ per ogni sotto gruppo $H \neq \{1\}$, $H_G \neq \{1\}$.

Esercizio 106 (Prodotto semi-diretto)
Siano A e B due gruppi e sia $\varphi : A \to Aut(B) : a \to \varphi_a$ un morfismo di gruppo. Quindi φ definisce un'azione di A su B. Con questi dati possiamo definire un gruppo nel modo seguente: gli elementi sono gli elementi dell'insieme prodotto $B \times A$, la moltiplicazione è definita da:

$$(b, a) \cdot (b', a') = (b\varphi_a(b'), aa')$$

Si verifica che questo definisce una struttura di gruppo sull'insieme $B \times A$, questo gruppo viene notato $B \rtimes_\varphi A$; è il prodotto semi-diretto (esterno) di B con A.

1. *Verificare che l'inverso di (b, a) è $(\varphi_{a^{-1}}(b), a^{-1})$, e che $(1, a) \cdot (b, 1) \cdot (1, a)^{-1} = (\varphi_a(b), 1)$. (Se abbreviamo $(1, a)$ in a e $(b, 1)$ in b, allora $A, B \leq B \rtimes_\varphi A$ e l'equazione precedente diventa: $\varphi_a(b) = aba^{-1}$, cioè in $B \rtimes_\varphi A$ l'azione di A su B è l'azione per coniugo.)*
2. *Mostrare che $B \lhd B \rtimes_\varphi A$ e $(B \rtimes_\varphi A)/B \simeq A$ (in generale A non è normale in $B \rtimes_\varphi A$).*
3. *Sia $N \lhd G$, un complemento di N in G è $H \leq G$ tale che: (1) $NH = G$, (2) $N \cap H = \{1\}$.*
   Per ogni $a \in H$ sia φ_a il coniugo ($\varphi_a(x) = axa^{-1}$). Osservare che $\varphi_a \in Aut(N)$ e $\varphi : H \to Aut(N)$ è un morfismo. Mostrare che $G \simeq N \rtimes_\varphi H$ (in questo caso si nota semplicemente $N \rtimes H$ (prodotto semi-diretto interno)).

In conclusione, una volta capita l'azione φ possiamo sempre vedere un prodotto semi-diretto esterno come un prodotto semi-diretto interno.

Esercizio 107 *Sia $\varphi : \mathbb{Z}_4 \to Aut(\mathbb{Z}_3)$ definito da $\varphi(y) = \iota$, dove $\mathbb{Z}_4 = \langle y \rangle$ e dove $\iota : \mathbb{Z}_3 \to \mathbb{Z}_3 : z \to z^{-1}$.*

1. *Mostrare che φ è ben definito ed è un morfismo.*

2. *Sia* $G = \mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_4$ *(di solito notato* $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$*). Se* $\mathbb{Z}_3 = \langle x \rangle$*, e scrivendo* $x^i y^j$ *al posto di* (x^i, y^j)*, per l'Esercizio 106 possiamo vedere* G *come* $\mathbb{Z}_3 \times \mathbb{Z}_4$ *con la legge*
$$(x^i y^j) \cdot (x^k y^t) = \begin{cases} x^{i+k} y^{j+t} & \text{se } j \text{ pari} \\ x^i (x^k)^{-1} y^{j+t} & \text{se } j \text{ dispari} \end{cases}$$
Quindi
$$G = \{1, y, y^2, y^3, x, xy, xy^2, xy^3, x^2, x^2y, x^2y^2, x^2y^3\}$$
con la moltiplicazione definita qui sopra.
3. *Mostrare che* y^2 *ha ordine due e che* xy *ha ordine quattro, inoltre* $\langle xy \rangle \neq \langle y \rangle$*. Concludere che* G *ha tre 2-Sylow tutti isomorfi a* $\mathbb{Z}_4$ *(il terzo è* $\langle x^2 y \rangle$*). In particolare non tutti i sotto gruppi di* G *sono normali.*
4. *Una verifica noiosa mostra che* y^2 *è l'unico elemento di ordine due. Mostrare che* G *non è abeliano e che* G *non è isomorfo a* $\mathcal{A}_4$
5. *Mostrare che* $S_1 \cap S_2 \cap S_3 = \langle y^2 \rangle$ *(gli* S_i *sono i 2-Sylow)*
6. *Mostrare che* $\langle x \rangle = \mathbb{Z}_3$ *è l'unico 3-Sylow e quindi, come sapevamo già per costruzione,* $\langle x \rangle \lhd G$
7. *Mostrare che se* $H \leq G$*,* H *non banale, allora* $H_G \neq \{1\}$ *(si ricorda che* H_G*, il* normal core *di* H *in* G*, è l'intersezione di tutti i coniugati di* H *in* G*, Esercizio 105)*
8. *Mostrare che* G *è risolubile (quindi per il teorema di Shafarevich* G *è di Galois su* $\mathbb{Q}$*)*
9. *Concludere che* G *ammette solo realizzazioni massimali (usare l'Esercizio 105)*

Nota: *Quindi la proprietà di avere tutti i sotto gruppi normali non caratterizza i gruppi con sole realizzazioni massimali (Cf Esercizio 71).*
Si può vedere che G *ha un unico sotto gruppo di ordine* 6*:* $\langle xy^2 \rangle \simeq \mathbb{Z}_6$ *e quindi abbiamo la lista di tutti i sotto gruppi di* G*. In particolare tutti i sotto gruppi di* G *sono abeliani.*

Scopo dei prossimi esercizi è la classificazione dei gruppi semplici di ordine ≤ 100.

Esercizio 108 *Sia* G *un gruppo di ordine* $2m$ *con* $(2, m) = 1$*.*

1. *Dimostrare che* G *ha un elemento di ordine due (se* $H = \{g \mid g = g^{-1}\}$*, considerare* H *e* $G \setminus H$*; oppure usate un risultato generale ...)*
2. *Sia* $\varphi : G \to Sym(G)$ *la rappresentazione regolare (quella del teorema di Cayley). Se* $x \in G$ *è un elemento di ordine due, mostrare che la segnatura di* φ_x *è* -1*.*
3. *Considerando il morfismo (segnatura)* $G \to \{\pm 1\}$*, concludere che* G *ha un sotto gruppo normale di ordine* m*.*

In conclusione, ogni gruppo, G*, di ordine* $2m$*, con* $(2, m) = 1$*, ha un sotto gruppo normale di ordine* m*; in particolare* G *non è semplice.*

Esercizio 109 *Un p-gruppo (p primo) è un gruppo il cui ordine è una potenza di p.*

1. *Se un p-gruppo G agisce su un insieme X, allora $\#(X) \equiv \#(X^G) \pmod p$ (usare le formule delle classi)*
2. *Il centro di G è $Z(G) = \{x \in G \mid xy = yx, \forall y \in G\}$. Mostrare che $Z(G) \lhd G$.*
3. *Se G è un p-gruppo, mostrare che $Z(G) \neq \{1\}$ (fare agire G su se stesso per coniugo). In particolare un p-gruppo non abeliano non è mai semplice.*

Esercizio 110 *Sia G un gruppo semplice, non abeliano, di ordine n. Sia p un primo che divide n e sia n_p il numero di p-Sylow. Si ricorda che G agisce sull'insieme X dei p-Sylow per coniugo e che questa azione è transitiva (teoremi di Sylow). Mostrare che si ottiene in questo modo un morfismo iniettivo $G \to S_{n_p}$. In particolare $n \mid n_p!$.*

Esercizio 111 *Sia G un gruppo non abeliano di ordine $n = p^2q$, p e q numeri primi, $p \neq q$. Si indica con n_p (risp. n_q) il numero di p-Sylow (risp. di q-Sylow). Si ricorda che $n_p \equiv 1 \pmod p$ e $n_p \mid \#(G)$.*

1. *Se $n_q = p^2$, mostrare che ci sono $p^2 - 1$ elementi il cui ordine è divisibile per p. Concludere che $n_p = 1$ e che G non è semplice*
2. *Se $n_q = p$, allora $p \geq q + 1$. Mostrare che $n_p = 1$*
3. *Concludere che in ogni caso G non è semplice*

Esercizio 112 *Mostrare che se uno dei seguenti casi si verifica, allora G non è semplice:*

1. *$n = 2m$, $(2, m) = 1$*
2. *$n = p^k$, $k \geq 1$*
3. *$n = pq$, p e q primi*
4. *$n = p^2q$, p e q primi*
5. *$n = 8p$, p primo*

Nel caso (3) ragionare come nell'Esercizio 111. Nel caso (5), se $n_p > 1$, allora: $p = 7$ o $p = 3$. Se $p = 7$, $n_7 = 8$, contare gli elementi il cui ordine divide 8 e concludere che $n_2 = 1$. Se $p = 3$, $n_3 = 4$ e $G \simeq S_4$ (usare l'Esercizio 110).

Esercizio 113 *Sia G un gruppo semplice non abeliano di ordine $n \leq 100$. Usando l'Esercizio 112 si verifica che le uniche possibilità sono:*

$$n \in \{36, 48, 60, 72, 80, 84, 96, 100\}.$$

1. *Se $n = 100$, mostrare che $n_5 = 1$, ossia c'è un unico 5-Sylow, quindi G non è semplice*
2. *Se $n = 96$, $n_2 = 3$, usare l'Esercizio 110 per ottenere un assurdo*
3. *Con ragionamenti analoghi concludere che necessariamente deve essere $n = 60$.*

Esercizio 114 *Sia G un gruppo semplice (non abeliano) di ordine 60. Sia n_2 il numero di 2-Sylow.*

1. *Mostrare che $n_2 = 5$ o $n_2 = 15$*
2. *Se $n_2 = 5$, esiste un morfismo iniettivo $G \to S_5$*
3. *Supponiamo $n_2 = 15$. Mostrare che $n_5 = 6$ e che ci sono 24 elementi di ordine cinque. Concludere che esistono due 2-Sylow, Q, Q_2 con $Q \cap Q_2 \neq \{1\}$*
4. *Sia $x \in Q \cap Q_2$, $x \neq 1$ e sia $T = \{y \in G \mid yx = xy\}$. Mostrare che $Q, Q_2 \subset T$, concludere che $\#(T) \geq 12$. Sia $r = \#(G/T)$, abbiamo $r \leq 5$. La rappresentazione transitva di permutazione associata fornisce $G \to S_r$. Concludere che $r = 5$.*
5. *Quindi in ogni caso esiste un morfismo iniettivo $G \to S_5$, concludere che $G \simeq \mathcal{A}_5$ (usare l'Esercizio 96)*

In conclusione se G è un gruppo semplice, non abeliano, di ordine ≤ 100, allora $G \simeq \mathcal{A}_5$.

6

Curve ellittiche e rappresentazioni di Galois.

6.1 Preliminari.

Questo capitolo, molto discorsivo e con poche dimostrazioni, è soprattutto un pretesto per introdurre alcune nozioni della teoria delle curve ellittiche, argomento affascinante dove algebra, geometria, analisi e aritmetica si mescolano con armonia. I prerequisiti sono una conoscenza delle nozioni di base sulle curve algebriche piane e l'aritmetica delle curve ellittiche. Un buon testo introduttivo è il libro di Silverman-Tate [17] (potete anche consultare, in italiano, le note [6]). Facciamo comunque un breve riassunto di queste nozioni di base.

Si lavoro nel piano proiettivo complesso $\mathbb{P}^2(\mathbb{C})$. Una curva algebrica piana, di grado n, $C \subset \mathbb{P}^2(\mathbb{C})$, è un polinomio (definito a meno di una costante non nulla) omogeneo di grado n, cioè un elemento di $\mathbb{P}(S_n)$ dove $S_n = \mathbb{C}[x, y, z]_n$ indica lo spazio vettoriale dei polinomi omogenei di grado n (con il polinomio nullo). Osserviamo che la curva è proprio l'equazione e non il luogo geometrico che definisce. Se $P(x, y, z) \in S_n$ indichiamo con $Z(P) = \{[x : y : z] \in \mathbb{P}^2(\mathbb{C}) \mid P(x, y, z) = 0\}$; $Z(P)$ è il luogo degli zeri di P (ben definito perché P è omogeneo). Allora due curve diverse possono avere lo stesso luogo degli zeri. Per esempio se $P(x, y, z) = x$ e $Q(x, y, z) = x^2$; $Z(P) = Z(Q) = \{[0 : y : z] \in \mathbb{P}^2(\mathbb{C})\}$, ma P e Q sono curve diverse: una ha grado uno e l'altra ha grado due! La curva definita da P è una retta mentre quella definita da Q è una conica ("retta doppia").

Una curva è *irriducibile* se la sua equazione è un polinomio irriducibile.

Ogni polinomio omogeneo F ammette una fattorizzazione in fattori irriducibili ($k[x, y, z]$ è fattoriale): $F = \prod F_i^{a_i}$, questa fattorizzazione è unica (a meno di costanti non nulle) e i fattori F_i sono omogenei. Se $a_i = 1, \forall i$, la curva si dice *ridotta*, se $a_i > 1$, si indica con $a_i C_i$ la curva di equazione $F_i^{a_i}$. Quindi ogni curva C si scrive in modo unico: $C = a_1 C_1 \cup a_2 C_2 \cup ... \cup a_r C_r$ dove C_i è irriducibile per ogni i; le curve C_i sono le *componenti irriducibili* di C.

Sia $C \subset \mathbb{P}^2(\mathbb{C})$ una curva qualsiasi di grado n e sia $L \subset \mathbb{P}^2(\mathbb{C})$ una retta. La retta L è definita da un'equazione del primo grado $l(x, y, z) = 0$ o in forma parametrica $L = \{\lambda P + \mu Q \mid [\lambda : \mu] \in \mathbb{P}^1\}$, dove P, Q sono due punti di L. L'intersezione $C \cap L$ e data da $F(\lambda P + \mu Q) = 0$, dove F è un'equazione di C. Se $l \nmid F$ (cioè se L non è una componente irriducibile di C), il polinomio $\varphi(\lambda, \mu) := F(\lambda P + \mu Q)$ è omogeneo di grado n.

Quindi $\varphi(\lambda, \mu) = a_n\lambda^n + a_{n-1}\lambda^{n-1}\mu + ... + a_0\mu^n$, con, per esempio, $a_n \neq 0$. Ponendo $\mu = 1$, viene un polinomio di grado n in una variabile, siccome $\mathbb{C}$ è algebricamente chiuso questo polinomio ha n radici, cioè $\varphi(\lambda, 1) = a_n \prod_{i=1}^{n}(\lambda - b_i)$ Pertanto $\varphi(\lambda, \mu) = a_n \prod_{i=1}^{n}(\lambda - b_i\mu)$, ossia:

$$\varphi(\lambda, \mu) = \prod_{j=1}^{r} l_i(\lambda, \mu)^{\alpha_j}$$

dove $l_j(\lambda, \mu) = a_j\lambda - b_j\mu$ sono delle forme lineari e dove $\alpha_1 + ... + \alpha_r = n$. I punti $[b_j : a_j] \in L \simeq \mathbb{P}^1(\mathbb{C})$ sono gli "zeri" (con molteplicità α_j) di φ in $\mathbb{P}^1$. In conclusione:

Proposizione 6.1. (Forma debole del teorema di Bezout)
Sia $C \subset \mathbb{P}^2(\mathbb{C})$ una curva di grado n e sia L una retta che non sia una componente irriducibile di C, allora $C \cap L$ consta di n punti contati con molteplicità.

Ovviamente questo risultato non è più vero con $\mathbb{R}$ al posto di $\mathbb{C}$ o $\mathbb{C}^2$ al posto di $\mathbb{P}^2(\mathbb{C})$ di cui l'interesse di lavorare nel piano proiettivo complesso. Il teorema di Bezout afferma che, su $\mathbb{C}$ (o un campo algebricamente chiuso qualsiasi) due curve piane di gradi n, m, *senza componenti irriducibili comuni* s'intersecano in mn punti, contati con molteplicità. La dimostrazione è nettamente più difficile (perché bisogna definire la molteplicità d'intersezione di due curve di grado > 1).

Se $P \in C \cap L$, allora P è uno dei punti $[b_j : a_j]$, diciamo $[b_1 : a_1]$. L'intero α_1 è la *molteplicità d'intersezione* della retta L e della curva C in P, viene denotata con $m(C, L; P)$.

Se $P \in C$ la molteplicità di P in C è: $m_P(C) := min\{m(C, L; P) \mid P \in L\}$. Il punto P è un punto non singolare (o liscio) della curva C se $m_P(C) = 1$. Questo significa che una generica retta passante per P interseca C in P con molteplicità uno e che esiste una ed un'unica *tangente* a C in P, dove una tangente in P è una retta D con $m(C, D; P) > 1$.

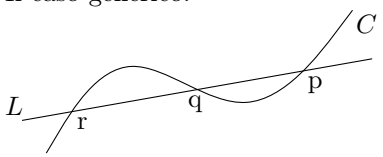
La curva C è non singolare (o liscia) se tutti i suoi punti sono non singolari. Si dimostra che $P \in C$ è non singolare se e solo se una delle derivate parziali $\frac{\partial F}{\partial x}(P)$, $\frac{\partial F}{\partial y}(P)$, $\frac{\partial F}{\partial z}(P)$ è non nulla.

Se C è non singolare, allora $F(x, y, z)$ è irriducibile ($F = 0$ un'equazione di C).

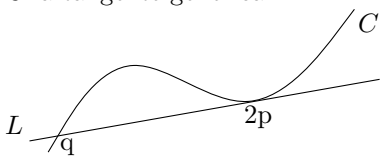
6.2 Legge di gruppo sulle cubiche liscie.

Sia $C \subset \mathbb{P}^2(\mathbb{C})$ una cubica liscia (quindi irriducibile). Da quanto detto prima ci sono tre casi per l'intersezione $C \cap L$ con una retta L:

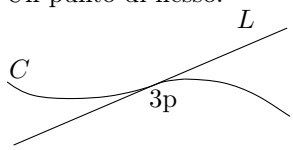
- Il caso generico:



  La retta L interseca C in tre punti distinti, in ognni punto la molteplicità d'intersezione è uno.
- Una tangente generica:



  La retta L è la tangente in p a C, L interseca C con molteplicità due in p e molteplicità uno in q.
- Un punto di flesso:



  La retta L è una tangente di flesso: è tangente in p ma la molteplicità d'intersezione è tre; L incontra C solo in p.

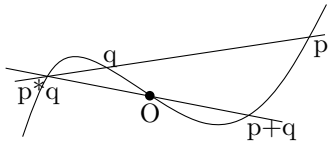
Si può dimostrare che una cubica liscia $C \subset \mathbb{P}^2(\mathbb{C})$ ha esattamente nove punti di flesso, tutti distinti.

Adesso vogliamo definire, geometricamente, una legge di gruppo su C. Per questo se p, q sono due punti di C indichiamo con $\langle p, q\rangle$ la retta generata da p e q (se $p = q$ prendiamo la tangente a C in p) e con $(p * q)$ il terzo punto dell'intersezione $\langle p, q\rangle \cap C$. Quindi se p non è di flesso $p * p = q$, $q \neq p$, mentre $p * p = p$ se p è di flesso.

Fatto ciò fissiamo un punto $O \in C$ (sarà il neutro) e definiamo

$$p + q := (O * (p * q))$$

Quindi $p+q$ è ottenuto nel modo seguente: dati p, q, prima si cerca il terzo punto $(p * q) = r$, poi si considera il terzo punto di $\langle O, r\rangle$, il risultato è $p + q$.



Proposizione 6.2. *Con questa legge* $(C, +)$ *è un gruppo abeliano.*

Dimostrazione (Cenni). La legge è chiaramente commutativa. Per ogni $p \in C$: $p + O = O + p = p$, infatti se $q = p * O$, allora $p + O$ è il terzo punto di $\langle q, O \rangle$, cioè p $(\langle q, O \rangle \cap C = \{p, q, O\})$.

Sia $O' = O * O$, il terzo punto della tangente a C in O. Per ogni $p \in C$, poniamo $-p = p * O'$. Si verifica facilmente che $p + (-p) = (-p) + p = O$.

Rimane da mostrare che la legge è associativa: $p + (q + r) = (p + q) + r$, $\forall (p, q, r) \in C^3$: questa è la parte difficile che si può trattare sia con argomenti di geometria algebrica (vedere per esempio [6] per maggior dettagli) che con le formule esplicite che vedremo più avanti.

Osserviamo che qualsiasi punto $O \in C$ può servire di origine; la legge diventa più semplice se O è un punto di flesso.

Lemma 6.3. *Se* O *è un flesso:* $O * O = O$*, pertanto* $-a = O * a$*, inoltre:*

1. *Se* O *è un punto di flesso allora per ogni* $(p, q, r) \in C^3 : p + q + r = O$ *se e solo se* p, q, r *sono allineati.*
2. p *è un punto di flesso se e solo se* $3p = O$
3. *Se* p *e* q *sono due flessi allora il terzo punto* $r := p * q$ *è anch'esso un flesso.*

Dimostrazione. Esercizio. □

Osserviamo che la disposizione dei nove flessi è assai particolare (due flessi determinano una retta la cui terza intersezione è un flesso, in tutto ci sono nove flessi, cercate di capire quante rette questo determina...)

6.3 Forma di Weierstrass, rappresentazioni affini.

Le considerazioni svolte finora sono valide per una cubica liscia $C \subset \mathbb{P}^2(k)$, dove k è un campo algebricamente chiuso qualsiasi.

A priori l'equazione di una cubica non singolare è un generico polinomio omogeneo di grado tre. Si può con varie trasformazioni ricondurre questa equazione ad una forma canonica, più precisamente si dimostra:

Proposizione 6.4. *Si assume $ch(k) \neq 2, 3$ (e k algebricamente chiuso). Sia $C \subset \mathbb{P}^2$ una cubica non singolare.*

1. *C è proiettivamente equivalente ad una curva di equazione $Y^2Z = X(X - Z)(X - \lambda Z)$, con $\lambda \neq 0, 1$ (forma di Legendre).*
2. *C è proiettivamente equivalente ad una curva di equazione: $Y^2Z = X^3 + aXZ^2 + bZ^3$, con $4a^3 + 27b^2 \neq 0$ (forma di Weierstrass).*

Passando nella carta affine U_Z $(Z = 1)$, l'equazione diventa: $y^2 = f(x)$, con $f(x) = x^3 + ax + b$.

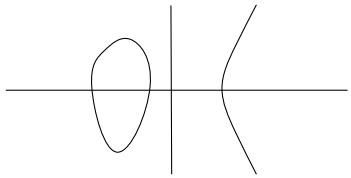
É spesso utile (per motivi aritmetici) usare una forma di Weierstrass più generale: $y^2 = x^3 + ax^2 + bx + c$.

Sia $C \subset \mathbb{P}^2(\mathbb{C})$ una cubica in forma di Weierstrass: $Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3$. Il punto $O = (0 : 1 : 0)$ è un punto di flesso di C quindi $C \cap T_OC = \{O\}$ (con molteplicità tre), dove T_OC è la retta $Z = 0$. Nella carta affine $U_Z \simeq \mathbb{C}^2$ la curva è data da $y^2 = x^3 + ax^2 + bx + c$. Siamo interessati in cubiche lisce, abbiamo:

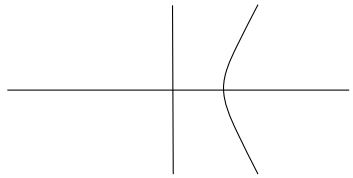
Lemma 6.5. *Con le notazioni precedenti, la cubica C è liscia se e solo se $\Delta \neq 0$ dove $\Delta = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27b^2$.*

Osservazione 6.6. Il numero Δ è il discriminante del polinomio $f(x) = x^3 + ax^2 + bx + c$; la condizione $\Delta \neq 0$ equivale a dire che $f(x) = 0$ ha tre radici distinte. Se $a = 0$, l'espressione di Δ è più simpatica: $D = -4b^3 - 27b^2$.

L'intersezione della curva affine $y^2 = f(x) := x^3 + ax^2 + bx + c$ con la retta all'infinito consta, come abbiamo visto, dell'unico punto O (che corrisponde alle direzioni verticali). Quindi i punti di C sono i punti a distanza finita e il punto all'infinito O, cioè: $\{(x, y) \in \mathbb{C}^2 \mid y^2 = f(x)\} \cup \{O\}$. In quanto segue si cercherà di esplicitare la struttura di gruppo su C con origine O. Se a, b, c sono reali la parte reale di C è del tipo:



($f(x) = 0$ ha tre radici reali).



($f(x) = 0$ ha una radice reale).

Se $P \in \mathbb{C}^2$ è un punto del piano noteremo $(x(P), y(P))$ le sue coordinate (o anche (x, y) se non c'è rischio di confusione). Cerchiamo di stabilire delle formule per le coordinate di $P + Q$, $-P$, $2P = P + P$, dove P, Q sono punti di C.

Il simmetrico: Sia $P \neq O$ un punto di C. Siccome O è un punto di flesso, $-P$ è il terzo punto di $R \cap C$ dove R è la retta generata da P e O. La retta R è la retta verticale passante per P, ossia la retta di equazione affine $x = x(P)$. Siccome C è simmetrica rispetto all'asse delle x:

Lemma 6.7. *Sia $P = (x(P), y(P))$ un punto di C ($P \neq O$). Allora $-P = (x(P), -y(P))$.*

Somma di due punti distinti: Siano $P = (x_1, y_1)$, $P' = (x_2, y_2)$ due punti distinti di C. Se $P * P' = (x_3, y_3)$ allora $P + P'$ è il terzo punto di $R \cap C$ dove R è la retta generata da O e $P * P'$; quindi $P + P' = (x3, -y3)$. Sia $y = \lambda x + \nu$ l'equazione della retta, D, per P e P' (se la retta è verticale $P = -P'$ e $P + P' = O$). Abbiamo $\lambda(x_1 - x_2) = y_1 - y_2$, cioè: $\lambda = (y_1 - y_2)/(x_1 - x_2)$ (se $x_1 = x_2$ allora $P = \pm P'$). Il punto $P * P'$ è il terzo punto di $D \cap C$, questa intersezione è data da:

$y^2 = (\lambda x + \nu)^2 = x^3 + ax^2 + bx + c$, cioè: $x^3 + x^2(a - \lambda^2) + x(b - 2\nu) + c - \nu^2 = 0$.

Questa equazione è verificata da $P, P', P * P'$, quindi:

$x^3 + x^2(a - \lambda^2) + x(b - 2\nu) + c - \nu^2 = (x - x_1)(x - x_2)(x - x_3)$.

Identificando i coefficienti di x^2 abbiamo: $x_3 = \lambda^2 - a - x_1 - x_2$; e poi $y_3 = \lambda x_3 + \nu$, dove $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$. Riassumendo:

Lemma 6.8. *Siano $P = (x_1, y_1)$, $P' = (x_2, y_2)$ due punti a distanza finita di C. Se $P \neq P'$, le coordinate (x, y) di $P + P'$ sono:*
$x = \lambda^2 - a - x_1 - x_2$
$y = -\lambda x - \nu$
dove $\lambda = (y_1 - y_2)/(x_1 - x_2)$, $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$.

Formula di duplicazione: Consideriamo adesso il caso $P = P'$, vogliamo quindi calcolare le coordinate di $2P = P + P$ in funzione delle coordinate (x_1, y_1) di P. Si procede come prima ma con la tangente in P al posto della retta $\langle P, P' \rangle$. L'equazione della tangente è: $-(x - x_1)f'(x_1) + (y - y_1)2y_1 = 0$. La tangente è verticale se e solo se $2P = O$. Se $y_1 \neq 0$ la tangente ha equazione $y = \lambda x + \nu$ con $\lambda = f'(x_1)/2y_1 = (3x_1^2 + 2ax_1 + b)/2y_1$, ragionando come prima viene $x(2P) = \lambda^2 - a - 2x_1$, e riducendo allo stesso denominatore:

Lemma 6.9. *Sia $P = (x, y)$ un punto di C a distanza finita. Se $y \neq 0$ allora:*

$$x(2P) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c} = \frac{f'(x)^2}{4f(x)} - a - 2x \quad (*)$$

Se $y = 0$, allora $2P = O$.

Osservazione 6.10. (i) La formula $(*)$ del Lemma 6.9 si chiama formula di duplicazione; si può ottenere una formula analoga per $y(2P)$.

(ii) Si possono usare le formule dei lemmi precedenti per una dimostrazione alternativa del fatto che l'addizione definisce una struttura di gruppo abeliano su C.

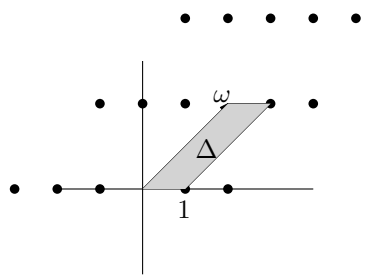
6.4 Punti di ordine n, i vari avatar delle curve ellittiche.

Sia $E \subset \mathbb{P}^2(\mathbb{C})$ una cubica liscia. Come abbiamo visto E è un gruppo abeliano, possiamo quindi considerare il sotto gruppo dei punti di n-torsione: $E[n] = \{P \in E \mid n.P = O\}$, quindi $E[n]$ è l'insieme degli elementi il cui ordine divide n. Si vede facilmente che $E[n] \subset E$ è un sotto gruppo (Esercizio). Abbiamo:

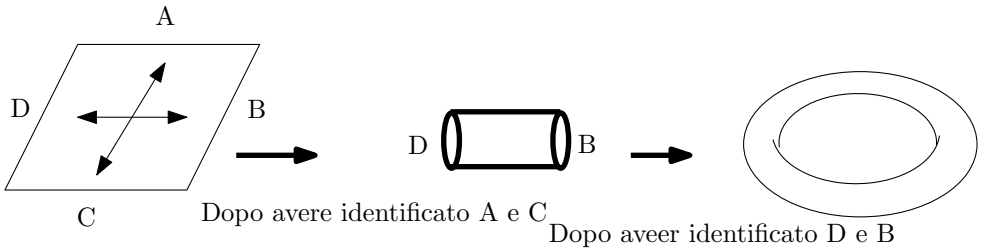
Proposizione 6.11. *Sia $E \subset \mathbb{P}^2(\mathbb{C})$ una cubica liscia, allora $E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$.*

Il modo più semplice (?) per dimostrare questa proposizione è di usare il fatto che una cubica liscia in $\mathbb{P}^2(\mathbb{C})$ è anche un toro complesso. Siccome questo è un punto fondamentale della teoria delle curve ellittiche, vale la pena accennare rapidamente di cosa si tratta.

Siano ω, ω' due numeri complessi, linearmente indipendenti su $\mathbb{R}$. Il reticolo generato da ω e ω' è $\Lambda = \{a\omega + b\omega' \mid a, b \in \mathbb{Z}\}$. Dato un reticolo, consideriamo $T := \mathbb{C}/\Lambda$, l'insieme quoziente della relazione di equivalenza su $\mathbb{C}$: $zRz' \Leftrightarrow z - z' \in \Lambda$. Come si vede su un disegno T è rappresentato da un *parallelogramma fondamentale*, Δ (zona in grigio):



Quindi T è un parallelogramma "chiuso" (prendendo tutto il bordo di Δ) i cui lati opposti vanno identificati:



Quindi T è una superficie reale (due dimensioni reali), compatta ed orientabile. Dal punto di visto complesso, T, è una curva (2 dimensioni reali = 1 dimensione complessa).

Osserviamo che T ha una struttura di gruppo abeliano (quella di $\mathbb{C}$ che passa al quoziente).

Una funzione su T è una funzione su $\mathbb{C}$ che prende gli stessi valori su punti equivalenti, una tale funzione è periodica: $f(z+\alpha) = f(z), \forall \alpha \in \Lambda$ (si dice anche che f è doppiamente periodica (secondo ω e ω') e che Δ è il parallelogramma dei periodi).

Una funzione *ellittica* (relativamente a Λ) è una funzione *meromorfa* su T, cioè una funzione periodica e meromorfa su $\mathbb{C}$. Se non sapete che cos'è una funziona meromorfa, pensate a funzione razionale...

Si dimostra che il campo delle funzioni ellittiche (relativamente a Λ) è $\mathbb{C}(\wp(z), \wp'(z))$ dove $\wp(z)$ è la funzione di Weierstrass:

$$\wp(z) = \frac{1}{z^2} + \sum_{\alpha \in \Lambda^*} \left(\frac{1}{(z-\alpha)^2} - \frac{1}{\alpha^2} \right)$$

($\Lambda^* = \Lambda \setminus \{0\}$). Questa serie converge per ogni $z \notin \Lambda$ e definisce una funzione meromorfa con poli (doppi) ai punti di Λ. La funzione di Weierstrass è legata alla sua derivata tramite una relazione:

$$(\wp'(z))^2 = 4\wp(z) - g_2\wp(z) - g_3$$

dove $g_2 = 60 \sum_{\alpha \in \Lambda^*} \frac{1}{\alpha^4}$, $g_3 = 140 \sum_{\alpha \in \Lambda^*} \frac{1}{\alpha^6}$. Adesso si definisce $f : \mathbb{C} \to \mathbb{P}^2(\mathbb{C}) : z \to (\wp(z), \wp'(z))$ (in coordinate affini) e si mostra che f definisce una biiezione tra $T = \mathbb{C}/\Lambda$ e la curva piana di equazione $y^2 = 4x^3 - g_2x - g_3$, cioè con la cubica piana di equazione omogenea $ZX^2 = 4X^3 - g_2XZ^2 - g_3Z^3$. Si vede poi che questa cubica è non singolare. In conclusione:

Ogni toro complesso è una cubica piana liscia.

Viceversa per mostrare che ogni cubica liscia si ottiene in questo modo (cioè ogni cubica liscia è un toro complesso), si introduce prima il j-invariante. Se $C \subset \mathbb{P}^2$ è una cubica liscia e se $P \in C$ è un punto di flesso si mostra che ci sono esattamente 4 tangenti a C passante per P. Il fascio di rette per P è naturalmente un $\mathbb{P}^1$, quindi abbiamo 4 punti in $\mathbb{P}^1$, possiamo con un automorfismo di $\mathbb{P}^1$ assumere che questi punti siano $\infty, 0, 1, \lambda$, quattro punti di $\mathbb{P}^1$ hanno un birapporto (anche più di uno) e un unico modulo, in questo caso $j := 2^8 \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$ (si aggiunge il fattore 2^8 per motivi "aritmetici"). Il modulo non dipende dal punto di flesso scelto e quindi $j(C) := j$ è ben definito. Si dimostra che due cubiche piane lisce sono proiettivamente equivalenti se e solo se hanno lo stesso modulo. Inoltre per ogni $\lambda \in \mathbb{C}$ esiste una cubica piana di modulo λ. Quindi $\{\textit{cubiche piane}\}/\{\textit{equivalenza proiettiva}\} \simeq \mathbb{C}$ (cf per esempio [6]).

Ma si può fare di più! Se ci dimentichiamo dell'immersione $C \subset \mathbb{P}^2$, una cubica piana liscia è una curva algebrica (proiettiva) di genere uno, cioè una *curva ellittica*. (Il genere di una curva proiettiva è la dimensione dello spazio delle sezioni globali del fibrato cotangente; il genere di una curva piana liscia di grado d è $(d-1)(d-2)/2$.) Con il teorema di Riemann-Roch si mostra

facilmente che ogni curva ellittica può essere immersa in $\mathbb{P}^2$ come una cubica liscia e che tutte queste immersioni hanno lo stesso j-invariante (se $P \in C$, il sistema lineare $|3P|$ è molto piano e definisce un'immersione $\varphi : C \to \mathbb{P}^2(\mathbb{C})$ e $\varphi(P)$ è un flesso di $\varphi(C)$). Finalmente due curve ellittiche sono isomorfe se e solo se hanno lo stesso j-invariante. In conclusione:

$$\{curve\ \ ellittiche\ \}/\{isomorfismo\} \simeq \mathbb{C}$$

dove l'isomorfismo è dato dal j-invariante. Finalmente siccome i j-invarianti dei tori complessi prendono tutti i valori di $\mathbb{C}$, ogni curva ellittica (cioè ogni cubica liscia) è (proviene da) un toro complesso! Quindi abbiamo tre modi diversi di considerare uno stesso oggetto:

- una curva proiettiva di genere uno
- una cubica piana liscia
- un toro complesso

Un'ultima osservazione: se $E \subset \mathbb{P}^2(\mathbb{C})$ è una cubica liscia definita da un polinomio a coefficienti in $\mathbb{Z}$, riducendo i coefficienti $\pmod p$, otteniamo una curva in $\mathbb{P}^2(\mathbb{F}_p)$, lo studio dei legami tra queste varie riduzioni $\pmod p$ e i tre *avatar* della curva ellittica è di una ricchezza infinita!

Tornando alle nostre cose possiamo finalmente dimostrare la Proposizione 6.11 sui punti di ordine n:

Dimostrazione (della Prop. 6.11). Per quanto precede possiamo considerare la nostra cubica come un toro complesso $E = \mathbb{C}/\Lambda$, dove $\Lambda = \{a\omega + b\omega' \mid a, b \in \mathbb{Z}\}$ e ci possiamo limitare ai punti del parallelogramma fondamentale: $\Delta = \{x\omega + y\omega' \mid 0 \leq x, y < 1\}$. Se $nP = O$, con $P = x\omega + y\omega'$, allora $nP = nx\omega + ny\omega'$ verifica $nx, ny \in \mathbb{Z}$. Quindi $nx = m$ cioè $x = m/n$, siccome $0 \leq x < 1$, questo implica $m \in \{0, ..., n-1\}$. Stessa cosa per y, da cui il risultato.

6.5 Rappresentazioni di Galois.

Nel seguito considereremo solo curve ellittiche, $E \subset \mathbb{P}^2(\mathbb{C})$, definite da equazioni di Weierstrass a coefficienti razionali: $y^2 = x^3 + ax^2 + bx + c$, con $a, b, c \in \mathbb{Q}$; si dice che E è *definita su* $\mathbb{Q}$.

Osservazione 6.12. Se $E \subset \mathbb{P}^2$ è definita da $zy^2 = x^3 + azx^2 + bz^2x + cz^3$, $a, b, c \in \mathbb{Q}$, allora E ha sempre un punto definito su $\mathbb{Q}$: è il punto $O = [0 : 1 : 0]$ (un punto di $\mathbb{P}^2(\mathbb{C})$ è definito su $\mathbb{Q}$ se ammette delle coordinate in $\mathbb{Q}$, quindi delle coordinate intere).

Però presa una curva, E, definita da un polinomio omogeneo qualsiasi del terzo grado a coefficienti in $\mathbb{Q}$, non esiste nessun algoritmo per determinare se E ha o meno un punto definito su $\mathbb{Q}$! Per esempio la curva definita da $3x^3 + 4y^3 + 5z^3 = 0$ non ha nessun punto definito su $\mathbb{Q}$ (Selmer (1951)). Esistono quindi curve definite su $\mathbb{Q}$ senza punti razionali (la forma di Weierstrass evidentemente non è a coefficienti in $\mathbb{Q}$).

Il considerare curve in forma di Weierstrass a coefficienti in $\mathbb{Q}$ torna a considerare curve definite su $\mathbb{Q}$ con (per ipotesi!) almeno un punto (di flesso) razionale.

Abbiamo visto che $E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$, quindi $E[n] = \{O, (x_1, y_1), ..., (x_m, y_m)\}$, $m = n^2 - 1$.

Lemma 6.13. *Le coordinate $x_1, y_1, ..., x_m, y_m$ dei punti di $E[n]$ sono numeri algebrici su $\mathbb{Q}$.*

Dimostrazione (Cenni). Nel caso $n = 2$, abbiamo $2P = O \Leftrightarrow P = -P$ e questo implica (Lemma 6.7) $y(P) = 0$. Pertanto $f(x(P)) = 0$ e quindi $x(P)$ è algebrico su $\mathbb{Q}$. Questo si può vedere anche usando le formule di duplicazione (Lemma 6.9). Quindi le coordinate di ogni punto di 2-torsione sono numeri algebrici su $\mathbb{Q}$.

Nel caso generale sia $P = (x, y) \in E$ e sia $nP = (x_n, y_n)$, generalizzando le formule di duplicazione, si dimostra (cf [19], Section 3.2, p. 80) che esistono dei polinomi a coefficienti razionali $\Phi(x), \Psi(x)$, tali che $x_n = \Phi(x)/\Psi(x)^2$; inoltre Ψ e Φ sono primi tra di loro. Abbiamo: $nP = O \Leftrightarrow x_n$ non è finito $\Leftrightarrow \Psi(x) = 0$ (Ψ e Φ non hanno radici comuni), pertanto x è algebrico.

Siccome $x \in \overline{\mathbb{Q}}$, dalla relazione $y^2 = x^3 + ax^2 + bx + c$ segue che anche $y^2 \in \overline{\mathbb{Q}}$ (perché $a, b, c \in \mathbb{Q}$). Siccome $\overline{\mathbb{Q}}$ è algebricamente chiuso, le radici del polinomio $X^2 - y^2 = (X - y)(X + y) \in \overline{\mathbb{Q}}[X]$, appartengono a $\overline{\mathbb{Q}}$, quindi anche y è un numero algebrico.

Segue dal Lemma 6.13 che l'estensione $L := \mathbb{Q}(x_1, y_1, ..., x_m, y_m)/\mathbb{Q}$ è algebrica finita.

Definizione 6.14. *Sia $K/\mathbb{Q}$ un'estensione algebrica finita, con $E(K)$ indichiamo l'insieme dei punti di E* definiti *su K, cioè $E(K) = \{(x, y) \in K^2 \mid (x, y) \in E\} \cup \{O\}$.*

Lemma 6.15. *Con le notazioni precedenti, $E(K)$ è un gruppo per l'addizione definita su E.*

Dimostrazione. Segue dal Lemma 6.8 (e Lemma 6.9) che se P, Q hanno le loro coordinate in K, allora anche $P + Q$ ha le sue coordinate in K.

La dimostrazione è forse più facile dal punto di vista proiettivo: $P \in \mathbb{P}^2(\mathbb{C})$ è definito su K se ammette delle coordinate proiettive in K: $P = [p_0 : p_1 : p_2]$ con $p_i \in K$ (idem per Q). In queste condizioni il terzo punto $P * Q$ si ottiene come la terza radice di $f(\lambda P + \mu Q) = 0$. Segue che $P * Q$ è definito su K (se un polinomio cubico $p(x) \in K[x]$ ha due radici in K allora anche la terza è in K, relazioni tra radici e coefficienti). Si conclude che $P + Q$ è definito su K perché $O = [0 : 1 : 0]$ ("per ipotesi", cf Osservazione 6.12). □

Osservazione 6.16. In particolare abbiamo il gruppo $E(\mathbb{Q})$ dei punti definiti su $\mathbb{Q}$ (sotto l'ipotesi che ci sia un flesso di E definito su $\mathbb{Q}$). Il famoso teorema di Mordell afferma che il gruppo abeliano $E(\mathbb{Q})$ è *finitamente generato*, cioè: $E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus T$, $r \in \mathbb{N}$, T il sotto gruppo di torsione (cioè il sotto gruppo dei punti di ordine finito).

Tutti i possibili sotto gruppi di torsione sono noti (teorema di Mazur) invece si sa pochissimo sui possibili valori di r (il *rango* di $E(\mathbb{Q})$).

Il teorema di Mordell è stato generalizzato da Weil: se K è un campo di numeri, $E(K)$ è finitamente generato.

Chiaramente, se $\mathbb{Q} \subset K$, abbiamo $E(\mathbb{Q}) \subset E(K) \subset E$.

Osservazione 6.17. Sia $K/\mathbb{Q}$ un'estensione algebrica finita e sia $\sigma : K \to \overline{\mathbb{Q}} = \Omega$ una $\mathbb{Q}$-immersione. Definiamo $\sigma_E : E(K) \to E$ tramite $\sigma_E(O) = O$ e $\sigma_E(P) = (\sigma(x), \sigma(y))$, se $P = (x, y)$ è a distanza finita. Osserviamo che dalla relazione $y^2 = x^3 + ax^2 + bx + c$, segue $\sigma(y)^2 = \sigma(x)^3 + a\sigma(x)^2 + b\sigma(x) + c$ (perché σ è un morfismo di campi e $\sigma|\mathbb{Q} = Id$), quindi $\sigma(P) \in E$.

Inoltre le formule di addizione (Lemma 6.8, Lemma 6.9) mostrano che $\sigma_E(P + Q) = \sigma_E(P) + \sigma_E(Q)$, ossia σ_E è un morfismo di gruppi.

Adesso abbiamo:

Proposizione 6.18. *L'estensione $L := \mathbb{Q}(x_1, y_1, ..., x_m, y_m)/\mathbb{Q}$ è di Galois (cioè è normale).*

Dimostrazione. Sia $[L : \mathbb{Q}] = t$, sappiamo che esistono t, $\mathbb{Q}$-immersioni $\sigma : L \to \overline{\mathbb{Q}}$, per mostrare che l'estensione è normale basta mostrare che $\sigma(x_i)$, $\sigma(y_i) \in L$, $\forall i$, $\forall \sigma$. Ma questo segue immediatamente dal fatto che σ_E è un morfismo di gruppi (Osservazione 6.17), infatti se $P \in E[n]$, $n\sigma_E(P) = \sigma_E(nP) = \sigma_E(O) = O$. Quindi $\sigma_E(P) = (\sigma(x_i), \sigma(y_i)) \in E[n]$, ossia $\sigma(x_i), \sigma(y_i) \in L$. □

Sia $G := Gal(\mathbb{Q}(x_1, y_1, ..., x_n, y_n)/\mathbb{Q})$, la dimostrazione precedente mostra che ogni elemento $\sigma \in G$ induce un automorfismo di $E[n]$, abbiamo quindi: $\psi : G \to Aut(E[n])$. Si verifica facilmente che ψ è un morfismo di gruppi.

Lemma 6.19. *Il morfismo di gruppi $\psi : G \to Aut(E[n])$ è iniettivo.*

Dimostrazione. Se $\psi(\sigma) = Id$, allora $\sigma(x_i) = x_i$, $\sigma(y_i) = y_i$, $\forall i$,, cioè $\sigma|L = Id$, siccome $\sigma \in Gal(L/\mathbb{Q})$, questo implica $\sigma = Id$. □

Lemma 6.20. *Abbiamo un isomorfismo di gruppi $Aut(E[n]) \simeq Gl(2, \mathbb{Z}_n)$.*

Dimostrazione. Abbiamo $E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$ (Proposizione 6.11). Siccome ogni gruppo abeliano è un $\mathbb{Z}$-modulo (cioè uno "spazio vettoriale" su $\mathbb{Z}$), per ogni morfismo di gruppi: $f : \mathbb{Z}_n \oplus \mathbb{Z}_n \to \mathbb{Z}_n \oplus \mathbb{Z}_n$, abbiamo $f(n\alpha) = nf(\alpha), \forall \alpha \in \mathbb{Z}_n \oplus \mathbb{Z}_n$, $\forall n \in \mathbb{Z}$ ($nx := x + ... + x$ se $n \geq 1$). Se $\alpha = (\overline{x}, \overline{y})$ ($\overline{x}$ è la classe di $x \in \mathbb{Z}$, $\pmod n$), abbiamo $n\alpha = (n\overline{x}, n\overline{y}) = (\overline{nx}, \overline{ny}) = \overline{n}.\alpha$. In conclusione il morfismo di gruppi f è $\mathbb{Z}_n$-lineare.

Se $\overline{a}, \overline{b}$ sono due generatori di $\mathbb{Z}_n$ (quindi $(a, n) = (b, n) = 1$), ogni $\alpha \in \mathbb{Z}_n \oplus \mathbb{Z}_n$ si scrive in modo unico $\alpha = \overline{n}.e_1 + \overline{m}.e_2$, dove $e_1 = (\overline{a}, 0)$, $e_2 = (0, \overline{b})$ (in altre parole $\mathbb{Z}_n \oplus \mathbb{Z}_n$ è un $\mathbb{Z}_n$-modulo libero di rango due e $B = (e_1, e_2)$ è una base). Ogni morfismo, f, $\mathbb{Z}_n$-lineare è determinato da $f(e_1)$, $f(e_2)$, ossia dalla sua matrice $mat(f; B, B) \in M_2(\mathbb{Z}_n)$. Inoltre f è un automorfismo se e solo se la matrice è invertibile. In conclusione $Aut(\mathbb{Z}_n \oplus \mathbb{Z}_n) \simeq Gl(2, \mathbb{Z}_n)$.

□

Combinando il Lemma 6.19 e il Lemma 6.20 otteniamo un morfismo iniettivo di gruppi: $\rho_n : G \to Gl(2, \mathbb{Z}_n)$.

Definizione 6.21. *Il morfismo iniettivo di gruppi*

$$\rho_n : Gal(\mathbb{Q}(x_1, y_1, ..., x_m, y_m)/\mathbb{Q}) \to Gl(2, \mathbb{Z}_n)$$

è una rappresentazione di Galois *associata alla curva ellittica E.*

Osservazione 6.22. Nella letteratura si trova spesso l'approccio seguente: il gruppo di Galois assoluto $\overline{G} := Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ agisce su $E[n]$ e questo permette di definire un morfismo $\overline{\rho}_n : \overline{G} \to Gl(2, \mathbb{Z}_n)$. Adesso l'immagine di $\overline{\rho}_n$ è uguale a quella di ρ_n, quindi stiamo parlando della stessa cosa.

Il morfismo ρ_n non è necessariamente suriettivo. Per esempio se tutti i punti di n-torsione hanno le loro coordinate razionali, allora $\mathbb{Q}(E[n]) = \mathbb{Q}$, $G = \{Id\}$ e ρ_n non è suriettivo.

- **Punti di 2-torsione:**
  Sia E una curva ellittica di equazione $y^2 = f(x)$, $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Q}[x]$. Se $\alpha_1, \alpha_2, \alpha_3$ sono le tre radici di f, i punti di 2-torsione sono: $E[2] = \{O, (\alpha_1, 0), (\alpha_2, 0), (\alpha_3, 0)\}$. Se $\alpha_i \in \mathbb{Q}$, $\forall i$, allora $\mathbb{Q}(E[2]) = \mathbb{Q}$, $G = \{Id\}$ e ρ_2 non è suriettivo.
  In ogni caso $\mathbb{Q}(E[2]) = L$ è il campo di spezzamento di f. Sappiamo (se f è irriducibile) che se $G = Gal(L/\mathbb{Q})$, allora $G \simeq \mathcal{A}_3$ o $G \simeq S_3$. Siccome $\#(Gl(2, \mathbb{F}_2)) = 6$, ρ_2 è suriettivo se e solo se $G = S_3$. Per esempio se f ha due radici complesse coniugate, ρ_2 è suriettivo.

- **Punti di 3-torsione:**
  Per semplificare i conti prendiamo l'equazione di E nella forma $y^2 = f(x)$, con $f(x) = x^3 + ax + b$, $a, b \in \mathbb{Q}$ (e con $4a^3 + 27b^2 \neq 0$ perché E è liscia). Abbiamo: $3P = O \Leftrightarrow 2P = -P$, si verifica con le solite formule che $P = (x, y)$ è di 3-torsione (cioè è un flesso) se e solo se x è radice di $\varphi(x) = 3x^4 + 6ax^2 + 12bx - a^2$. Il discriminante di φ vale $-6912(4a^3 + 27b^2)^2 \neq 0$, quindi $\varphi(x)$ ha quattro radici distinte $\alpha_1, ..., \alpha_4$. Ognuna di queste radice fornisce due valori di y tramite $y^2 = \alpha_i^3 + a\alpha + b$, otteniamo così 8 flessi $(\alpha_1, \pm\beta_i), 1 \leq i \leq 4$. Quindi $E[3] = \{O, (\alpha_i, \pm\beta_i)\}$ e ritroviamo il fatto che ci sono esattamente 9 flessi.
  Abbiamo $\mathbb{Q}(E[3]) = \mathbb{Q}(\alpha_i, \beta_i) := L$, d'altra parte $\#(Gl(2, \mathbb{F}_3)) = 48$. Osserviamo che L contiene $K = \mathbb{Q}(\alpha_i)$, il campo di spezzamento di $\varphi(x)$.
  Per mostrare che ρ_3 è suriettivo si può procedere così:
  1. trovare a e b (con $4a^3 + 27b^2 \neq 0$) tali che $Gal(K/\mathbb{Q}) = S_4$
  2. mostrare che $K \neq L$.

  Infatti siccome $\#(S_4) = 24$, se $K \neq L$, S_4 è un sotto gruppo proprio di $G = Gal(\mathbb{Q}(E[3]/\mathbb{Q})$, quindi $\#(G) = 24t$ con $t > 1$, pertanto $\#(G) \geq 48$ e siccome ρ_3 è iniettivo si avrà $G \simeq Gl(2, \mathbb{F}_3)$.
  Iniziamo col vedere come si può determinare il gruppo di Galois di una quartica. Sia $\varphi(x) = x^4 + ax^3 + bx^2 + cx + d \in \mathbb{Q}[x]$, irriducibile, con radici $r_1, ..., r_4$ e sia $L = \mathbb{Q}(r_1, ..., r_4)$; finalmente sia $G = Gal(L/\mathbb{Q})$.
  Fissato un ordine sulle radici possiamo considerare G come un sotto gruppo (transitivo perché φ è irriducibile) di S_4. Osserviamo che abbiamo una successione esatta:
  $$1 \to V_4 \to S_4 \xrightarrow{p} S_3 \to 1$$
  dove $p : S_4 \to S_3$ è definita nel modo seguente: ci sono tre modi di partizionare $X = \{1, 2, 3, 4\}$ in due sotto insiemi di due elementi ($a = (12)(34)$, $b = (13)(24)$, $c = (14)(23)$). Ogni permutazione di X induce una permutazione di $\{a, b, c\}$, questo definisce $pS_4 \to S_3$. Si verifica facilmente che p è un morfismo di gruppi suriettivo con nucleo il gruppo di Klein V_4.
  Per restrizione abbiamo $p_| : G \to S_3$, il cui nucleo è $H := G \cap V_4$. Supponiamo $p_|$ suriettiva, allora $\#(G) = 6\#(H)$. Siccome $H \leq V_4$, $\#(H) \in \{1, 2, 4\}$. D'altra parte $4 \mid \#(G)$ perché $\#G) = [L : \mathbb{Q}] = [L : \mathbb{Q}(r_1)][bQ(r_1) : \mathbb{Q}]$. Segue che $\#(G) = 12$ o 24. Nel primo caso $G = \mathcal{A}_4$, nel secondo $G = S_4$. Possiamo scartare il primo caso se Δ_φ, il discriminante di φ, non è un quadrato in $\mathbb{Q}$. In conclusione $G = S_4$ se $p_|$ è suriettiva e se $\sqrt{\Delta_\varphi} \notin \mathbb{Q}$.
  Poniamo $\alpha = r_1r_2 + r_3r_4$, $\beta = r_1r_3 + r_2r_4$, $\gamma = r_1r_4 + r_3r_2$. Abbiamo: $\mathbb{Q}(\alpha, \beta, \gamma) = L^H$ (dove $H = G \cap V_4$). Adesso consideriamo $\psi(x) = \varphi(x - \frac{a}{3}) = x^4 + g_2x^2 + g_1x + g_0$, le cui radici x_i sono $x_i = r_i + a/3$. Osservare che $x_1 + x_2 + x_3 + x_4 = 0$ (relazioni tra radici e coefficienti). Poniamo $A = x_1 + x_2$, $B = x_1 + x_3$, $C = x_1 + x_4$, allora con notazioni che parlano da sé: $A^2 = -\beta(\psi) - \gamma(\psi)$, $B^2 = -\alpha(\psi) - \gamma(\psi)$, $C^2 = -\alpha(\psi) - \beta(\psi)$; inoltre:

$$\mathbb{Q}(A^2, B^2, C^2) = \mathbb{Q}(\alpha(\psi), \beta(\psi), \gamma(\psi)) = \mathbb{Q}(\alpha, \beta, \gamma) = L^H$$

Sia $f(x) = (x - A^2)(x - B^2)(x - C^2)$, se f è irriducibile su $\mathbb{Q}$, L^H è il campo di spezzamento di f (e $Gal_{\mathbb{Q}}(f) \simeq Im(p_|)$). Inoltre un calcolo noioso mostra che $\Delta_\varphi = \Delta_f$. In queste condizioni, se $\sqrt{\Delta_f} \notin \mathbb{Q}$, abbiamo $Gal_{\mathbb{Q}}(f) = S_3$.
Un altro calcolo noioso mostra che $f(x) = x^3 + 2g_2x^2 + (g_2^2 - 4g_0)x - g_1^2$. Il polinomio f è la *risolvente cubica* di φ.

Si tratta adesso di applicare tutto quanto alla nostra quartica $3x^4+6ax^2+12bx-a^2 = 3(x^4+2ax^2+4bx-\frac{a^2}{3})$, quindi sostanzialmente a: $\varphi(x) = x^4+2ax^2+4bx-a^2/3$. (La risolvente cubica è: $f(x) = x^3+4ax^2+\frac{16a^2}{3}x-16b^2$.)
Il lettore si divertirà (?) a svolgere i calcoli (magari con l'aiuto di qualche software) per trovare qualche esempio utile.
A questo punto "abbiamo" una curva ellittica tale che l'immagine di ρ_3 sia un gruppo di ordine 24 o 48; cioè la prima condizione è soddisfatta.
Rimane da verificare la seconda condizione $K \neq L$, cioè che le coordinate y date da $y^2 = f(x)$ non appartengo al campo di spezzamento, K, di $\varphi(x)$. Questo torna a mostrare che esiste i, tale che $y^2 - \alpha_i^3 - a\alpha_i - b$ sia irriducibile in $K[y]$ (α_i una radice di φ). Anche qui l'uso di qualche software può essere d'aiuto...

Si arriva così a dimostrare:

Corollario 6.23. *Il gruppo $Gl(2, \mathbb{F}_3)$ è di Galois su $\mathbb{Q}$.*

Chiaramente questo tipo di analisi diventa presto impraticabile. Tuttavia un risultato famoso (e di difficile dimostrazione) di Serre afferma che "in generale" ρ_n è suriettivo. Più precisamente:

Teorema 6.24. (Serre [16])
Sia E una curva ellittica definita da un'equazione di Weierstrass a coefficienti razionali. Se E non ha moltiplicazione complessa, esiste un intero, N_E, dipendente solo da E, tale che per ogni n primo con N_E, ρ_n sia suriettiva.

Rimane da spiegare l'ipotesi E senza moltiplicazione complessa. Come abbiamo detto $E(\mathbb{C})$ è un gruppo abeliano e possiamo considerare i morfismi di gruppo $f : E(\mathbb{C}) \to E(\mathbb{C})$ che sono anche morfismi algebrici (un tale morfismo si chiama *isogenia*). L'insieme delle isogenie, $End(E(\mathbb{C}))$, è l'anello degli endomorfismi di E. Se $n \in \mathbb{Z}$, la moltiplicazione per n è un'isogenia. D'altra parte guardando E come un toro complesso $\mathbb{C}/\Lambda$, si dimostra che darsi un'isogenia è equivalente a darsi $c \in \mathbb{C}$ tale che $c\Lambda \subset \Lambda$ (da questo punto di vista è chiara che la moltiplicazione per n è un'isogenia). Una curva ellittica "generale" non ha altri endomorfismi: $End(E) \simeq \mathbb{Z}$. Ma per alcune curve esiste $c \notin \mathbb{Z}$ tale che $c\Lambda \subset \Lambda$, si dimostra inoltre che un tale c non può essere reale, da cui la terminologia *moltiplicazione complessa*. Se siete interessati a questi argomenti e più

generalmente all'aritmetica delle curve ellittiche, vi raccomando vivamente il libro di Silverman-Tate ([17]), di facile lettura e grande chiarezza.

In realtà le rappresentazioni di Galois sono soprattutto interessanti, non per il problema di Galois inverso, ma per lo studio delle curve ellittiche e problemi annessi.

Intorno agli anni 1970-80, Hellegouach e Frey si accorsero di uno strano fenomeno: se $a^p + b^p = c^p$ era una soluzione non banale dell'equazione di Fermat ($abc \neq 0$, p primo), la curva ellittica definita da $y^2 = x(x - a^p)(x - b^p)$ doveva avere delle proprietà "straordinarie", in particolare Frey congetturò che non doveva essere *modulare* (cioè parametrizzata da funzioni modulari); insomma doveva avere delle proprietà così particolari che alla fine...non doveva esistere. Nel 1990 Ribet dimostrò (grazie a risultati anteriori di Mazur, Serre e altri) che, effettivamente, una soluzione non banale di Fermat dava luogo ad una curva ellittica definita su $\mathbb{Q}$, non modulare. Finalmente nel 1995, Wiles (con l'aiuto di Taylor) dimostrò che ogni curva ellittica "semi-stabile" è modulare. Questo basta per dimostrare Fermat perché le curve di Frey sono "semi-stabili" (oggi si sa che ogni curva ellittica definita su $\mathbb{Q}$ è modulare). La dimostrazione di Wiles è un vero *tour de force* i cui grandi temi sono la teoria delle curve ellittiche, la teoria delle forme modulari e le rappresentazioni di Galois! Per maggiori informazioni vedere [19] e [12].

That's all folks!

Bibliografia

1. Artin, E.: *Galois theory*, Notre Dame Mathematical Lectures, 2, pp. 82 (1959)
2. Butler, G.-McKay, J.: *The transitive groups of degree up to eleven*, Comm. Algebra, 11, 863-911 (1983)
3. Chambert-Loir, A.: *A field guide to algebra*, Undergraduate Texts in Math., Springer (2005)
4. Chevalley, C.: *Sur certains groupes simples*, Tohoku Math. J. (2) 7, 14-66 (1955)
5. Edwards, H.M.: *Galois theory*, Graduate Texts in Math., 101, Springer (1984)
6. Ellia, Ph.: *Un'introduzione light alla geometria algebrica* (2006) [reperibile sul sito www.unife.it/philippe.ellia]
7. Feit, W.-Thompson, J.: *Solvability of groups of odd order*, Pacific J. Math. 13, 775-1029 (1963)
8. Gabelli, S.: *Teoria delle equazioni e teoria di Galois*, Springer (2008)
9. Galois, É.: *Sur les conditions de résolubilité des équations par radicaux*, J. Math. Pures et Appl. (1), 11, 417-433 (1846)
10. Gorenstein, D.: *The classification of finite simple groups. I Simple groups and local analysis*, Bulletin of the American Math. Soc., vol. 1, n. 1, 43-199 (1979)
11. Gorenstein, D.: *Classifying the simple finite groups*, Bulletin of the American Math. Soc., vol 14, n.1, 1-98 (1986)
12. Hellegouach, Y.: *Invitation to the mathematics of Fermat-Wiles*,
13. Hilbert, D.: *The theory of algebraic number fields*, (translated by Adamson, with an introduction by F. Lemmermeyer and N. Schappacher), Springer-Verlag (1998)
14. Lorenz, F.: *Algebra, volume I: fields and Galois theory*, Universitext, Springer (2006)
15. Menini, C.- Van Oystaeyen, F.: *Abstract algebra*, M. Dekker (2004)
16. Serre, J.P.: *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math., 15, 259-331 (1972)
17. Silverman, J-Tate, J.: *Rational points on elliptic curves*, Undergraduated Texts in Math., Springer (1992)
18. Tignol, J.P.: *Galois' theory of algebraic equations*, World Scientific (2001)
19. Washington, L.C.: *Elliptic curves, number theory and criptography*, 2d edition, Chapman & Hall (2008)
20. Weyl, H.: *The classical groups. Their invariants, their representations*, Princeton University Press (1939)