

ALGEBRA¹

Università degli Studi di Verona
– Corso di Laurea in Matematica Applicata –

* * *

Prof. Lidia Angeleri

Anno accademico 2015-2016²

¹**si veda la nota a pagina seguente!**

²appunti aggiornati in data 14 gennaio 2016

Nota importante:

Questi appunti **non** sono le dispense del corso, ma vogliono soltanto fornire un “filo rosso” attraverso il corso. Sicuramente il materiale qui raccolto non è sufficiente per preparare l’esame.

Lascio spazio apposito per poter **inserire le osservazioni, gli esempi, le dimostrazioni ecc.** che verranno presentati e discussi a lezione, e aggiungo riferimenti bibliografici per chi non segue le lezioni.

Buon lavoro!

Bibliografia:

S. BOSCH, *Algebra*, Springer, Unitext 2003.
I.N.HERSTEIN, *Algebra*, Editori Riuniti 2003.

Aspetti storici:

J.P.TIGNOL, *Galois’ Theory of Algebraic Equations*. World Scientific 2001.
J.DERBYSHIRE, *Unknown quantity. A real and imaginary history of algebra*. Plume 2006.
M.LIVIO, *L’equazione impossibile*. Rizzoli 2005.

Indice

I	<u>GRUPPI</u>	9
1	Gruppi e sottogruppi	9
1.1	Gruppo	9
1.2	Sottogruppo	9
1.3	Esempi	9
1.4	Laterale di G modulo H , ordine, indice.	10
1.5	Teorema di Lagrange	11
1.6	Lemma	11
2	Il gruppo quoziente	12
2.1	Sottogruppo normale	12
2.2	Il gruppo quoziente.	12
2.3	Esempi	12
2.4	Omomorfismo, isomorfismo	13
2.5	Nucleo e immagine di un omomorfismo.	13
2.6	Teorema di Fattorizzazione di Omomorfismi	14
2.7	Teorema Fondamentale dell'Omomorfismo	14
3	Gruppi ciclici	15
3.1	Esempio: I sottogruppi generati da un elemento in $(\mathbb{Z}/6\mathbb{Z}, +)$	15
3.2	L'ordine di un elemento	15
3.3	Gruppo ciclico	15
3.4	Classificazione dei gruppi ciclici	15
4	Il gruppo simmetrico	16
4.1	Teorema di Cayley	16
4.2	Permutazioni	16
4.3	Notazione per le permutazioni	16
4.4	Esempi	17
4.5	Il segno di una permutazione	17
4.6	Il gruppo alterno	18
4.7	Cicli disgiunti	18
4.8	Esempio	18
4.9	Scomposizione di permutazioni	18
5	Gruppi risolubili	20
5.1	Definizione	20
5.2	Proprietà del sottogruppo commutatore	20
5.3	Gruppi risolubili	21
5.4	Corollario	21
5.5	Risolubilità del gruppo simmetrico	21

II	<u>ANELLI</u>	23
6	Il concetto di anello	23
6.1	Definizione	23
6.2	Elemento invertibile. Campo	23
6.3	Sottoanello e sottocampo	23
6.4	Esempi	24
6.5	L'anello dei polinomi.	24
7	Ideali	25
7.1	Definizione.	25
7.2	Esempi.	26
7.3	L'anello quoziente di R modulo I	26
7.4	Esempio: $\mathbb{Z}/n\mathbb{Z}$	27
7.5	Omomorfismi	29
7.6	Nucleo e immagine.	29
7.7	Esempi	29
7.8	Teorema di Fattorizzazione di Omomorfismi	30
7.9	Teorema Fondamentale dell'Omomorfismo	30
7.10	Ideali massimali.	30
7.11	Esempi	30
8	Divisibilità	31
8.1	Anelli euclidei.	31
8.2	Esempi.	31
8.3	Dominio a ideali principali.	31
8.4	Divisibilità.	32
8.5	Massimo comun divisore e minimo comune multiplo.	32
8.6	L'Algoritmo Euclideo.	33
8.7	Elementi coprimi.	33
8.8	Bézout, Euclide, Diofanto	33
8.9	Elementi irriducibili.	34
8.10	Dominio a fattorizzazione unica.	34
III	<u>POLINOMI</u>	35
9	Zeri di polinomi	36
9.1	Polinomi irriducibili su un campo.	36
9.2	Zero di un polinomio	36
9.3	Teorema di Ruffini	37
9.4	Polinomi irriducibili di grado ≤ 3	37
9.5	Esempi.	38

10 Criteri di irriducibilità	39
10.1 Polinomi primitivi.	39
10.2 Riduzione modulo p	39
10.3 Criterio di Eisenstein.	39
10.4 Lemma di Gauss.	40
10.5 Proposizione	40
10.6 Esempi	41
10.7 Sostituzione	41
10.8 Esempio.	41
 IV CAMPI	 42
11 Estensioni algebriche	42
11.1 Estensione di un campo, grado dell'estensione	42
11.2 L'estensione di campi $K \subset F = K[x]/(f)$	42
11.3 Esempi	42
11.4 Teorema di Kronecker	43
11.5 Aggiunzioni, elementi algebrici, elementi trascendenti.	44
11.6 Il polinomio minimo	44
11.7 Esempi	45
11.8 Lemma sul grado	45
11.9 Corollario.	45
11.10 Esempi.	46
 12 Campi di riducibilità completa.	 46
12.1 Teorema e Definizione.	46
12.2 Esempi	47
12.3 Lemma.	48
12.4 Unicità del campo di riducibilità completa.	48
12.5 Estensioni normali.	49
12.6 Esempi.	49
12.7 Teorema.	49
12.8 Corollario.	50
 13 Separabilità	 50
13.1 La caratteristica di un campo.	50
13.2 Esempi	51
13.3 Teorema	51
13.4 Corollario: la cardinalità di un campo finito.	51
13.5 Molteplicità degli zeri.	52
13.6 La derivata formale di un polinomio.	52

13.7	Proposizione.	52
13.8	Teorema.	52
13.9	Polinomi separabili.	53
13.10	Esempi.	53
13.11	Campi perfetti.	54
13.12	Teorema.	54
13.13	Estensioni separabili.	54
V	<u>TEORIA DI GALOIS</u>	56
14	Campi intermedi e sottogruppi	56
14.1	Il campo fisso.	56
14.2	Lemma.	56
14.3	Lemma di Dedekind.	57
14.4	La traccia di un gruppo finito.	57
14.5	Teorema di Artin.	58
14.6	Il gruppo di Galois.	58
14.7	Esempi.	59
14.8	Teorema.	59
15	Estensioni di Galois	60
15.1	Teorema e Definizione.	60
15.2	Esempi	60
15.3	Teorema Fondamentale della Teoria di Galois	61
15.4	Calcolo del polinomio minimo	63
15.5	Teorema	63
15.6	Esempio	64
VI	<u>APPLICAZIONI DELLA TEORIA DI GALOIS</u>	65
16	Campi finiti	65
16.1	Lemma	65
16.2	Teorema di classificazione dei campi finiti	65
16.3	Lemma	66
16.4	Teorema dell'elemento primitivo	66
17	Risolubilità per radicali	68
17.1	Radici n -sime dell'unità	68
17.2	Radici n -sime di un elemento	68
17.3	Radici primitive	69
17.4	Osservazione	69

17.5	Estensione per radicali	69
17.6	Osservazioni	70
17.7	Equazioni risolubili per radicali	70
17.8	Teorema (Galois)	70
18	Risolubilità del polinomio generale di grado n	72
18.1	Il gruppo di Galois è dato da permutazioni.	73
18.2	Il caso $n \leq 4$	73
18.3	Esempi	73
18.4	Funzioni razionali simmetriche	74
18.5	Esempio	74
18.6	Funzioni simmetriche elementari	74
18.7	Proposizione	75
18.8	Teorema (Abel - Ruffini)	75
18.9	Ancora sul caso $n \leq 4$	76
19	Costruzioni con riga e compasso	78
19.1	Costruzioni elementari.	78
19.2	Esempi	78
19.3	Il campo intermedio dei numeri costruibili.	79
19.4	Lemma	79
19.5	Teorema.	80
19.6	Corollario (costruzioni impossibili).	80
19.7	Costruzione del poligono regolare.	81
20	Bibliografia	82

Parte I

GRUPPI

1 Gruppi e sottogruppi

1.1 Gruppo

Un *gruppo* $(G, +)$ è costituito da un insieme non vuoto G e un'operazione $+: G \times G \rightarrow G$, $(a, b) \mapsto a + b$ su G che gode delle seguenti proprietà:

(G1) associatività: $a + (b + c) = (a + b) + c$ per $a, b, c \in G$;

(G2) elemento neutro: $a + 0_G = 0_G + a = a$ per ogni $a \in G$;

(G3) elemento inverso: per ogni $a \in G$ esiste $b \in G$ tale che $a + b = b + a = 0_G$;

Il gruppo $(G, +)$ si dice *abeliano*¹ se vale anche la proprietà:

(G4) commutativa: $a + b = b + a$ per $a, b \in G$.

OSSERVAZIONI

(1) 0_G è univocamente determinato e per ogni $a \in G$ l'elemento inverso è univocamente determinato e si indica con $-a$.

(2) In un gruppo si ha la proprietà cancellativa:

se $a + x = a + y$ allora $x = y$ per $a, x, y \in G$.

(3) Si usa spesso la notazione moltiplicativa $(G, \cdot)$. In tal caso l'elemento neutro si indica con e oppure con 1_G e l'elemento inverso di a si indica con a^{-1} .

ESEMPI

(1) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$ sono gruppi abeliani. L'insieme $\text{Gl}(n, K)$ di tutte le matrici invertibili di ordine n su un campo K è un gruppo rispetto alla moltiplicazione di matrici, non è abeliano per $n \geq 2$.

(2) Sia A un insieme non vuoto e sia $S(A)$ l'insieme di tutte le applicazioni biettive $f: A \rightarrow A$. La composizione di applicazioni definisce un'operazione $\circ: S(A) \times S(A) \rightarrow S(A)$, $(f, g) \mapsto g \circ f$. Con questa operazione $(S(A), \circ)$ diventa un gruppo, in generale non abeliano.

1.2 Sottogruppo

Sia $(G, +)$ un gruppo. Un sottoinsieme non vuoto $H \subset G$ si dice *sottogruppo* di G se H è un gruppo rispetto all'operazione $+$ di G . In tal caso si scrive $H \leq G$.

OSSERVAZIONE

Un sottoinsieme $H \subset G$ è un sottogruppo se e solo se $H \neq \emptyset$ e per tutti gli $a, b \in H$ si ha $a - b \in H$.

1.3 Esempi

(0) L'insieme dei numeri dispari *non* forma un sottogruppo di $(\mathbb{Z}, +)$ perché non è chiuso rispetto all'operazione $+$.

(1) Ogni gruppo $(G, \cdot)$ possiede i sottogruppi banali $\{e\}$ e G .

¹Niels Abel, matematico norvegese (1802-1829)

(2) Il sottogruppo generato da un elemento. Sia $(G, \cdot)$ un gruppo con elemento neutro e . Per $a \in G$ e un intero $n \in \mathbb{Z}$ si pone

$$a^n = \begin{cases} \underbrace{a \cdot a \cdot \dots \cdot a}_n & \text{se } n > 0 \\ e & \text{se } n = 0 \\ \underbrace{a^{-1} \cdot a^{-1} \cdot \dots \cdot a^{-1}}_n & \text{se } n < 0 \end{cases}$$

L'insieme $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ è un sottogruppo di G , detto il *sottogruppo generato da a* .

(3) Il gruppo abeliano $(\mathbb{Z}, +)$. Il sottogruppo di $(\mathbb{Z}, +)$ generato da un elemento n è

$$\langle n \rangle = \{nz \mid z \in \mathbb{Z}\} = n\mathbb{Z}$$

I sottogruppi di $(\mathbb{Z}, +)$ sono precisamente i sottoinsiemi di forma $n\mathbb{Z}$ con $n \in \mathbb{N}_0$.

Infatti:

⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮

Dati $n \in \mathbb{N}_0$ e due numeri interi z, z' , si ha $z - z' \in \langle n \rangle = n\mathbb{Z}$ se e solo se il resto della divisione di z per n coincide con quello della divisione di z' per n . Per $0 \leq r \leq n - 1$ chiamiamo *classe di resto di r modulo n* l'insieme

$$\bar{r} = \{z \in \mathbb{Z} \mid r \text{ è il resto della divisione di } z \text{ per } n\} = \{nq + r \mid q \in \mathbb{Z}\}$$

Abbiamo quindi che $z - z' \in \langle n \rangle = n\mathbb{Z}$ se e solo se z e z' appartengono alla stessa classe di resto.

Si noti che le classi di resto $\bar{0}, \bar{1}, \dots, \overline{n-1}$ sono disgiunte a due a due, e la loro unione è $\mathbb{Z} = \bar{0} \cup \bar{1} \cup \dots \cup \overline{n-1}$.

1.4 Laterale di G modulo H , ordine, indice.

Ogni sottogruppo H di gruppo $(G, +)$ definisce una *relazione di equivalenza* su G

$$a \sim b \quad \text{se} \quad a - b \in H$$

La classe di equivalenza di un elemento a rispetto a $\sim$

$$\bar{a} = \{x \in G \mid x \sim a\} = \{h + a \mid h \in H\} = H + a$$

si chiama *laterale destro* di G modulo H con rappresentante a .

L'insieme di tutti i laterali destri si indica con

$$G/H = \{\bar{a} \mid a \in G\}.$$

L'*ordine* $|G|$ di G è il numero degli elementi dell'insieme G . Il gruppo G si dice *finito* se il suo ordine è finito. L'ordine di G/H (cioè il numero dei laterali destri di G modulo H) è detto *indice di H in G* e si indica con $[G : H]$.

DIMOSTRAZIONE :

⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮

ESEMPIO : I laterali (destri e sinistri) di $\mathbb{Z}$ modulo $n\mathbb{Z}$ sono esattamente le classi di resto $\overline{0}, \overline{1}, \dots, \overline{n-1}$.

1.5 Teorema di Lagrange

Sia $(G, +)$ un gruppo finito e sia $H \leq G$. Allora

$$|G| = |H| \cdot [G : H]$$

In particolare, l'ordine $|H|$ divide l'ordine $|G|$.

Per la dimostrazione serve il seguente

1.6 Lemma

Sia A un insieme non vuoto con una relazione di equivalenza $\sim$. Per $a, b \in A$ si ha

$$a \sim b \Leftrightarrow \bar{a} = \bar{b} \Leftrightarrow \bar{a} \cap \bar{b} \neq \emptyset.$$

Quindi $\sim$ induce una partizione su A : l'insieme A è l'unione di classi di equivalenza disgiunte a due a due.

DIMOSTRAZIONE :

⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮

DIMOSTRAZIONE del Teorema di Lagrange :

⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮

2 Il gruppo quoziente

Sia $(G, \cdot)$ un gruppo con sottogruppo $H \leq G$. Vogliamo definire un'operazione sui laterali come segue:

$$Ha \cdot Hb = Hab$$

Affinché l'operazione sia ben definita, dobbiamo garantire che

⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮

serve quindi la condizione seguente:

2.1 Sottogruppo normale

Un sottogruppo $H \leq G$ di un gruppo $(G, \cdot)$ si dice *normale* se soddisfa

$$aha^{-1} \in H \text{ per ogni } a \in G, h \in H.$$

In tal caso scriviamo $H \triangleleft G$.

OSSERVAZIONE : $H \triangleleft G$ se e solo se $aH = Ha$ per ogni $a \in G$ (Esercizio).

2.2 Il gruppo quoziente.

Sia $(G, \cdot)$ un gruppo con sottogruppo normale $H \triangleleft G$. Allora l'insieme dei laterali G/H con l'operazione

$$Ha \cdot Hb = Hab, \text{ ovvero } \bar{a} \cdot \bar{b} = \overline{ab},$$

è un gruppo con elemento neutro $e_{G/H} = \bar{e} = H$, detto *gruppo quoziente di G modulo H* .

Si ha $\bar{a} = \bar{e}$ se e solo se $a \in H$.

Infatti

⋮
⋮
⋮

2.3 Esempi

(1) Ogni sottogruppo di un gruppo abeliano è normale. Per un esempio di un sottogruppo non normale si vedano gli Esercizi.

(2) $(\mathbb{Z}/n\mathbb{Z}, +)$ è un gruppo rispetto all'operazione $\bar{a} + \bar{b} = \overline{a+b}$.

Per $n = 2$:

⋮
⋮
⋮
⋮
⋮
⋮
⋮

⋮

2.6 Teorema di Fattorizzazione di Omomorfismi

Sia $(G, \cdot)$ un gruppo con sottogruppo normale $H \triangleleft G$. Sia inoltre $f : G \rightarrow G'$ un omomorfismo tale che $H \subset \text{Ker} f$. Allora esiste uno e un solo omomorfismo $\bar{f} : G/H \rightarrow G'$ tale che

$$\bar{f} \nu = f.$$

Si ha $\text{Ker} \bar{f} = \text{Ker} f / H = \{\bar{x} \mid x \in \text{Ker} f\}$ e $\text{Im} \bar{f} = \text{Im} f$.

DIMOSTRAZIONE

⋮

2.7 Teorema Fondamentale dell'Omomorfismo

Sia $f : G \rightarrow G'$ un omomorfismo. Allora esiste uno e un solo omomorfismo $\bar{f} : G/\text{Ker} f \rightarrow G'$ tale che $\bar{f} \nu = f$. In particolare

$$G/\text{Ker} f \cong \text{Im} f.$$

DIMOSTRAZIONE

⋮

3 Gruppi ciclici

3.1 Esempio: I sottogruppi generati da un elemento in $(\mathbb{Z}/6\mathbb{Z}, +)$

⋮
⋮
⋮
⋮

3.2 L'ordine di un elemento

Sia $(G, \cdot)$ un gruppo e sia $a \in G$. L'ordine dell'elemento a è definito come $\text{ord}(a) = |\langle a \rangle|$.

(1) Se $a^l \neq a^k$ per $l \neq k$ allora $\text{ord}(a) = \infty$.

(2) Se esistono $l \neq k$ tali che $a^l = a^k$ allora $\text{ord}(a) = m < \infty$, dove m è il minimo intero positivo tale che $a^m = e$.

Infatti

⋮
⋮
⋮
⋮

COROLLARIO del Teorema di Lagrange

Se $|G| = n$, allora $\text{ord}(a)$ divide n e quindi $a^n = e$.

DIMOSTRAZIONE:

Per il Teorema di Lagrange si ha: $\text{ord}(a) = m \mid n$, quindi $n = mq$, e perciò $a^n = a^{mq} = (a^m)^q = e$. $\square$

3.3 Gruppo ciclico

Un gruppo $(G, \cdot)$ è detto *ciclico* se esiste un elemento $a \in G$ tale che $G = \langle a \rangle$.

In particolare, un gruppo ciclico è sempre abeliano.

3.4 Classificazione dei gruppi ciclici

Sia $(G, \cdot)$ un gruppo ciclico.

(1) Se $|G| = \infty$, allora $(G, \cdot) \cong (\mathbb{Z}, +)$.

(2) Se $|G| = m$ allora $(G, \cdot) \cong (\mathbb{Z}/m\mathbb{Z}, +)$.

DIMOSTRAZIONE:

Sia $G = \langle a \rangle$ con $a \in G$.

Allora nel caso (1) $f: \mathbb{Z} \rightarrow G, n \mapsto a^n$ è isomorfismo. Infatti $f(n+m) = a^{n+m} = a^n a^m = f(n)f(m)$.

Nel caso (2) analogamente $f: \mathbb{Z}/m\mathbb{Z} \rightarrow G, \bar{n} \mapsto a^n$ è un isomorfismo per il Teorema Fondamentale dell'Omomorfismo. $\square$

OSSERVAZIONE. Ogni gruppo che abbia un numero primo p di elementi è ciclico (e isomorfo a $\mathbb{Z}/p\mathbb{Z}$).

Infatti, se $a \in G \setminus \{e\}$, allora per il Teorema di Lagrange $\text{ord}(a)$ è un divisore di $|G| = p$ diverso da 1, e se p è primo segue $\text{ord}(a) = p$, quindi $\langle a \rangle = G$.

Vedremo in 4.4 che già per ordine 4 esistono gruppi non ciclici, e per ordine 6 esistono gruppi non abeliani.

4 Il gruppo simmetrico

4.1 Teorema di Cayley

Ogni gruppo G è isomorfo a un sottogruppo del gruppo simmetrico $(S(G), \circ)$.

DIMOSTRAZIONE

Ogni elemento $a \in G$ definisce un'applicazione biiettiva

$$f_a : G \rightarrow G, x \mapsto ax$$

Infatti, f_a è iniettiva per la proprietà cancellativa, ed è suriettiva poiché ogni elemento $b \in G$ può essere scritto come $b = aa^{-1}b = f_a(a^{-1}b)$. Abbiamo quindi un'applicazione

$$\iota : G \rightarrow S(G), a \mapsto f_a$$

Verifichiamo che ι è un omomorfismo: se $a, b \in G$, dobbiamo mostrare $\iota(ab) = \iota(a) \circ \iota(b)$, ovvero l'uguaglianza delle applicazioni $f_{ab} = f_a \circ f_b$. Prendiamo quindi un elemento $x \in G$ e controlliamo: $f_{ab}(x) = (ab)x = a(bx) = a f_b(x) = f_a(f_b(x)) = f_a \circ f_b(x)$.

Verifichiamo inoltre che ι è un'applicazione iniettiva: se $a, b \in G$ soddisfano $\iota(a) = \iota(b)$, ovvero l'uguaglianza delle applicazioni $f_a = f_b$, allora in particolare si ha $f_a(e) = f_b(e)$, che significa $a = b$.

A questo punto sappiamo (per il Teorema Fondamentale dell'Omomorfismo) che

$$G \cong \text{Im } \iota \leq S(G)$$

quindi abbiamo dimostrato il teorema.

4.2 Permutazioni

Consideriamo il gruppo simmetrico di un insieme finito A . Possiamo assumere $A = \{1, 2, \dots, n\}$. Il gruppo $S_n = S(A)$ è detto gruppo simmetrico su n oggetti e i suoi elementi si chiamano *permutazioni*. Abbiamo

$$|S_n| = n!$$

4.3 Notazione per le permutazioni

(1) Per indicare un elemento $\sigma \in S_n$ useremo la notazione

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$$

Ad esempio per $n = 3$ l'applicazione $\sigma : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$ con $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1$ si indica con

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

mentre

$$\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

indica l'applicazione $\tau : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$ con $\tau(1) = 2, \tau(2) = 1, \tau(3) = 3$.

(2) Una permutazione $\pi \in S_n$ è detta *ciclo di lunghezza k* se permuta ciclicamente k elementi di $\{1, 2, \dots, n\}$ e lascia fissi i restanti $n - k$ elementi, ovvero esistono $k \geq 2$ elementi distinti $m_1, \dots, m_k \in \{1, \dots, n\}$ tali che

$$\begin{aligned}\sigma(m_1) &= m_2 \\ \sigma(m_2) &= m_3 \\ &\vdots \\ \sigma(m_{k-1}) &= m_k \\ \sigma(m_k) &= m_1\end{aligned}$$

e $\sigma(m) = m$ per tutti gli altri elementi $m \in \{1, \dots, n\} \setminus \{m_1, \dots, m_k\}$. In tal caso possiamo anche scrivere

$$\pi = (m_1, \dots, m_k)$$

tralasciando dunque gli $n - k$ elementi fissati da π .

Ad esempio $\tau = (12) \in S_3$ è un ciclo di lunghezza 2, detto anche *trasposizione* o *scambio*, e $\sigma = (123)$ è un ciclo di lunghezza 3.

Ogni ciclo di lunghezza k è un elemento di S_n di ordine k .

Per ogni ciclo $\pi = (m_1, \dots, m_k) \in S_n$ e ogni permutazione $\sigma \in S_n$ si ha

$$\sigma \circ \pi \circ \sigma^{-1} = (\sigma(m_1), \dots, \sigma(m_k))$$

(vedi Esercizi).

4.4 Esempi

(1) S_3 è un gruppo di 6 elementi non abeliano, quindi in particolare non isomorfo a $\mathbb{Z}/6\mathbb{Z}$.

(2) L'insieme

$$\mathcal{V} = \{\text{id}, (12)(34), (13)(24), (14)(23)\} \subset S_4$$

è un sottogruppo normale di S_4 , detto *gruppo di Klein*², che è abeliano ma non ciclico, quindi in particolare non isomorfo a $\mathbb{Z}/4\mathbb{Z}$. Si dimostra che, a meno di isomorfismo, esistono solo due gruppi di quattro elementi: $\mathbb{Z}/4\mathbb{Z}$ e $\mathcal{V}$ - vedi Esercizi.

4.5 Il segno di una permutazione

Data una permutazione $\sigma \in S_n$, una coppia di numeri (i, j) con $1 \leq i < j \leq n$ è detta *inversione per σ* se $\sigma(i) > \sigma(j)$. Se r è il numero delle inversioni per σ , chiamiamo *segno* di σ il numero

$$\varepsilon(\sigma) = (-1)^r = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

Diremo che σ è *pari* se $\varepsilon(\sigma) = +1$, ovvero il numero delle inversioni è pari, altrimenti σ è detta *dispari*.

⋮
⋮
⋮
⋮
⋮
⋮

²Felix Klein, matematico tedesco (1849-1925)

Lemma: Dati un gruppo $(G, \cdot)$ e un insieme non vuoto A , supponiamo che G agisca su A , cioè che esista un'applicazione

$$G \times A \rightarrow A, (\sigma, x) \mapsto \sigma(x)$$

con le seguenti proprietà:

- (A1) $e(x) = x$ per ogni $x \in A$,
- (A2) $(\sigma\tau)(x) = \sigma(\tau(x))$.

Per ogni elemento $x \in A$ consideriamo l'orbita di x attraverso l'azione di G , cioè l'insieme

$$O(x) = \{\sigma(x) \mid \sigma \in G\}.$$

Le orbite degli elementi di A attraverso l'azione di G inducono una partizione di A , cioè A è l'unione di orbite disgiunte a due a due.

Dimostrazione: Consideriamo la relazione su A definita da

$$a \sim b \text{ se } a \in O(b).$$

E' una relazione riflessiva poiché $a = e(a) \in O(a)$; è simmetrica poiché $a \in O(b)$ significa che $a = \sigma(b)$ per un $\sigma \in G$ e implica $b = \sigma^{-1}(a) \in O(a)$; è transitiva perché se $a \in O(b)$ e $b \in O(c)$ allora $a = \sigma(b)$ e $b = \tau(c)$ con $\sigma, \tau \in G$ e perciò $a = \sigma\tau(c) \in O(c)$.

Abbiamo quindi una relazione di equivalenza le cui classi di equivalenza sono esattamente le orbite degli elementi di A attraverso l'azione di G . L'enunciato segue dunque da 1.6.

DIMOSTRAZIONE del Teorema: Sia adesso $G = \langle \sigma \rangle \leq S_n$ e sia $A = \{1, \dots, n\}$. Ovviamente G agisce su A attraverso l'operazione $G \times A \rightarrow A, (\sigma, x) \mapsto \sigma(x)$ e per (a) le orbite inducono una partizione

$$A = O(x_1) \cup \dots \cup O(x_r).$$

Ogni orbita è di forma

$$O(x_i) = \{x_i, \sigma(x_i), \sigma^2(x_i), \dots, \sigma^{m_i}(x_i)\}$$

per un $m_i \in \mathbb{N}_0$ opportuno. Per ogni i consideriamo il ciclo di ordine m_i

$$\tau_i = (x_i, \sigma(x_i), \sigma^2(x_i), \dots, \sigma^{m_i}(x_i))$$

Poiché le orbite sono disgiunte, anche i cicli $\tau_1, \dots, \tau_r$ sono disgiunti. E poiché l'unione delle orbite è tutto l'insieme A , si ha

$$\sigma = \tau_1 \dots \tau_r.$$

Tale scomposizione è unica a meno dell'ordine: se anche $\sigma = \rho_1 \dots \rho_s$, allora gli insiemi $\{x \in A \mid \rho_i(x) \neq x\}$, $1 \leq i \leq s$ determinano le orbite degli elementi di A attraverso l'azione di $G = \langle \sigma \rangle$. Quindi $r = s$ e $\{\tau_1, \dots, \tau_r\} = \{\rho_1, \dots, \rho_s\}$.

OSSERVAZIONI:

(1) Una permutazione è pari (rispettivamente, dispari) se e solo se può essere espressa come prodotto di un numero pari (rispettivamente, dispari) di trasposizioni.

(2) La scomposizione

$$\sigma = \tau_1 \circ \dots \circ \tau_r$$

in prodotto di trasposizioni non è unica, però il numero delle trasposizioni in qualsiasi scomposizione è unico a meno di congruenza modulo 2. Più precisamente: se abbiamo anche $\sigma = \rho_1 \circ \dots \circ \rho_s$, allora $\bar{r} = \bar{s} \in \mathbb{Z}/2\mathbb{Z}$, ovvero r, s sono entrambi pari o entrambi dispari.

(3) Possiamo adesso dare una descrizione alternativa del determinante di una matrice: Data una matrice $A = (a_{ij}) \in M_n(K)$ di ordine n su un campo K , si ha

$$\det A = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} \cdot a_{2\sigma(2)} \cdots a_{n\sigma(n)}$$

5 Gruppi risolubili

5.1 Definizione

Sia G un gruppo. Per $a, b \in G$ il *commutatore* di a e b è l'elemento

$$[a, b] = a b a^{-1} b^{-1}$$

Il sottogruppo di G generato da tutti i commutatori $[a, b]$ si denota con

$$K(G) = \langle \{ [a, b] \mid a, b \in G \} \rangle$$

ed è detto *sottogruppo commutatore* di G .

Per iterazione definiamo

$$\begin{aligned} K^2(G) &= K(K(G)) \\ K^{i+1}(G) &= K(K^i(G)) \end{aligned}$$

5.2 Proprietà del sottogruppo commutatore

Sia G un gruppo.

1. G è abeliano se e solo se $K(G) = \{e\}$.
2. Per ogni omomorfismo di gruppi $f : G \rightarrow G'$ si ha $f(K(G)) \subset K(G')$. Se f è suriettivo si ha addirittura $f(K(G)) = K(G')$.
3. $K(G)$ è un sottogruppo normale di G .
4. $K(G)$ è il più piccolo sottogruppo normale N di G tale che G/N sia abeliano.

DIMOSTRAZIONE

(1) per definizione.

(2) Un elemento di $K(G)$ è di forma

$$[a_1, b_1] \cdots [a_2, b_2] \cdots [a_n, b_n]$$

e per ogni $1 \leq i \leq n$ si ha

$$f([a_i, b_i]) = f(a_i)f(b_i)f(a_i)^{-1}f(b_i)^{-1} = [f(a_i), f(b_i)]$$

Quindi $f(K(G)) \subset K(G')$. Analogamente si dimostra l'altra inclusione quando f è suriettivo.

(3) Sia $a \in G$. Per l'automorfismo $f : G \rightarrow G, x \mapsto axa^{-1}$ abbiamo $a K(G) a^{-1} = f(K(G)) = K(G)$ per (2), quindi $K(G)$ è un sottogruppo normale di G .

(4) $G/K(G)$ è abeliano: per tutti gli elementi $a, b \in G$ si ha $ab(ba)^{-1} = [a, b] \in K(G)$, quindi nel gruppo quoziente $G/K(G)$ otteniamo $\bar{a}\bar{b} = \bar{b}\bar{a}$. Se inoltre N è un sottogruppo normale tale che G/N sia abeliano, allora per tutti gli elementi $a, b \in G$ abbiamo $Na Nb = Nb Na$ in G/N , ovvero $Nab = Nba$, quindi $[a, b] = ab(ba)^{-1} \in N$, che dimostra $K(G) \subset N$.

5.3 Gruppi risolubili

Per un gruppo G sono equivalenti i seguenti enunciati:

1. Esiste un $n \in \mathbb{N}_0$ tale che $K^n G = \{e\}$.
2. G possiede una catena finita di sottogruppi

$$\{e\} = N_n \leq N_{n-1} \leq \dots \leq N_2 \leq N_1 \leq G$$

con le proprietà

- (a) N_i è sottogruppo normale di N_{i-1} ,
- (b) il gruppo quoziente N_{i-1}/N_i è abeliano.

Con queste proprietà G è detto un *gruppo risolubile*.

DIMOSTRAZIONE

$\Rightarrow$: Per 5.2 (3) e (4)

$$\{e\} = K^n(G) \leq K^{n-1}(G) \leq \dots \leq K^2(G) \leq K(G) \leq G$$

è una catena di sottogruppi normali con quozienti abeliani.

$\Leftarrow$: Sia

$$\{e\} = N_n \leq N_{n-1} \leq \dots \leq N_2 \leq N_1 \leq G$$

una catena di sottogruppi tale che N_i è sottogruppo normale di N_{i-1} e il gruppo quoziente N_{i-1}/N_i è abeliano per ogni $1 \leq i \leq n$. Procediamo per induzione su n .

$n = 1$: in questo caso G è abeliano, quindi $K(G) = \{e\}$.

$n \rightarrow n + 1$: per l'ipotesi induttiva esiste $m \in \mathbb{N}$ tale che $K^m(N_1) = \{e\}$. Inoltre $K(G/N_1) = \{e_{G/N_1}\}$ poiché G/N_1 è abeliano. Applicando 5.2 (2) all'omomorfismo $\nu : G \rightarrow G/N_1$ vediamo che $\nu(K(G)) = \{e_{G/N_1}\}$, quindi $K(G) \subset \text{Ker } \nu = N_1$ e perciò $K^{m+1}(G) \subset K^m(N_1) = \{e\}$.

5.4 Corollario

Sia G un gruppo risolubile. Allora sono risolubili anche ogni sottogruppo $H \leq G$ e ogni gruppo quoziente G/N (dove N è un sottogruppo normale). Inoltre G è risolubile se (e solo se) esiste un sottogruppo normale N tale che N e G/N sono risolubili.

DIMOSTRAZIONE

Sia $K^n(G) = \{e\}$. Applicando 5.2 (2) all'immersione $H \hookrightarrow G$ e all'epimorfismo canonico $\nu : G \rightarrow G/N$ si ottiene $K^n(H) = \{e\}$ e $K^n(G/N) = \{e_{G/N}\}$.

Dato infine un gruppo G con un sottogruppo normale N tale che N e G/N sono risolubili, si procede come nella dimostrazione del passo induttivo in 5.3 per concludere che G è risolubile.

5.5 Risolubilità del gruppo simmetrico

Il gruppo S_n è risolubile se e solo se $n \leq 4$.

DIMOSTRAZIONE

(1) Ogni gruppo abeliano è risolubile: si scelga $\{e\} \leq G$. Quindi S_1 e S_2 sono risolubili.

(2) S_3 è risolubile:

$$\{\text{id}\} \leq A_3 \leq S_3$$

è una catena di sottogruppi normali dove i quozienti $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ e $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$ sono tutti abeliani.

(3) S_4 è risolubile:

$$\{\text{id}\} \leq \mathcal{V} \leq A_4 \leq S_4$$

è una catena di sottogruppi normali dove i quozienti $\mathcal{V}$, $A_4/\mathcal{V} \cong \mathbb{Z}/3\mathbb{Z}$ e $S_4/A_4 \cong \mathbb{Z}/2\mathbb{Z}$ sono tutti abeliani.

(4) S_n non è risolubile se $n \geq 5$:

(i) Verifichiamo che se N è un sottogruppo normale di S_n che contiene tutti i 3-cicli, anche $K(N)$ è un sottogruppo normale di S_n che contiene tutti i 3-cicli: infatti $K(N)$ è normale in S_n poiché segue da 5.2(2) che $\sigma K(N) \sigma^{-1} = K(\sigma N \sigma^{-1}) = K(N)$. Inoltre N deve contenere $a = (123)$ e $b = (145)$ (stiamo usando $n \geq 5$), quindi $K(N)$ contiene $[a, b] = (123)(145)(321)(541) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots & n \\ 2 & 4 & 3 & 1 & 5 & \dots & n \end{pmatrix} = (124)$,

ed essendo un sottogruppo normale, $K(N)$ deve contenere anche $\sigma^{-1}(124)\sigma$ per tutte le permutazioni $\sigma \in S_n$. Allora ogni 3-ciclo (xyz) con $x, y, z \in \{1, \dots, n\}$ appartiene a $K(N)$ poiché possiamo scrivere $(xyz) = \sigma^{-1}(124)\sigma$ scegliendo una permutazione σ con $\sigma(1) = x, \sigma(2) = y, \sigma(4) = z$, vedi Esercizi.

(ii) Poiché $G = S_n$ contiene tutti i 3-cicli, deduciamo da (i) che $K(G)$ contiene tutti i 3-cicli, quindi anche $K^2(G)$, anche $K^3(G), \dots$, anche $K^n(G)$ per qualsiasi $n \in \mathbb{N}$. Da 5.3 segue che G non è risolubile.

Parte II

ANELLI

6 Il concetto di anello

6.1 Definizione

Un anello $(R, +, \cdot)$ è costituito da un insieme non vuoto R e due operazioni $+, \cdot : R \times R \rightarrow R$ su R che godono delle proprietà:

(R1) $(R, +)$ è un gruppo abeliano con elemento neutro 0_R ;

(R2) $(R, \cdot)$ gode della proprietà associativa e possiede un elemento neutro 1_R ;

(R3) Leggi distributive:

$$a(b + c) = ab + ac,$$

$$(a + b)c = ac + bc.$$

Un anello si dice *commutativo* se $(R, \cdot)$ gode della proprietà commutativa.

OSSERVAZIONI:

(1) $a \cdot 0_R = 0_R \cdot a = 0_R$ per $a \in R$.

Infatti $a \cdot 0_R + a \cdot a = a \cdot (0_R + a) = a \cdot a$ quindi $a \cdot 0_R = 0_R$.

(2) $(-a) \cdot b = a \cdot (-b) = -a \cdot b$ per $a, b \in R$.

(3) 0_R e 1_R sono univocamente determinati. Se $R \neq \{0_R\}$ allora $1_R \neq 0_R$.

Da ora in poi i nostri anelli saranno tutti diversi da zero: $R \neq \{0_R\}$.

6.2 Elemento invertibile. Campo

Sia $(R, +, \cdot)$ un anello.

(1) Un elemento $a \in R$ è *invertibile* se esiste un elemento $b \in R$ tale che $ab = ba = 1_R$.

In tal caso b è univocamente determinato e si indica con a^{-1} .

(2) Sia R^* l'insieme di tutti gli elementi invertibili dell'anello R . Sicuramente $R^* \subset R \setminus \{0\}$ e $(R^*, \cdot)$ è un gruppo con elemento neutro 1_R .

(3) $(R, +, \cdot)$ si dice *campo* se R è commutativo e $R^* = R \setminus \{0\}$, in altre parole, se $(R \setminus \{0\}, \cdot)$ è un gruppo abeliano.

(4) $(R, +, \cdot)$ si dice *dominio* (di integrità) se R è commutativo e non possiede divisori di zero, ovvero se non esistono elementi $x, y \in R \setminus \{0\}$ tali che $x \cdot y = 0$.

6.3 Sottoanello e sottocampo

Sia $(R, +, \cdot)$ un anello (un campo). Un sottoinsieme $S \subset R$ si dice *sottoanello* (*sottocampo*) se $1_R \in S$ e S è un anello (un campo) rispetto alle operazioni $+$ e $\cdot$ definite in R .

OSSERVAZIONE:

(1) Un sottoinsieme $S \subset R$ è un sottoanello se e solo se:

(i) $(S, +)$ è un sottogruppo del gruppo abeliano $(R, +)$,

(ii) $1_R \in S$,

(iii) se $x, y \in S$, allora $x \cdot y \in S$.

(2) Un sottoinsieme $S \subset R$ è un sottocampo se e solo se:

- (i) $(S, +)$ è un sottogruppo del gruppo abeliano $(R, +)$,
- (ii) $(S \setminus \{0\})$ è un sottogruppo del gruppo abeliano $(R \setminus \{0\}, \cdot)$.

6.4 Esempi

- (1) $(\mathbb{Z}, +, \cdot)$ è un anello con $Z^* = \{1, -1\}$.
- (2) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$ sono campi. Si ha una catena di sottocampi $\mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}$.
- $(\mathbb{Z}, +, \cdot)$ è sottoanello di $(\mathbb{Q}, +, \cdot)$.
- (3) Ogni campo è un dominio. $\mathbb{Z}$ è un dominio, ma non un campo.
- (4) Le matrici quadrate di ordine n su un campo K formano un anello $(K^{n \times n}, +, \cdot)$ non commutativo, con divisori di zero. Ad esempio:

$$\begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Si ha $(K^{n \times n})^* = \{A \in K^{n \times n} \mid \det A \neq 0\} = GL(n, K)$.

- (5) Se $R_1, \dots, R_n$, $n \geq 2$ sono anelli, anche il loro prodotto cartesiano $R = R_1 \times \dots \times R_n$ è un anello rispetto all'addizione e moltiplicazione per componenti. Si ha $0_R = (0_{R_1}, \dots, 0_{R_n})$ e $1_R = (1_{R_1}, \dots, 1_{R_n})$.
- (6) Siano I un insieme non vuoto e R un anello. L'insieme R^I di tutte le applicazioni $f : I \rightarrow R$ è un anello rispetto a

$$f + g : I \rightarrow R, x \mapsto f(x) + g(x)$$

$$f \cdot g : I \rightarrow R, x \mapsto f(x) \cdot g(x)$$

Si ha $1 : I \rightarrow R, x \mapsto 1$ e $0 : I \rightarrow R, x \mapsto 0$.

Se I è uno spazio topologico, allora l'insieme $\mathcal{C}(I, R)$ di tutte le funzioni continue è un sottoanello di R^I . In particolare, per $I = \mathbb{N}_0 = \{0, 1, 2, \dots\}$, otteniamo l'anello $R^{\mathbb{N}_0}$ di tutte le successioni di elementi di R .

6.5 L'anello dei polinomi.

- (1) Dato un anello R , l'insieme $R^{(\mathbb{N}_0)}$ di tutte le successioni $(a_0, a_1, a_2, \dots)$ di elementi di R con $a_n = 0$ per quasi tutti gli n è un anello rispetto a

$$(a_0, a_1, \dots) + (b_0, b_1, \dots) = (a_0 + b_0, a_1 + b_1, \dots)$$

$$(a_0, a_1, \dots) \cdot (b_0, b_1, \dots) = (a_0 \cdot b_0, a_0 b_1 + a_1 b_0, \dots, \sum_{i=0}^n a_i b_{n-i}, \dots)$$

Si ha $0 = (0, \dots)$ e $1 = (1, 0, \dots)$.

- (2) Per $x = (0, 1, 0, \dots)$ si ottiene $x^2 = (0, 0, 1, 0, \dots)$, $x^3 = (0, 0, 0, 1, 0, \dots)$ ecc.

Quindi possiamo scrivere ogni elemento

$$(a_0, a_1, a_2, \dots) = \sum_{i=0}^n a_i x^i$$

(4) Data una famiglia $(I_k)_{k \in K}$ di ideali, anche la *somma* $\sum_{k \in K} I_k = \{\sum_{i=1}^n a_i \mid n \in \mathbb{N}, a_k \in I_k\}$ e l'intersezione $\bigcap_{k \in K} I_k$ sono ideali.

(5) Ogni sottoinsieme non vuoto $A \subset R$ di un anello R definisce un ideale

$$(A) = \bigcap \{I \mid I \subset R \text{ è un ideale con } A \subset I\},$$

il più piccolo ideale di R che contiene l'insieme A , detto *l'ideale generato da A* .

Per $A = \{a_1, \dots, a_r\}$ scriviamo

$$(A) = (a_1, \dots, a_r).$$

Se R è commutativo, allora

$$(A) = \left\{ \sum_{i=1}^n r_i a_i \mid n \in \mathbb{N}, r_1, \dots, r_n \in R, a_1, \dots, a_n \in A \right\}$$

In particolare, ogni elemento $a \in R$ definisce un ideale

$$(a) = \{ra \mid r \in R\}$$

detto *ideale principale* generato da a .

7.2 Esempi.

(1) Ogni campo possiede soltanto gli ideali banali 0 e K .

(2) Gli ideali di $\mathbb{Z}$ sono tutti principali.

Infatti:

$\vdots$
 $\vdots$
 $\vdots$
 $\vdots$

(2) Siano $A \subset I$ due insiemi e sia R un anello. Allora $\mathcal{N}(A) = \{f \in R^I \mid f|_A = 0\}$ è un ideale di R^I .

7.3 L'anello quoziente di R modulo I

Sia $(R, +, \cdot)$ un anello e sia $I \subset R$ un ideale. Poichè $I \leq (R, +)$ possiamo considerare i laterali (destri o sinistri) di $(R, +)$ modulo I . Per $a \in R$ si pone

$$\bar{a} = \{x \in R \mid x - a \in I\} = \{a + y \mid y \in I\} = a + I$$

Si ha che $\bar{a} = \bar{a'}$ se e solo se $a - a' \in I$.

L'insieme di tutti i laterali di R modulo I si indica con R/I . Definiamo le operazioni seguenti su R/I :

$$\begin{aligned} \bar{a} + \bar{b} &= \overline{a + b} \\ \bar{a} \cdot \bar{b} &= \overline{ab} \end{aligned}$$

Le operazioni sono ben definite:

⋮
⋮
⋮
⋮
⋮
⋮

Con queste operazioni R/I diventa un anello, detto l'*anello quoziente di R modulo I* , con

$$0_{R/I} = \bar{0} = 0 + I = I$$

$$1_{R/I} = \bar{1} = 1 + I$$

7.4 Esempio: $\mathbb{Z}/n\mathbb{Z}$.

Per $n \in \mathbb{N}$ consideriamo $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$, l'anello quoziente di $\mathbb{Z}$ rispetto all'ideale $I = n\mathbb{Z}$.

(1) Abbiamo

$$\mathbb{Z}/n\mathbb{Z}^* = \{\bar{a} \mid 0 < a < n, \text{MCD}(a, n) = 1\}.$$

Infatti $\bar{a}$ è invertibile se e solo se esiste $\bar{\alpha}$ tale che $\bar{\alpha}\bar{a} = \bar{1}$, ovvero esistono $\alpha, \beta \in \mathbb{Z}$ tali che $\alpha a + \beta n = 1$. Ma ciò significa proprio che i numeri a ed n sono primi tra loro (identità di Bézout, vedi 8.8), cioè $\text{MCD}(a, n) = 1$. Vedremo in 8.6 come determinare i numeri α e β attraverso l'Algoritmo Euclideo.

Concludiamo immediatamente che

(2) $\mathbb{Z}/n\mathbb{Z}$ è un campo se e solo se n è un numero primo.

(3) **La funzione di Eulero**³: Per ogni n denotiamo con $\varphi(n)$ il numero di tutti i numeri naturali $0 < a < n$ che sono primi con n , ovvero

$$\varphi(n) = |\mathbb{Z}/n\mathbb{Z}^*|$$

Otteniamo così una funzione $\varphi : \mathbb{N} \rightarrow \mathbb{N}$, detta *funzione di Eulero*, che si calcola come segue: Se $p_1, \dots, p_r$ sono i divisori primi distinti di n , ovvero $n = p_1^{m_1} \cdot p_r^{m_r}$, allora

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_r}\right)$$

In particolare, per ogni numero primo p si ha

$$\varphi(p) = p - 1$$

(4) **Teorema di Fermat⁴-Eulero**. Dati due numeri naturali $a, n \in \mathbb{N}$ che siano primi tra loro, in $\mathbb{Z}/n\mathbb{Z}$ si ha sempre

$$\bar{a}^{\varphi(n)} = \bar{1}$$

⋮
⋮
⋮
⋮
⋮
⋮

(5) **Piccolo Teorema di Fermat**. Dati un numero naturale $a \in \mathbb{N}$ e un numero primo p che non divida a , in $\mathbb{Z}/p\mathbb{Z}$ si ha sempre

$$\bar{a}^{p-1} = \bar{1}$$

⋮
⋮

³Leonhard Euler, matematico svizzero (1707-1783)

⁴Pierre de Fermat, matematico francese (1601-1665)

L'algoritmo RSA (Rivest-Shamir-Adleman)

Supponiamo che una persona (una banca, un sito web...) voglia farsi inviare messaggi criptati da altre persone (clienti, utenti...). Per permettere una transazione semplice e veloce, invece di concordare una chiave di criptazione segreta con ciascun utente, spesso si preferisce usare una *chiave pubblica*.

Per garantire la sicurezza di un tale sistema di criptazione serve una procedura *asimmetrica*: dev'essere facile produrre la chiave di criptazione, ma dev'essere praticamente impossibile risalire da questa alla chiave di decrittazione. Nel 1977 Rivest, Shamir e Adleman⁵ ebbero l'idea di sfruttare il fatto che è facile trovare numeri primi p, q molto grandi (attraverso opportuni test di primalità) e calcolare il loro prodotto $n = p \cdot q$, mentre è praticamente impossibile, dato n , risalire alla scomposizione in fattori primi $n = p \cdot q$. Quando si dice "praticamente impossibile" si intende che il tempo necessario a trovare p e q con i mezzi attualmente a disposizione è così lungo da rendere irrilevante la soluzione; basterà cioè sostituire di tanto in tanto i numeri p e q per garantire la sicurezza del sistema (naturalmente soltanto finché non saranno disponibili metodi più veloci per la fattorizzazione in numeri primi...)

Vediamo in dettaglio come funziona l'algoritmo di Rivest, Shamir e Adleman. Dati numeri primi p, q molto grandi (di 300 e più cifre), poniamo

$$n = p \cdot q,$$

$$m = \varphi(n) = (p-1)(q-1)$$

e scegliamo un numero naturale $1 < a < m$ che sia primo con m .

Vogliamo inviare un *messaggio* che, con qualche procedimento, è stato trasformato in una sequenza di numeri di lunghezza inferiore a $\min(p, q)$. Il nostro messaggio è quindi un numero $1 \leq x < \min(p, q) < n$.

La *chiave di criptazione* è (a, n) :

per la cifratura di un messaggio $1 \leq x < \min(p, q) < n$ si trasforma x nell'intero $y \in \{1, \dots, n-1\}$ con

$$\bar{y} = \bar{x}^a \text{ in } \mathbb{Z}/n\mathbb{Z}.$$

La *chiave di decrittazione* è (α, n) :

per la decifrazione di un messaggio $y \in \{1, \dots, n-1\}$ si trasforma y nell'intero $x' \in \{1, \dots, n-1\}$ con

$$\bar{x}' = \bar{y}^\alpha \text{ in } \mathbb{Z}/n\mathbb{Z},$$

dove $\alpha \in \{1, \dots, n-1\}$ è determinato dall'elemento inverso $\bar{\alpha} = \bar{a}^{-1}$ di $\bar{a}$ nell'anello $\mathbb{Z}/m\mathbb{Z}$, vedi 7.4, 8.6.

Per chi conosce soltanto la chiave di criptazione (a, n) è praticamente impossibile risalire a m e α . Quindi si può rendere pubblica la chiave (a, n) e mantenere segreta (α, n) , o anche viceversa.

Verifichiamo che $x = x'$. sappiamo che $\bar{\alpha} \cdot \bar{a} = \bar{1}$, quindi $\alpha a = 1 + \beta m$ per un $\beta \in \mathbb{Z}$, e perciò

$$\bar{x}' = \bar{y}^\alpha = \bar{x}^{\alpha a} = \bar{x}^{1+\beta m} = \bar{x} \cdot \bar{x}^{\beta m} \text{ in } \mathbb{Z}/n\mathbb{Z}.$$

Ricordando che $m = \varphi(n)$ e che $x < \min(p, q)$ è primo con n , segue dal Teorema di Fermat-Eulero

$$\bar{x}^{\beta m} = (\bar{x}^{\varphi(n)})^\beta = \bar{1} \text{ in } \mathbb{Z}/n\mathbb{Z}$$

e pertanto

$$\bar{x}' = \bar{x} \text{ in } \mathbb{Z}/n\mathbb{Z}.$$

Poiché $x, x' \in \{1, \dots, n-1\}$, possiamo dunque concludere che $x = x'$.

⁵matematici e informatici al Massachusetts Institute for Technology

7.5 Omomorfismi

Siano R e S due anelli.

Un'applicazione $\varphi : R \rightarrow S$ si dice:

- *omomorfismo* se per tutti gli elementi $a, b \in R$ si ha:

$$\varphi(a + b) = \varphi(a) + \varphi(b),$$

$$\varphi(ab) = \varphi(a) \cdot \varphi(b),$$

$$\varphi(1_R) = 1_S;$$

- *monomorfismo* se φ è un omomorfismo iniettivo,

- *epimorfismo* se φ è un omomorfismo suriettivo,

- *isomorfismo* se φ è un omomorfismo biiettivo.

Se esiste un isomorfismo $\varphi : R \rightarrow S$, si dice che R e S sono isomorfi e si scrive $R \cong S$.

7.6 Nucleo e immagine.

Siano R, S anelli e $\varphi : R \rightarrow S$ un omomorfismo.

1. $\text{Ker}\varphi = \{a \in R \mid \varphi(a) = 0\}$ è un ideale di R , detto il *nucleo* di φ .

2. $\text{Im}\varphi = \{\varphi(a) \mid a \in R\}$ è un sottoanello di S .

3. $\varphi(0_R) = 0_S$. Inoltre φ è un monomorfismo se e solo se $\text{Ker}\varphi = 0$.

DIMOSTRAZIONE

⋮
⋮
⋮
⋮
⋮
⋮

7.7 Esempi

(1) Se $R \subset S$ è un sottoanello, allora l'inclusione $R \hookrightarrow S$ è un monomorfismo di anelli. In particolare, $\varphi : \mathbb{Z} \hookrightarrow \mathbb{Q}$ è un monomorfismo; si noti che la sua immagine $\text{Im}\varphi = \mathbb{Z}$ non è un ideale di $\mathbb{Q}$.

(2) Sia R un dominio. L'applicazione

$$\varphi : R[x] \rightarrow R, f = \sum_{i=0}^n a_i x^i \mapsto a_0$$

è un epimorfismo con nucleo $\text{Ker}\varphi = (x)$.

Infatti

⋮
⋮
⋮
⋮
⋮
⋮
⋮

(3) Siano K un campo ed R un anello. Ogni omomorfismo di anelli $K \rightarrow R$ è iniettivo.

Infatti

⋮

(4) L'applicazione

$$\nu : R \rightarrow R/I, x \mapsto \bar{x} = x + I$$

è un epimorfismo con nucleo $\text{Ker} \nu = I$, detto *epimorfismo canonico*.

Come in 2.6 e 2.7 si dimostra

7.8 Teorema di Fattorizzazione di Omomorfismi

Siano R un anello e I un ideale di R con l'epimorfismo canonico $\nu : R \rightarrow R/I$. Sia inoltre $f : R \rightarrow S$ un omomorfismo di anelli tale che $f(I) = 0$. Allora esiste uno e un solo omomorfismo $\bar{f} : R/I \rightarrow S$ tale che

$$\bar{f} \nu = f.$$

Si ha $\text{Ker} \bar{f} = \text{Ker} f / I = \{\bar{x} \mid x \in \text{Ker} f\}$ e $\text{Im} \bar{f} = \text{Im} f$.

7.9 Teorema Fondamentale dell'Omomorfismo

Siano R, S anelli e sia $\varphi : R \rightarrow S$ un omomorfismo. Allora $R/\text{Ker} \varphi \cong \text{Im} \varphi$.

7.10 Ideali massimali.

Dato un anello R , gli ideali propri di R formano un insieme ordinato rispetto all'inclusione $\subset$. Gli elementi massimali sono detti *ideali massimali* di R . Quindi un ideale proprio $I \subset R$ è massimale se e solo se per ogni ideale A con $I \subset A \subset R$ si ha $I = A$ oppure $A = R$.

Osservazione. Sia R un anello commutativo. Un ideale I di R è massimale se e solo se R/I è un campo.

DIMOSTRAZIONE :

⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮

7.11 Esempi

(1) Gli ideali massimali di $\mathbb{Z}$ sono gli ideali di forma $p\mathbb{Z}$ con p primo.

(2) Siano I un insieme, $x \in I$ e K un campo. Allora

$$\{f \in K^I \mid f(x) = 0\}$$

è un ideale massimale di K^I .

⋮
⋮
⋮
⋮
⋮

8.4 Divisibilità.

Dati due elementi $x, y \in R$ di un dominio R , diremo che

- x divide y , e scriveremo $x \mid y$, se esiste $r \in R$ tale che $rx = y$, ovvero se $y \in (x)$.
- $x, y \in R$ sono associati, e scriveremo $x \sim y$, se x divide y e y divide x , ovvero se $(x) = (y)$.

OSSERVAZIONE: Due numeri interi $x, y \in \mathbb{Z}$ sono associati in $\mathbb{Z}$ se e solo se $x = y$ oppure $x = -y$. Più in generale, in un dominio R si ha $x \sim y$ se e solo se esiste $r \in R^*$ tale che $y = rx$.

Infatti

⋮
⋮
⋮
⋮
⋮

8.5 Massimo comun divisore e minimo comune multiplo.

Lemma e Definizione. Sia (R, δ) un anello euclideo e siano $a_1, \dots, a_n \in R \setminus \{0\}$. Allora esistono

- un elemento $d \in R$, detto *massimo comun divisore* di $a_1, \dots, a_n$, tale che
 1. d è comun divisore: $d \mid a_i$ per ogni $1 \leq i \leq n$,
 2. d è multiplo di qualsiasi altro comun divisore: se $t \mid a_i$ per ogni $1 \leq i \leq n$, allora $t \mid d$;
- un elemento $m \in R$, detto *minimo comune multiplo* di $a_1, \dots, a_n$, tale che
 1. m è comune multiplo: $a_i \mid m$ per ogni $1 \leq i \leq n$,
 2. m divide qualsiasi altro comune multiplo: se $a_i \mid c$ per ogni $1 \leq i \leq n$, allora $m \mid c$.

Gli elementi d e m sono univocamente determinati a meno di associazione.

Scriveremo $d = MCD(a_1, \dots, a_n)$ e $m = mcm(a_1, \dots, a_n)$.

DIMOSTRAZIONE:

Per 8.3 esiste $d \in R$ tale che

$$(d) = (a_1, \dots, a_n).$$

Si verifica che d è massimo comun divisore di $a_1, \dots, a_n$:

1. d è comun divisore poiché $a_1, \dots, a_n \in (d)$.
2. Se t è comun divisore di $a_1, \dots, a_n$, allora $a_1, \dots, a_n \in (t)$ e anche $(a_1, \dots, a_n) = \{\sum_{i=1}^n r_i a_i \mid r_1, \dots, r_n \in R\} \subset (t)$, quindi $d \in (t)$, e pertanto t deve dividere anche d .

Inoltre, se anche d' è massimo comun divisore, allora d è multiplo del comun divisore d' , e d' è multiplo del comun divisore d , quindi $d \sim d'$.

Infine, per 8.3 esiste anche $m \in R$ tale che

$$(m) = (a_1) \cap \dots \cap (a_n).$$

Si verifica analogamente che m è minimo comune multiplo di $a_1, \dots, a_n$ e che come tale è univocamente determinato a meno di associazione. $\square$

OSSERVAZIONE. In $\mathbb{Z}$ il massimo comun divisore e il minimo comune multiplo sono univocamente determinati a meno del segno, cf. l'osservazione in 8.4.

DIMOSTRAZIONE:

$$I_1 \subset I_2 \subset I_3 \subset \dots R$$

Infatti

.....

(3) Per dimostrare (i), supponiamo per assurdo che esistano elementi in $R \setminus (R^* \cup \{0\})$ senza scomposizione in irriducibili. Consideriamo l'insieme S di tutti gli ideali principali generati da tali elementi. Abbiamo visto in (2) che questo insieme deve contenere un elemento massimale I . Per definizione $I = (a)$ è generato da un elemento a che non è irriducibile, né invertibile, né zero. Quindi esistono due elementi non invertibili $x, y \in R$ tali che $a = x \cdot y$. Abbiamo dunque che l'ideale I è propriamente contenuto negli ideali (x) e (y) . Per la massimalità di I ciò implica che (x) e (y) non appartengono all'insieme S e significa quindi che sia x che y possono essere scritti come prodotto di elementi irriducibili. Ma allora lo stesso vale per $a = x \cdot y$, e otteniamo la contraddizione desiderata.

.....

⁹Emmy Noether, matematica tedesca (1882-1935)

⋮
⋮
⋮
⋮
⋮

9.5 Esempi.

(1) **Teorema Fondamentale dell'Algebra:** I polinomi irriducibili di $\mathbb{C}[x]$ sono i polinomi di grado 1. Quindi ogni $f \in \mathbb{C}[x]$ è di forma $f = a(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$ con $a, \alpha_1, \dots, \alpha_n \in \mathbb{C}$.

(2) Sia $f = x^n - a \in \mathbb{C}[x]$. Gli zeri di f sono le radici n-sime di a .
Ricordiamo: ponendo

$$a = r(\cos \alpha + i \sin \alpha)$$

in forma trigonometrica, le radici n-sime di a sono

$$z_k = \sqrt[n]{r} \left(\cos \frac{\alpha + 2\pi k}{n} + i \sin \frac{\alpha + 2\pi k}{n} \right), \quad k = 0, 1, \dots, n-1.$$

(3) Sia $f = x^4 + 1 \in \mathbb{C}[x]$ (caso $n = 4, a = -1$). Vediamo che $f = gh$ con $g, h \in \mathbb{R}[x]$ di grado 2, dunque f non è irriducibile in $\mathbb{R}[x]$ pur non avendo zeri in $\mathbb{R}$, e l'enunciato di 9.4(3) non può essere esteso a polinomi di grado superiore!

Infatti gli zeri di $f \in \mathbb{C}$ sono le radici quarte di $-1 = \cos \pi + i \sin \pi$,

cioè $z_k = \cos \frac{\pi + 2\pi k}{4} + i \sin \frac{\pi + 2\pi k}{4}$, $k = 0, 1, 2, 3$, in particolare

$$z_0 = \cos \frac{\pi}{4} + i \sin \frac{\pi}{4} = \frac{1}{2}\sqrt{2} + i\frac{1}{2}\sqrt{2}$$

$$z_1 = \cos \frac{3\pi}{4} + i \sin \frac{3\pi}{4} = -\frac{1}{2}\sqrt{2} + i\frac{1}{2}\sqrt{2}.$$

Quindi $f = \underbrace{(x - z_0)(x - \bar{z}_0)}_g \underbrace{(x - z_1)(x - \bar{z}_1)}_h \in \mathbb{C}[x]$ con $g = x^2 - \sqrt{2}x + 1$ e $h = x^2 + \sqrt{2}x + 1$.

Infatti

⋮
⋮
⋮
⋮
⋮
⋮

(4) I polinomi irriducibili in $\mathbb{R}[x]$ sono esattamente i polinomi di primo grado e quelli di secondo grado $f = a_0 + a_1x + a_2x^2$ con $a_0, a_1 \in \mathbb{R}$, $a_2 \in \mathbb{R} \setminus \{0\}$ e $\Delta = a_1^2 - 4a_0a_2 < 0$.

Infatti

⋮
⋮
⋮
⋮
⋮

Quindi ogni polinomio $f \in \mathbb{R}[x]$ è prodotto di polinomi di grado ≤ 2 in $\mathbb{R}[x]$.

(5) Il polinomio $f = x^2 + x + 1$ è irriducibile su $\mathbb{Z}/2\mathbb{Z}$ ma non su $K = \mathbb{Z}/3\mathbb{Z}$.

Il polinomio $x^4 + x^2 + 1 = (x^2 + x + 1)^2$ è riducibile su $\mathbb{Z}/2\mathbb{Z}$ pur non avendo zeri.

Il polinomio $f = 2x + 2 = 2(x + 1)$ è irriducibile in $\mathbb{Q}[x]$, ma non in $\mathbb{Z}[x]$. Il polinomio $6x^2 + 5x + 1 = (3x + 1)(2x + 1) \in \mathbb{Z}[x]$ è riducibile di grado 2, pur non avendo zeri in $\mathbb{Z}$.

10 Criteri di irriducibilità

10.1 Polinomi primitivi.

OSSERVAZIONE: Per ogni polinomio $0 \neq f \in \mathbb{Q}[x]$ esiste $0 \neq \alpha \in \mathbb{Q}$ tale che $\alpha \cdot f$ sia un polinomio di $\mathbb{Z}[x]$ con coefficienti coprimi. Un polinomio in $\mathbb{Z}[x] \setminus \{0\}$ i cui coefficienti sono coprimi si dice *primitivo*. Ad esempio, se $f = \frac{2}{3} + \frac{4}{7}x^2$, possiamo prendere $\alpha = \frac{21}{2}$ per ottenere il polinomio primitivo $\alpha \cdot f = 7 + 6x^2$. Ovviamente f è irriducibile in $\mathbb{Q}[x]$ se e solo se $\alpha \cdot f$ è irriducibile in $\mathbb{Q}[x]$. Vedremo in 10.5 che basta esaminare l'irriducibilità su $\mathbb{Z}$, cioè: f è irriducibile in $\mathbb{Q}[x]$ se e solo se $\alpha \cdot f$ è irriducibile in $\mathbb{Z}[x]$.

ESEMPLI.

- (1) Ogni polinomio monico è primitivo.
- (2) Ogni polinomio irriducibile $f \in \mathbb{Z}[x]$ di grado $n > 0$ è primitivo. Altrimenti otteniamo una fattorizzazione non banale $f = d \cdot f'$ dove $d \in \mathbb{Z}$ è il massimo comun divisore dei coefficienti di f .
- (3) $2 \in \mathbb{Z}[x]$ è irriducibile ma non primitivo.
- (4) I polinomi irriducibili di $\mathbb{Z}[X]$ sono (Esercizio):
 - i polinomi costanti p dove p è un numero primo, e
 - i polinomi primitivi di grado $n > 0$ che non sono prodotto di due polinomi di grado $< n$.

10.2 Riduzione modulo p .

Sia p un numero primo e

$$\rho : \mathbb{Z}[x] \rightarrow \mathbb{Z}/p\mathbb{Z}[x], \quad \sum_{i=0}^n a_i x^i \mapsto \sum_{i=0}^n \overline{a_i} x^i.$$

Allora

1. ρ è un epimorfismo con nucleo

$$p\mathbb{Z}[x] = \{f \in \mathbb{Z}[x] \mid \text{tutti i coefficienti di } f \text{ appartengono a } p\mathbb{Z}\}.$$

2. Se $f = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x]$ è un polinomio primitivo di grado $n > 0$ tale che p non divide a_n e $\rho(f)$ è irriducibile in $\mathbb{Z}/p\mathbb{Z}[x]$, allora f è irriducibile in $\mathbb{Z}[x]$.

DIMOSTRAZIONE. Il polinomio $f \in \mathbb{Z}[x] \setminus \{0\}$ non è invertibile. Siano $g, h \in \mathbb{Z}[x]$ tali che $f = gh$. Poiché $\overline{a_n} \neq 0$, il polinomio $\rho(f)$ ha grado n . Inoltre $\rho(f) = \rho(g)\rho(h)$ in $\mathbb{Z}/p\mathbb{Z}[x]$ e per ipotesi uno dei due fattori, ad esempio $\rho(g)$, è costante e l'altro, $\rho(h)$, ha grado n . Ma $\deg h \geq \deg \rho(h)$, quindi anche h ha grado n e g dev'essere costante. Dunque $g \in \mathbb{Z}$ è un comun divisore dei coefficienti di f ed è pertanto invertibile in $\mathbb{Z}$. $\square$

10.3 Criterio di Eisenstein.

Un polinomio primitivo $f = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x]$ di grado $n > 0$ è irriducibile in $\mathbb{Z}[x]$ se esiste un numero primo p tale che:

- (i) p non divide a_n
- (ii) p divide $a_0, a_1, \dots, a_{n-1}$
- (iii) p^2 non divide a_0 .

10.6 Esempi

(1) $f = x^4 + 3x + 9$ è irriducibile in $\mathbb{Z}[x]$ e $\mathbb{Q}[x]$. Riduzione modulo 2:

⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮

(2) $x^5 + 8x^3 + 6x^2 + 10$ è irriducibile in $\mathbb{Z}[x]$ e $\mathbb{Q}[x]$ per il criterio di Eisenstein ($p = 2$).

(3) Siano $n \in \mathbb{N}$, $a \in \mathbb{Z}$, p un numero primo tale che p/a , ma p^2 non divide a . Allora $x^n - a$ è irriducibile in $\mathbb{Z}[x]$ e $\mathbb{Q}[x]$ (per il criterio di Eisenstein).

10.7 Sostituzione

Sia K un campo, $f = \sum_{i=0}^n a_i x^i \in K[x]$. Sostituamo x con $ax + b$ dove $a, b \in K$ e $a \neq 0$. Otteniamo il polinomio $\tilde{f} = \sum_{i=0}^n a_i (ax + b)^i \in K[x]$. Allora f è irriducibile se e solo se $\tilde{f}$ è irriducibile.

DIMOSTRAZIONE :

⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮

10.8 Esempio.

Per ogni primo p il polinomio $f = x^{p-1} + x^{p-2} + \dots + x^2 + x + 1$ è irriducibile in $\mathbb{Z}[x]$.

Infatti

⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮

12.3 Lemma.

Siano K, K' campi con un omomorfismo $\sigma : K \rightarrow K'$ e sia $K \subset F$ un'estensione finita. Allora esistono un'estensione finita $K' \subset F'$ e un omomorfismo $\tau : F \rightarrow F'$ che *estende* σ , cioè che soddisfa $\tau|_K = \sigma$.

DIMOSTRAZIONE : Per 11.9(2) esistono elementi algebrici $\alpha_1, \dots, \alpha_n \in F$ tali che $F = K(\alpha_1, \dots, \alpha_n)$. Procediamo per induzione su n .

$n = 0$: Allora $F = K$ e possiamo scegliere $\tau = \sigma$.

$n > 0$: σ induce un omomorfismo di anelli

$$\tilde{\sigma} : K[x] \rightarrow K'[x], \quad \sum_{i=0}^n a_i x^i \mapsto \sum_{i=0}^n \sigma(a_i) x^i$$

Sia f il polinomio minimo di α_1 su K e sia $f' = \tilde{\sigma}(f) \in K'[x]$. Sappiamo che $(f) = \text{Ker } \varepsilon$ dove $\varepsilon : K[x] \rightarrow K(\alpha_1) \subset F$, $h \mapsto h(\alpha_1)$ per la definizione 11.6. Sia g' un fattore irriducibile di f' , e consideriamo

$$\nu : K'[x] \rightarrow K'[x]/(g') = F_1.$$

Per 11.2 abbiamo un'estensione finita $\nu|_{K'} : K' \subset F_1$. Inoltre poiché $\tilde{\sigma}(f) = f' \in (g')$, abbiamo $\nu\tilde{\sigma}(f) = 0$, e quindi $\text{Ker } \varepsilon = (f) \subset \text{Ker } \nu\tilde{\sigma}$. Per il Teorema 7.8 possiamo fattorizzare $\nu\tilde{\sigma} : K[x] \rightarrow F_1$ attraverso ε , cioè esiste $\tau_1 : K(\alpha_1) \cong K[x]/\text{Ker } \varepsilon \rightarrow F_1$ tale che

$$\tau_1 \varepsilon = \nu\tilde{\sigma}.$$

Quindi $\tau_1 : K(\alpha_1) \rightarrow F_1$ estende $\sigma : K \rightarrow K'$. Per l'ipotesi induttiva esistono inoltre un'estensione finita $F_1 \subset F'$ e un omomorfismo $\tau : F = K(\alpha_1)(\alpha_2, \dots, \alpha_n) \rightarrow F'$ che estende τ_1 , ovvero tale che $\tau|_{K(\alpha_1)} = \tau_1$. Allora anche $\tau|_K = \sigma$. $\square$

12.4 Unicità del campo di riducibilità completa.

Teorema: Siano K, K' campi con un isomorfismo $\sigma : K \rightarrow K'$. Siano inoltre $f = \sum_{i=0}^n a_i x^i \in K[x]$ un polinomio di grado $n > 0$ e $f' = \sum_{i=0}^n \sigma(a_i) x^i \in K'[x]$, e siano F, F' campi di riducibilità completa rispettivamente di f su K e di f' su K' . Allora esiste un isomorfismo $\tau : F \rightarrow F'$ che estende σ e che induce una biiezione fra gli zeri di f in F e gli zeri di f' in F' .

In particolare, il campo di riducibilità completa di un polinomio non costante è unico a meno di isomorfismo.

DIMOSTRAZIONE : Per il Lemma esistono un'estensione finita $F' \subset L$ e un omomorfismo $\tau : F \rightarrow L$ che estende $K \xrightarrow{\sigma} K' \subset F'$, ovvero $\tau|_K$ coincide con $K \xrightarrow{\sigma} K' \subset F' \subset L$. Poiché $\tau \neq 0$, sappiamo per 7.7(3) che τ è iniettivo. Resta da dimostrare $\text{Im } \tau = F'$.

Sappiamo che $f = a(x - \alpha_1) \dots (x - \alpha_n)$ dove $a \in K$ e $\alpha_1, \dots, \alpha_n$ sono gli zeri di f in F . Abbiamo $F = K(\alpha_1, \dots, \alpha_n)$ e $\text{Im } \tau = K'(\tau(\alpha_1), \dots, \tau(\alpha_n))$. Come nel Lemma, σ e τ inducono omomorfismi di anelli

$$\tilde{\sigma} : K[x] \rightarrow K'[x] \quad \text{e} \quad \tilde{\tau} : F[x] \rightarrow L[x].$$

Si noti che $\tilde{\tau}|_{K[x]} = \tilde{\sigma}$.

Allora $f' = \tilde{\sigma}(f) = \tilde{\tau}(f) = \tilde{\tau}(a(x - \alpha_1) \dots (x - \alpha_n))$ e poiché $\tilde{\tau}$ è un omomorfismo, abbiamo $f' = \tau(a)\tilde{\tau}((x - \alpha_1)) \dots \tilde{\tau}((x - \alpha_n)) = \sigma(a)(x - \tau(\alpha_1)) \dots (x - \tau(\alpha_n)) \in L[x]$. Dunque vediamo che gli zeri di f' sono $\tau(\alpha_1), \dots, \tau(\alpha_n) \in \text{Im } \tau$ e perciò $\text{Im } \tau = F'$. Concludiamo che τ è un omomorfismo con le proprietà desiderate. $\square$

12.8 Corollario.

Sia $K \subset F$ un'estensione finita e normale. Se $\alpha, \beta \in F$ possiedono lo stesso polinomio minimo su K , allora esiste un automorfismo $\tau : F \rightarrow F$ tale che $\tau(\alpha) = \beta$ e $\tau|_K = \text{id}_K$.

DIMOSTRAZIONE :

⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮

13 Separabilità

A. LA CARATTERISTICA DI UN CAMPO.

13.1 La caratteristica di un campo.

(1) Dato un campo K , consideriamo l'omomorfismo di anelli

$$\Psi : \mathbb{Z} \rightarrow K, n \mapsto n \cdot 1 = \begin{cases} \underbrace{1_K + 1_K + \dots + 1_K}_n & \text{se } n > 1 \\ 0_K & \text{se } n = 0 \\ \underbrace{-1_K - 1_K - \dots - 1_K}_n & \text{se } n < 0 \end{cases}$$

Se Ψ è iniettivo, allora $\text{Ker}\Psi = 0$ e diremo che il campo K ha *caratteristica* 0.

Se Ψ non è iniettivo, allora $\text{Ker}\Psi = (m)$ per un numero $m \in \mathbb{Z}$.

Verifichiamo che m è un numero primo:

⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮

Dunque $\text{Ker}\Psi = (p)$ per un numero primo p e diremo che K ha *caratteristica* p .

OSSERVAZIONE: In un campo K di caratteristica $p \neq 0$ si ha:

(1) Se $0 \neq x \in K$ e $m \in \mathbb{Z}$, allora $mx = 0_K$ se e solo se $m \in p\mathbb{Z}$.

Infatti

⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮

(2) $(x + y)^p = x^p + y^p$ per tutti gli $x, y \in K$.

Infatti

⋮
⋮
⋮
⋮
⋮

(3) L'applicazione $\varphi : K \rightarrow K, x \mapsto x^p$ è un monomorfismo, detto *omomorfismo di Frobenius*¹³.

Infatti

⋮
⋮
⋮
⋮
⋮

13.2 Esempi

(1) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ hanno caratteristica 0.

(2) Se p è un numero primo, allora $\mathbb{Z}/p\mathbb{Z}$ e il campo delle funzioni razionali $\mathbb{Z}/p\mathbb{Z}(x)$ sono campi di caratteristica p .

(3) Ogni campo finito ha caratteristica $p \neq 0$.

13.3 Teorema

Per un campo K consideriamo il più piccolo sottocampo di K

$$P = \bigcap \{L \mid L \text{ è un sottocampo di } K\},$$

detto *sottocampo fondamentale* di K . Si ha $P = \{(n \cdot 1_K)(m \cdot 1_K)^{-1} \mid n, m \in \mathbb{Z}\}$. Inoltre

$\text{char } K = 0$ se e solo se $P \cong \mathbb{Q}$,

$\text{char } K = p$ se e solo se $P \cong \mathbb{Z}/p\mathbb{Z}$.

DIMOSTRAZIONE :

⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮

13.4 Corollario: la cardinalità di un campo finito.

Se K è un campo finito, allora esistono un numero primo p e un numero $n \in \mathbb{N}$ tali che $|K| = p^n$.

DIMOSTRAZIONE :

⋮
⋮
⋮
⋮

¹³Georg Ferdinand Frobenius, matematico tedesco (1849-1917)

⋮

B. MOLTEPLICITÀ DEGLI ZERI.

13.5 Molteplicità degli zeri.

Siano F un campo, $f \in F[x]$ un polinomio e $\alpha \in F$ uno zero di f . Diremo che α è uno zero di *molteplicità* n se il polinomio f è divisibile per $(x - \alpha)^n$, ma non per $(x - \alpha)^{n+1}$.

13.6 La derivata formale di un polinomio.

Sia K un campo. L'applicazione

$$D : R[x] \rightarrow R[x], f = \sum_{i=0}^n a_i x^i \mapsto Df = \sum_{i=1}^n i \cdot a_i x^{i-1},$$

detta *derivata formale*, è una derivazione dell'anello $R[x]$, cioè soddisfa per $f, g \in R[x]$:

1. $D(f + g) = Df + Dg$
2. $D(fg) = D(f)g + fD(g)$

13.7 Proposizione.

Siano F un campo, $f \in F[x]$ un polinomio e $\alpha \in F$. Allora α è uno zero di f di molteplicità > 1 se e solo se è uno zero comune a f e $D(f)$.

DIMOSTRAZIONE: $\Rightarrow$: Supponiamo che $f = (x - \alpha)^2 g$. Allora $D(f) = 2(x - \alpha)g + (x - \alpha)^2 D(g)$ è divisibile per $(x - \alpha)$ e quindi α è uno zero comune a f e $D(f)$.

$\Leftarrow$: Poiché α è zero di f , abbiamo $f = (x - \alpha)g$ con $g \in K[x]$. Poiché α è zero di $D(f)$, sappiamo che $(x - \alpha)$ divide anche $D(f) = g + (x - \alpha)D(g)$ e quindi anche g . Ma allora f è divisibile per $(x - \alpha)^2$. $\square$

13.8 Teorema.

Siano K un campo e $f \in K[x]$ un polinomio di grado $n > 0$. Sono equivalenti i seguenti enunciati.

- (1) Non esiste estensione $K \subset F$ in cui f abbia zero di molteplicità > 1 .
- (2) Esiste un'estensione $K \subset F$ nella quale

$$f = a(x - \alpha_1) \dots (x - \alpha_n)$$

con $a \in K$ ed elementi distinti $\alpha_1, \dots, \alpha_n \in F$.

- (3) f e $D(f)$ sono polinomi coprimi in $K[x]$.

Se f è irriducibile, (1) - (3) sono inoltre equivalenti a

- (4) $D(f) \neq 0$.

vede con un argomento analogo a 10.6(3) e 10.5 che f è irriducibile su $\mathbb{Z}/p\mathbb{Z}[x]$ e quindi anche sul campo delle frazioni K . Poiché $D(f) = py^{p-1} = 0$, concludiamo che f non è separabile. Pertanto il campo di riducibilità completa F di f su K è un'estensione finita e normale che non è separabile.

.....

DIMOSTRAZIONE

Se $F = \mathbb{F}_{p^n}$, segue dal Lemma che $F \setminus \{0\} = \langle \alpha \rangle = \{1, \alpha, \alpha^2, \dots, \alpha^{p^n-2}\}$ per un $\alpha \in F$.

Passiamo quindi il caso in cui K è un campo infinito. Sappiamo che $F = K(\alpha_1, \dots, \alpha_n)$ con elementi separabili $\alpha_1, \dots, \alpha_n \in F$. Per ogni $i = 1, \dots, n$ consideriamo il polinomio minimo f_i di α_i su K e denotiamo con F' il campo di riducibilità completa di $f = f_1 \cdots f_n$ su F . In $F'[x]$ abbiamo quindi $f = (x - a_1) \cdots (x - a_m)$ con $\alpha_1, \dots, \alpha_n \in \{a_1, \dots, a_m\}$.

Si noti che F' è anche campo di riducibilità completa di f su K poiché $F' = F(a_1, \dots, a_m) = K(a_1, \dots, a_m)$, ed essendo f separabile su K , segue che $K \subset F'$ è un'estensione di Galois. Deduciamo che esiste solo un numero finito di campi intermedi di $K \subset F'$. Infatti questi sono anche campi intermedi di $K \subset F'$ e corrispondono pertanto a sottogruppi del gruppo finito $G = \text{Gal}(F'/K)$.

Supponiamo che $n = 2$, ovvero $F = K(\alpha_1, \alpha_2)$. In particolare esiste solo un numero finito di campi intermedi di forma

$$K \subset K(\alpha_1 + k\alpha_2) \subset F$$

con $k \in K \setminus \{0\}$, e poiché K è infinito, ciò implica l'esistenza di $k, \ell \in K \setminus \{0\}$ tali che

$$K(\alpha_1 + k\alpha_2) = K(\alpha_1 + \ell\alpha_2).$$

Dunque

$$\alpha_1 + \ell\alpha_2 \in K(\alpha_1 + k\alpha_2),$$

perciò

$$\alpha_2 = (k - \ell)^{-1}((\alpha_1 + k\alpha_2) - (\alpha_1 + \ell\alpha_2)) \in K(\alpha_1 + k\alpha_2)$$

e anche

$$\alpha_1 = (\alpha_1 + k\alpha_2) - k\alpha_2 \in K(\alpha_1 + k\alpha_2).$$

Ma allora $\alpha = \alpha_1 + k\alpha_2$ è un elemento primitivo con

$$F = K(\alpha_1, \alpha_2) = K(\alpha).$$

Per $n > 2$ proseguiamo induttivamente: se β è un elemento primitivo di $K(\alpha_1, \dots, \alpha_{n-1})$, procediamo come sopra per trovare un elemento primitivo di $F = K(\beta, \alpha_n)$. $\square$

17.6 Osservazioni

(1) Nella definizione 17.5 possiamo assumere senza perdita di generalità che $K \subset F$ sia anche un'estensione di Galois.

Infatti, data un'estensione $K \subset F$ come nella Definizione, esiste sempre un'estensione $K \subset F \subset F'$ tale che $K \subset F'$ è un'estensione per radicali e un'estensione di Galois.

Lo dimostriamo per induzione sul grado $[F : K]$. L'enunciato è chiaro per $[F : K] = 1$. Supponiamo $[F : K] > 1$ con una catena di campi intermedi come nella Definizione

$$K = L_0 \subset L_1 \subset L_2 \subset \dots \subset L_{n-1} = L \subset L_n = F.$$

In particolare $F = L(\alpha)$ dove α è una radice m -sima di un elemento di L .

Poiché $[L : K] < [F : K]$, per ipotesi induttiva esiste un'estensione $K \subset L \subset L'$ tale che $K \subset L'$ è un'estensione per radicali e un'estensione di Galois.

Consideriamo adesso il gruppo di Galois $G' = \text{Gal}(L'/K)$. L'elemento $\alpha^m \in L \subset L'$ dà luogo a un insieme $\{\sigma(\alpha^m) \mid \sigma \in G'\} \subset L'$. Si verifica facilmente che il polinomio

$$g = \prod_{\sigma \in G'} (x^m - \sigma(\alpha^m)) \in L'[x]$$

giace in $K[x]$ poiché i suoi coefficienti vengono fissati dagli automorfismi di G' e pertanto appartengono a $\text{Fix}_{L'}(G') = K$.

Il campo di riducibilità completa $L' \subset F'$ di g su L' è un'estensione per radicali, poiché $F' = L'(\beta_1, \dots, \beta_s)$ si ottiene da L' aggiungendo gli zeri $\beta_1, \dots, \beta_s$ di g , i quali sono radici m -sime di elementi di L' : infatti sono elementi $\beta \in F'$ tali che $\beta^m = \sigma(\alpha^m) \in L'$ per un opportuno $\sigma \in G'$.

Dunque $K \subset L' \subset F'$ è un'estensione per radicali. Inoltre $F = L(\alpha) \subset F'$ poiché $\alpha \in \{\beta_1, \dots, \beta_s\}$ è uno zero di g . Resta da verificare che $K \subset F'$ è un'estensione di Galois. L'estensione di Galois $K \subset L'$ è campo di riducibilità completa di un polinomio f su K , ovvero $L' = K(\alpha_1, \dots, \alpha_r)$ dove $\alpha_1, \dots, \alpha_r \in L$ sono zeri di f . Ma allora $F' = K(\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_s)$ è campo di riducibilità completa del polinomio fg (separabile poiché siamo in caratteristica zero). $\square$

(2) Un'estensione per radicali $K = L_0 \subset L_1 \subset L_2 \subset \dots \subset L_n = F$ che sia anche un'estensione di Galois dà luogo a estensioni di Galois $L_i \subset F$ i cui gruppi di Galois

$$H_i = \text{Gal}(F/L_i)$$

formano una catena finita di sottogruppi

$$\{id\} = H_n \leq H_{n-1} \leq \dots \leq H_2 \leq H_1 \leq G = \text{Gal}(F/K)$$

17.7 Equazioni risolubili per radicali

Dato un polinomio non costante $f \in K[x]$ su un campo K , diremo che l'equazione $f(x) = 0$ è *risolubile per radicali* su K se esiste un'estensione per radicali $K \subset F$ tale che f è prodotto di fattori lineari in $F[x]$. Inoltre chiamiamo *gruppo di Galois di f su K* il gruppo $\text{Gal}(f/K) = \text{Gal}(F/K)$ dove F è un campo di riducibilità completa di f su K .

17.8 Teorema (Galois)

Per un polinomio non costante $f \in K[x]$ su un campo K sono equivalenti i seguenti enunciati.

1. L'equazione $f(x) = 0$ è risolubile per radicali su K .
2. $\text{Gal}(f/K)$ è un gruppo risolubile.

DIMOSTRAZIONE

(1) $\Rightarrow$ (2) : Per 17.6 possiamo supporre che esista un'estensione di Galois $K \subset F$ tale che

- (i) f è prodotto di fattori lineari in $F[x]$ e
- (ii) si ha una catena di campi intermedi

$$K = L_0 \subset L_1 \subset L_2 \subset \dots \subset L_m = F$$

di forma

$$L_i = L_{i-1}(\alpha_i)$$

dove α_i è una radice n_i -sima di un elemento di L_{i-1} .

Useremo ripetutamente 5.4: se G è un gruppo risolubile, allora sono risolubili anche ogni sottogruppo $H \leq G$ e ogni gruppo quoziente G/N (dove N è un sottogruppo normale). Inoltre G è risolubile se (e solo se) esiste un sottogruppo normale N tale che N e G/N sono risolubili.

Per (i) sappiamo che F contiene un campo di riducibilità completa L di f su K . Poiché K è un campo perfetto ($\text{char} K = 0$), il polinomio f è separabile e quindi $K \subset L$ è un'estensione di Galois. Abbiamo dunque un campo intermedio $K \subset L \subset F$ con

$$\text{Gal}(f/K) = \text{Gal}(L/K) = \text{Gal}(F/K)/\text{Gal}(F/L)$$

per il Teorema Fondamentale 15.3, e quindi basta verificare che $\text{Gal}(F/K)$ è risolubile, vedi 5.4.

Procediamo per induzione su m .

$m = 0$: in questo caso $F = K$, quindi $\text{Gal}(F/K) = \{\text{id}\}$ è risolubile.

$m \rightarrow m+1$: consideriamo l'estensione $K = L_0 \subset L_1 = K(\alpha_1)$ ponendo $n = n_1$, quindi α_1 è una radice n -sima di un elemento di K . Per ricondurre la situazione al caso considerato in 17.2 aggiungiamo a K le radici n -sime dell'unità. Poniamo quindi $K' = K_n = K(z)$ dove z è una radice primitiva dell'unità, e sostituiamo l'estensione $K \subset F$ con l'estensione $K' = K_n \subset F' = F(z)$.

(a) Vediamo che $K \subset F$, $K \subset K'$, $F \subset F'$ e $K' \subset F'$ sono tutte estensioni di Galois. Infatti l'estensione $K \subset K'$ è di Galois e $\text{Gal}(K'/K)$ è abeliano per 17.3, e analogamente per $F \subset F'$. Per $K' \subset F'$ usiamo che F è campo di riducibilità completa di un polinomio su K e quindi F' può essere visto come campo di riducibilità completa dello stesso polinomio su K' .

(b) Considerando il campo intermedio $K \subset F \subset F'$, deduciamo da (a) con 15.3 che

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

quindi sempre per 5.4 basta dimostrare che

$$G = \text{Gal}(F'/K)$$

è risolubile.

(c) Dalla catena di campi intermedi

$$K = L_0 \subset L_1 = K(\alpha_1) \subset L_2 = K(\alpha_1, \alpha_2) \subset \dots \subset L_m = K(\alpha_1, \dots, \alpha_m) = F$$

si ottiene una catena di campi intermedi

$$K \subset K' = K_n \subset K_n(\alpha_1) \subset K_n(\alpha_1, \alpha_2) \subset \dots \subset K_n(\alpha_1, \dots, \alpha_m) = F'$$

e ponendo $L = K_n(\alpha_1)$ sappiamo per l'ipotesi induttiva che

$$H = \text{Gal}(F'/L)$$

è un gruppo risolubile. Abbiamo quindi i campi intermedi

$$K \subset K' \subset L \subset F'$$

per i quali sappiamo:

- $K' = K_n \subset L = K_n(\alpha_1)$ è un'estensione di Galois con gruppo di Galois $\text{Gal}(L/K')$ ciclico (vedi 17.2),
 - $K \subset K' = K_n$ è un'estensione di Galois con gruppo di Galois $\text{Gal}(K'/K)$ abeliano (vedi 17.3).
- (d) Applicando il Teorema Fondamentale 15.3 a

$$K' \subset L \subset F'$$

si ottiene che

$$G' = \text{Gal}(F'/K')$$

ha un quoziente $G'/H \cong \text{Gal}(L/K')$ ciclico e pertanto risolubile. Poiché anche H è risolubile, deduciamo da 5.4 che G' è risolubile. Applicando il Teorema Fondamentale 15.3 a

$$K \subset K' \subset F'$$

vediamo che $G/G' \cong \text{Gal}(K'/K)$ è abeliano e pertanto risolubile, e per 5.4 concludiamo che G è risolubile.

(2) $\Rightarrow$ (1): Sia L un campo di riducibilità completa di f su K . Poiché K è un campo perfetto ($\text{char} K = 0$), il polinomio f è separabile e quindi $K \subset L$ è un'estensione di Galois. Per ipotesi $G = \text{Gal}(L/K)$ è risolubile.

(a) Si dimostra che la catena di sottogruppi normali di G con quozienti abeliani

$$\{e\} = N_m \leq N_{m-1} \leq \dots \leq N_1 \leq G$$

può essere scelta tale che ogni quoziente N_{i-1}/N_i sia addirittura ciclico di ordine primo p_i .

(b) Ponendo $L_i = \text{Fix}_L(N_i)$ si ottiene una catena di campi intermedi

$$K = K_0 \subset L_1 \subset \dots \subset L_{m-1} \subset L_m = L$$

dove ogni $L_i \subset L$ è un'estensione di Galois con gruppo di Galois N_i . Inoltre il fatto che N_i sia un sottogruppo normale di N_{i-1} implica per il Teorema Fondamentale 15.3 che anche ogni $L_{i-1} \subset L_i$ è un'estensione di Galois il cui gruppo di Galois $\text{Gal}(L_i/L_{i-1}) \cong N_{i-1}/N_i$ è ciclico di ordine primo p_i .

(c) Si dimostra che ogni estensione di Galois $L'' \subset L'$ il cui gruppo di Galois $\text{Gal}(L''/L')$ è ciclico di ordine primo p dev'essere di forma $L' = L''(\alpha)$ dove α è una radice p -sima di un elemento di L'' .

Ma allora abbiamo verificato che l'equazione $f(x) = 0$ è risolubile per radicali. $\square$

18 Risolubilità del polinomio generale di grado n

Sia K un campo di *caratteristica* 0.

18.4 Funzioni razionali simmetriche

(1) Per $n \in \mathbb{N}$ definiamo ricorsivamente

$$K[x_1, x_2] = K[x_1][x_2]$$

$$\vdots$$

$$K[x_1, \dots, x_n] = K[x_1, \dots, x_{n-1}][x_n]$$

l'anello dei polinomi $K[x_1, \dots, x_n]$ su K nelle variabili $x_1, \dots, x_n$. I suoi elementi sono espressioni di forma

$$p = \sum_{(i_1, \dots, i_n) \in I} a_{(i_1, \dots, i_n)} x_1^{i_1} \dots x_n^{i_n}$$

dove $I \subset \mathbb{N}_0^n$ è un sottoinsieme finito e $a_{(i_1, \dots, i_n)} \in K \setminus \{0\}$.

(2) Il campo dei quozienti $F = Q(R) = K(x_1, \dots, x_n)$ di $R = K[x_1, \dots, x_n]$ è detto campo delle *funzioni razionali* su K nelle variabili $x_1, \dots, x_n$.

(3) Ogni permutazione $\sigma \in S_n$ definisce un automorfismo $\hat{\sigma}$ di F :

$$\hat{\sigma} : F \rightarrow F, \quad \frac{p}{q} = \frac{p(x_1, \dots, x_n)}{q(x_1, \dots, x_n)} \mapsto \frac{p(x_{\sigma(1)}, \dots, x_{\sigma(n)})}{q(x_{\sigma(1)}, \dots, x_{\sigma(n)})}$$

Possiamo quindi interpretare S_n come sottogruppo di $\text{Aut} F$ e considerare $L = \text{Fix}_F(S_n)$. Gli elementi di L sono detti *funzioni razionali simmetriche* nelle variabili $x_1, \dots, x_n$.

18.5 Esempio

Sia $n = 2$, quindi $R = K[x, y]$, $F = K(x, y)$, e $S_2 = \{\text{id}, (12)\}$.

Per $\sigma = (12) \in S_2$ si ha $\hat{\sigma}(\frac{x+2y}{x+y}) = \frac{y+2x}{x+y}$, quindi $\frac{x+2y}{x+y} \notin \text{Fix}_F(S_2)$, mentre $\hat{\sigma}(\frac{xy}{x+y}) = \frac{xy}{x+y}$, quindi $\frac{xy}{x+y} \in \text{Fix}_F(S_2)$.

18.6 Funzioni simmetriche elementari

I seguenti polinomi in R

$$s_0 = 1$$

$$s_1 = x_1 + \dots + x_n$$

$$s_2 = x_1 x_2 + x_1 x_3 + \dots + x_{n-1} x_n = \sum_{i < j} x_i x_j$$

$$s_3 = \sum_{i < j < k} x_i x_j x_k$$

$$\vdots$$

$$s_n = x_1 \dots x_n$$

sono funzioni razionali simmetriche dette *funzioni simmetriche elementari* nelle variabili $x_1, \dots, x_n$.

Consideriamo il polinomio

Consideriamo il polinomio

$$f = (x - x_1)(x - x_2) \dots (x - x_n) \in F[x].$$

Allora

1. **(Newton)** $f = x^n - s_1 x^{n-1} + s_2 x^{n-2} + \dots + (-1)^n s_n = \sum_{k=0}^n (-1)^k s_k x^{n-k} \in L[x]$
2. $L = K(s_1, \dots, s_n)$.
3. $\text{Gal}(f/L) \cong S_n$.

(ovvero: un polinomio f può essere visto come polinomio nelle funzioni simmetriche sugli zeri di f , e come tale il suo gruppo di Galois è S_n).

DIMOSTRAZIONE

(1) si dimostra per induzione.

(2) (3) Poiché $s_1, \dots, s_n \in L$, si ha $K(s_1, \dots, s_n) \subset L \subset F$, dove $L \subset F$ è un'estensione di Galois con $\text{Gal}(F/L) = S_n$, e quindi $[F : L] = n!$. D'altra parte possiamo considerare F come campo di riducibilità completa di f su $K(s_1, \dots, s_n)$, da cui segue $[F : K(s_1, \dots, s_n)] \leq n!$ e per il Lemma del Grado concludiamo $L = K(s_1, \dots, s_n)$ e $\text{Gal}(f/L) = \text{Gal}(F/L) = S_n$. $\square$

18.8 Teorema (Abel - Ruffini)

L'equazione

$$p(x) = 0$$

per il polinomio generale di grado $n \geq 5$ non è risolubile per radicali.

Più precisamente: Se K è un campo di caratteristica 0 e

$$p = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots + a_{n-1} x + a_n \in K[x],$$

allora nell'anello $K(a_1, \dots, a_n)[x]$ si ha

1. il gruppo di Galois di p su $K(a_1, \dots, a_n)$ è S_n ,
2. l'equazione $p(x) = 0$ non è risolubile per radicali su $K(a_1, \dots, a_n)$.

DIMOSTRAZIONE

[illegible]

18.9 Ancora sul caso $n \leq 4$.

Sia $f \in K[x]$ un polinomio monico non costante di grado $n \leq 4$. Siano inoltre E il campo di riducibilità completa di f su K e $G = \text{Gal}(f/K) = \text{Gal}(E/K)$ il gruppo di Galois di f su K .

In $E[x]$ abbiamo $f = (x - \alpha_1) \cdots (x - \alpha_n)$, e gli elementi di G corrispondono a permutazioni di $\alpha_1, \dots, \alpha_n$. Identifichiamo quindi G con un sottogruppo di S_n , vedi 18.1.

Poniamo

$$\delta = \prod_{i < j} (\alpha_i - \alpha_j) \in E$$

e chiamiamo *discriminante* di f l'elemento

$$\Delta = \delta^2 = \prod_{i < j} (\alpha_i - \alpha_j)^2 \in \text{Fix}_E(G) = K.$$

Si noti che $\sigma(\delta) = \delta$ se e solo se σ è una permutazione pari, quindi $\delta \in K$ se e solo se $G \subset A_n$.

Caso n=2: $f = x^2 + px + q$

Abbiamo

$$\tilde{s}_1 = \alpha_1 + \alpha_2 = -p$$

$$\tilde{s}_2 = \alpha_1 \alpha_2 = q$$

Inoltre $\delta = \alpha_1 - \alpha_2$, $\Delta = p^2 - 4q$ e gli zeri di f sono $\{\alpha_1, \alpha_2\} = \left\{ \frac{-p+\delta}{2}, \frac{-p-\delta}{2} \right\}$.

Se $\delta \in K$, allora $G = \{id\} = A_2$.

Se $\delta \notin K$, allora $G = S_2 \cong \mathbb{Z}/2\mathbb{Z}$.

Caso n=3: (1) Basta considerare il caso $f = x^3 + px + q$.

Infatti se $f = x^3 + a_2x^2 + a_1x + a_0$, sostituendo x con $x - \frac{1}{3}a_1$, si ottiene un polinomio della forma $f' = x^3 + px + q$ tale che z è zero di f' se e solo se $z - \frac{1}{3}a_1$ è zero di f , e f, f' hanno lo stesso discriminante e lo stesso gruppo di Galois.

$$(2) \Delta = -4p^3 - 27q^2$$

$$\text{Infatti } \delta = -\det \begin{pmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{pmatrix}, \text{ quindi } \Delta = \det \begin{pmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{pmatrix}^T.$$

Notiamo che

$$\tilde{s}_1 = \alpha_1 + \alpha_2 + \alpha_3 = 0$$

$$\tilde{s}_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = p$$

$$\tilde{s}_3 = \alpha_1\alpha_2\alpha_3 = -q$$

quindi

$$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = \tilde{s}_1^2 - 2\tilde{s}_2 = -2p$$

$$\alpha_1^3 + \alpha_2^3 + \alpha_3^3 = -3q$$

$$\alpha_1^4 + \alpha_2^4 + \alpha_3^4 = 2p^2$$

(per le ultime due uguaglianze si usi che $\alpha_i^3 + p\alpha_i + q = 0$ per ogni $i = 1, 2, 3$).

$$\text{Dunque } \Delta = \det \begin{pmatrix} 3 & 0 & -2p \\ 0 & -2p & -3q \\ -2p & -3q & 2p^2 \end{pmatrix} = -4p^3 - 27q^2.$$

(3) Abbiamo uno dei casi seguenti:

1. f è prodotto di fattori lineari in $K[x]$ e $G = \{id\}$.

2. $f = (x - a)g$ dove $a \in K$ e $g \in K[x]$ è irriducibile.

In tal caso g ha due zeri distinti e $G = \text{Gal}(g/K) \cong \mathbb{Z}/2\mathbb{Z}$.

3. f è irriducibile su K .

In tal caso si ha:

Se $\delta \in K$, allora $G = A_3 \cong \mathbb{Z}/3\mathbb{Z}$.

Se $\delta \notin K$, allora $G = S_3$.

⋮
⋮
⋮
⋮

(4) *Formule di Cardano-Tartaglia-Del Ferro* (vedi Esercizio)¹⁷:

Data una radice primitiva terza dell'unità $z \in E_3(K)$ e dati

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}}, \quad v = \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}}$$

con la proprietà

$$3uv = -p,$$

si ha

$$\{\alpha_1, \alpha_2, \alpha_3\} = \{u + v, z^2u + zv, zu + z^2v\}.$$

Si noti che $u = \sqrt[3]{a}$, $v = \sqrt[3]{b}$ dove $a, b \in K(\delta)$ sono le soluzioni dell'equazione quadratica

$$x^2 + qx - \left(\frac{p}{3}\right)^3 = 0.$$

(5) Sia adesso $f \in \mathbb{R}[x]$. Allora f ha tre zeri distinti in $\mathbb{R}$ se $\Delta > 0$, al più due zeri distinti in $\mathbb{R}$ se $\Delta = 0$, uno zero in $\mathbb{R}$ e due zeri coniugati in $\mathbb{C} \setminus \mathbb{R}$ se $\Delta < 0$ (Esercizio).

Caso n=4: (1) Basta considerare il caso $f = x^4 + px^2 + qx + r$.

Infatti se $f = x^3 + a_2x^2 + a_1x + a_0$, sostituendo x con $x - \frac{1}{4}a_3 \dots$

⋮
⋮
⋮
⋮
⋮
⋮

(2) *Formule di Ferrari*:

Date le soluzioni z_1, z_2, z_3 dell'equazione cubica

$$x^3 - 2px^2 + (p^2 - 4r)x + q^2 = 0$$

e dati

$$u_1 = \sqrt{-z_1}, \quad u_2 = \sqrt{-z_2}, \quad u_3 = \sqrt{-z_3},$$

con la proprietà

$$u_1u_2u_3 = -q$$

si ha

$$\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} = \left\{ \frac{1}{2}(u_1 + u_2 + u_3), \frac{1}{2}(u_1 - u_2 - u_3), \frac{1}{2}(-u_1 + u_2 - u_3), \frac{1}{2}(-u_1 - u_2 + u_3) \right\}.$$

¹⁷Girolamo Cardano (1501-1576), Niccolò Tartaglia (1499?-1557), Scipione Del Ferro (1465-1526), matematici italiani

19 Costruzioni con riga e compasso

19.1 Costruzioni elementari.

Sia $M \subset \mathbb{C}$. Denotiamo con $E(M)$ l'insieme di tutti i punti $a \in \mathbb{C}$ che si ottengono da M mediante una delle seguenti *costruzioni elementari*:

1. *intersecare due rette*: se R_1, R_2 sono due rette non parallele passanti rispettivamente per i punti $p_1, q_1 \in M$ e per $p_2, q_2 \in M$,

⋮

allora il punto di intersezione a di R_1 e R_2 appartiene a $E(M)$;

2. *intersecare una retta con una circonferenza*: se C è la circonferenza di centro $c \in M$ passante per il punto $d \in M$ e R è la retta passante per i punti $p, q \in M$,

⋮

allora i punti di intersezione a di C e R appartengono a $E(M)$;

3. *intersecare due circonferenze*: se C_1, C_2 sono due circonferenze, dove C_i ha centro $c_i \in M$ e passa per il punto $d_i \in M$, $i = 1, 2$,

⋮

allora i punti di intersezione di C_1 e C_2 appartengono a $E(M)$.

Diremo che il punto $a \in \mathbb{C}$ *si costruisce con riga e compasso da M* se a è ottenuto da M mediante un numero finito di costruzioni elementari, ovvero esistono $a_1, \dots, a_n \in \mathbb{C}$ tali che $a_1 \in E(M)$, $a_2 \in E(M \cup \{a_1\})$, $\dots$, $a_n \in E(M \cup \{a_1, \dots, a_{n-1}\})$ e $a = a_n$.

Infine diciamo che il punto $a \in \mathbb{C}$ è *costruibile* se si costruisce con riga e compasso dall'insieme $M = \{0, 1\}$.

19.2 Esempi

- (1) Gli interi di Gauss, ovvero gli elementi di $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, sono costruibili.

⋮

- (2) Siano $M \subset \mathbb{C}$, $p, q, c \in M$ e R la retta passante per p, q . Allora si costruiscono con riga e compasso la retta normale a R passante per c e la retta parallela a R passante per c .

⋮

⋮

Inoltre si costruiscono con riga e compasso la bisettrice di un angolo, la somma di due angoli, il punto medio di un segmento.

19.3 Il campo intermedio dei numeri costruibili.

1. I numeri complessi costruibili formano un campo intermedio $\mathbb{Q} \subset \mathbb{K} \subset \mathbb{C}$.
2. Se $c \in \mathbb{C}$ è un numero complesso tale che $c^2 \in \mathbb{K}$, allora anche $c \in \mathbb{K}$.

DIMOSTRAZIONE

⋮

19.4 Lemma

Sia $L \subset \mathbb{C}$ un sottocampo tale che $i \in L$ e $\overline{L} = \{\bar{a} \mid a \in L\} = L$, e sia $M \subset L$.

Per ogni $a \in E(M)$ esiste $b \in \mathbb{C}$ tale che $b^2 \in L$ e $a \in L(b)$.

(ovvero: i punti di $E(M)$ si ottengono aggiungendo radici quadrate)

DIMOSTRAZIONE

⋮

Infatti per tale $a \in \mathbb{K}$ si avrebbe $\pi = a^2 \in \mathbb{K}$, contraddicendo il Teorema di Lindemann secondo il quale π è trascendente su $\mathbb{Q}$, vedi 11.10 e 19.5.

(2) La duplicazione del cubo è impossibile: non esiste un cubo il cui lato $a \in \mathbb{K}$ sia costruibile e il cui volume sia il doppio del volume del cubo di lato 1.

Infatti per tale $a \in \mathbb{K}$ si avrebbe $a^3 = 2$, quindi $f = x^3 - 2$ sarebbe il polinomio minimo di a su $\mathbb{Q}$, e $[\mathbb{Q}(a) : \mathbb{Q}] = 3$ non sarebbe una potenza di 2, contraddicendo 19.5.

(3) La trisezione dell'angolo è impossibile, ad esempio per l'angolo $\alpha = 60^\circ = \frac{\pi}{3}$.

Infatti, se fosse costruibile $\frac{\alpha}{3} = \frac{\pi}{9}$, allora lo sarebbe anche $2\frac{\alpha}{3}$, ovvero la radice nona primitiva dell'unità $z = \cos \frac{2\pi}{9} + i \sin \frac{2\pi}{9} \in \mathbb{K}$. Ma il polinomio minimo di z su $\mathbb{Q}$ è $\Phi_9 = x^6 + x^3 + 1$, perché

⋮
⋮
⋮

Quindi $[\mathbb{Q}(z) : \mathbb{Q}] = \deg \Phi_9 = 6$ non sarebbe una potenza di 2, contraddicendo 19.5.

19.7 Costruzione del poligono regolare.

Per un numero naturale $n \in \mathbb{N}, n > 1$, denotiamo con

$$\varphi(n) = |\{a \mid 1 \leq a < n, \text{MCD}(a, n) = 1\}|$$

la *funzione di Eulero*. Sappiamo che $\varphi(n)$ coincide con l'ordine del gruppo $(\mathbb{Z}/n\mathbb{Z}^*, \cdot)$ degli elementi invertibili nell'anello $\mathbb{Z}/n\mathbb{Z}$, vedi 7.4.

Teorema (Gauss). Il poligono regolare di $n \geq 3$ lati è costruibile se e solo se $\varphi(n)$ è una potenza di 2.

Dimostrazione (schizzo): Il poligono regolare di n lati è costruibile se e solo se è costruibile la radice primitiva n -sima dell'unità

$$z = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n} \in \mathbb{K}.$$

Poiché il campo di riducibilità completa $\mathbb{Q}_n$ di $x^n - 1$ coincide con $\mathbb{Q}(z)$, abbiamo

$$[\mathbb{Q}(z) : \mathbb{Q}] = [\mathbb{Q}_n : \mathbb{Q}] = |\text{Gal}(\mathbb{Q}_n/\mathbb{Q})|.$$

Inoltre si dimostra che nel Lemma 17.3(2) con $K = \mathbb{Q}$ si ha addirittura $\text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong \mathbb{Z}/n\mathbb{Z}^*$.

Quindi $[\mathbb{Q}(z) : \mathbb{Q}] = \varphi(n)$ e pertanto il Teorema è un'applicazione di 19.5. □

20 Bibliografia

Classici:

- Emil Artin, *Galois Theory*, Dover Publications, 1998. ISBN 0-486-62342-4
- N. Bourbaki: *Algèbre* 4,5, Hermann (1964 usw.), Masson (1980 usw.)
- N. Jacobson: *Basic algebra* 1, Dover Publications Ed. 2, 2009 ISBN: 9780486471891
- Bartel Van Der Waerden, *Algebra: Volume I*, Springer 2003. ISBN: 9780387406244

in italiano:

- S. BOSCH, *Algebra*, Springer, Unitext 2003. ISBN: 978-88-470-0221-0
- I.N.HERSTEIN, *Algebra*, Editori Riuniti 2003.

di storia dell'algebra / divulgazione:

- John Derbyshire, *Unknown quantity. A real and imaginary history of algebra*. Plume 2006.
- Mario Livio, *L'equazione impossibile*, Rizzoli 2005