ALGEBRA[1]

Università degli Studi di Verona

– Corso di Laurea in Matematica Applicata –

∗ ∗ ∗

Prof. Lidia Angeleri

Anno accademico 2009-2010

[1]si veda la nota a pagina seguente!

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.

Indice

Parte I

RICHIAMI DI TEORIA DEI GRUPPI

1 Gruppi e sottogruppi

1.1 Gruppo

Un *gruppo* $(G, +)$ è costituito da un insieme non vuoto G e un'operazione $+ : G \times G \to G$, $(a, b) \mapsto ab$ 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* se vale anche la proprietá:
(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 1_G e l'elemento inverso di a si indica con a^{-1}.

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 Laterale di G modulo H.

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 $\sim$ è

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

Infatti:
$\vdots$
$\vdots$
$[a]$ si chiama *laterale destro* di G modulo H con rappresentante a.

1.4 Esempio: il gruppo abeliano $(\mathbb{Z}, +)$

$(\mathbb{Z}, +)$ è un gruppo abeliano.
(1) I suoi sottogruppi sono i sottoinsiemi di forma $n\mathbb{Z}$ con $n \in \mathbb{N}_0$.
Infatti:
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$

(2) I laterali (destri e sinistri) di $\mathbb{Z}$ modulo $n\mathbb{Z}$ sono esattamente le classi di resto $[0], [1], [2], ..., [n-1]$ di $\mathbb{Z}$ modulo n.
Infatti:
$\vdots$
$\vdots$
$\vdots$
$\vdots$

1.5 Teorema di Lagrange

Sia $(G, +)$ un gruppo finito e sia $H \leq G$. Allora l'ordine $\mid H \mid$ divide l'ordine $\mid G \mid$.
Più precisamente si ha

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

dove $[G : H]$ è *l'indice* di H in G, ovvero il numero dei laterali destri di G modulo H.

2 Gruppi ciclici

2.1 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

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

Definiamo $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$. L'insieme $\langle a \rangle$ è un sottogruppo di G. Il suo ordine si indica con $ord(a) =\mid \langle a \rangle \mid$ e si chiama *ordine dell'elemento* a.

2.2 Teorema sull'ordine di un elemento

Sia $(G, \cdot)$ un gruppo e sia $a \in G$.
(1) Se $a^l \neq a^k$ per $l \neq k$ allora $ord(a) = \infty$.
(2) Se esistono $l \neq k$ tali che $a^l = a^k$ allora $ord(a) = m < \infty$, dove m è il minimo intero positivo tale che $a^m = e$.
COROLLARIO

Se $\mid G \mid = n$, allora $ord(a)$ divide n e quindi $a^n = e$.

DIMOSTRAZIONE :

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

2.3 Gruppo ciclico

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

2.4 Omomorfismo, isomorfismo

Siano $(G, \cdot)$ e $(G', *)$ due gruppi. Un'applicazione $f : G \to G'$ si dice:
- *omomorfismo* se $f(a \cdot b) = f(a) * f(b)$ per $a, b \in G$;
- *isomorfismo* se f è un omomorfismo biiettivo.

Se esiste un isomorfismo $f : G \to G'$ si dice che G e G' sono *isomorfi* e si scrive $G \cong G'$.

2.5 Classificazione dei gruppi ciclici

Sia $(G, \cdot)$ un gruppo ciclico.
(1) Se $\mid G \mid = \infty$, allora $(G, \cdot) \cong (\mathbb{Z}, +)$.
(2) Se $\mid G \mid = m$ allora $(G, \cdot) \cong (\mathbb{Z}/m\mathbb{Z}, +)$.

DIMOSTRAZIONE :

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

Parte II

<u>ANELLI</u>

3 Il concetto di anello

3.1 Definizione

Un anello $(R,+,\cdot)$ è costituito da un insieme non vuoto R e due operazioni $+,\cdot : R\times R \to R$ 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.
<u>*OSSERVAZIONI :*</u>

(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: $R\neq\{0_R\}$.

3.2 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\{0}, ·) 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 $x\cdot y = 0$.

3.3 Sottoanello e sottocampo

Sia $(R,+,\cdot)$ un anello (un campo). Un sottoinsieme non vuoto $S\subset R$ si dice *sottoanello (sottocampo)* se S è un anello (un campo) rispetto alle operazioni $+$ e $\cdot$ definite in R.
<u>OSSERVAZIONE:</u>

(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$\setminus\{0\}$, $\cdot$).

3.4 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 $\mathbb{Q} \subsetneqq \mathbb{R} \subsetneqq \mathbb{C}$.

$(\mathbb{Z}, +, \cdot)$ 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 $(K^{n\times n})^* = \{A \in K^{n\times n} \mid detA \neq 0\} = Gl(n, K)$.
(5) Se $R_1, \ldots, R_n$, $n \geq 2$ sono anelli, anche il loro prodotto cartesiano $R = R_1 \times \ldots \times R_n$ è un anello rispetto all'addizione e moltiplicazione per componenti. Si ha $0_R = (0_{R_1}, \ldots, 0_{R_n})$ e $1_R = (1_{R_1}, \ldots, 1_{R_n})$.
(6) Siano I un insieme non vuoto e R un anello. L'insieme R^I di tutte le applicazioni $f : I \to R$ è un anello rispetto a

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

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

Si ha $1 : I \to R$, $x \mapsto 1$ e $0 : I \to R$, $x \mapsto 0$.
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 $I = \mathbb{N}_0 = \{0, 1, 2, \ldots\}$, otteniamo l'anello $R^{\mathbb{N}_0}$ di tutte le successioni di elementi di R.

3.5 L'anello dei polinomi.

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

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

$$(a_0, a_1, \ldots) \cdot (b_0, b_1, \ldots) = (a_0 \cdot b_0,\ a_0b_1 + a_1b_0, \ldots, \sum_{i=0}^{n} a_i b_{n-i}, \ldots)$$

Si ha $0 = (0, \ldots)$ e $1 = (1, 0, \ldots)$.
(2) Per $x = (0, 1, 0, \ldots)$ si ottiene $x^2 = (0, 0, 1, 0, \ldots)$, $x^3 = (0, 0, 0, 1, 0, \ldots)$ ecc.
Quindi possiamo scrivere ogni elemento

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

dove a_n è l'ultima componente diversa da zero di $(a_0, a_1, a_2, \dots)$.
Diremo che $\sum_{i=0}^{n} a_i x^i$ è un *polinomio* in x su R con i *coefficienti* $a_0, \dots, a_n$, dove a_n è detto il *coefficiente direttivo* e $n = \deg f$ il *grado* di f. Il polinomio $0 = (0, 0, \dots)$ per convenzione ha grado -1.
L'anello $R^{(\mathbb{N}_0)}$ con queste operazioni è detto *anello dei polinomi* in x su R e si indica con $R[x]$.
Identificando gli elementi di R con i *polinomi costanti* (di grado ≤ 0), possiamo interpretare R come sottoanello di $R[x]$.

(3) Se R è un dominio, allora

(i) $R[x]$ è un dominio,

(ii) $\deg(fg) = \deg f + \deg g$ per $f, g \in R[x] \setminus \{0\}$,

(iii) $R[x]^* = R^*$.

Infatti:
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$

4 Ideali

A. L'anello quoziente.

4.1 Definizione.

Sia $(R, +, \cdot)$ un anello. Un sottoinsieme non vuoto $I \subset R$ è detto *ideale* (bilatero) se per tutti gli elementi $a, b \in I$, $r \in R$ si ha $a + b \in I$, $ra \in I$ e $ar \in I$. Se $I \neq R$ si dice che I è un *ideale proprio*.

OSSERVAZIONI:
(1) Ogni anello possiede gli ideali banali R e $0 = \{0_R\}$.

(2) Ogni ideale I di R è un sottogruppo del gruppo abeliano $(R, +)$.
Infatti:
$\vdots$
$\vdots$

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

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

detto *l'ideale generato da* A.
Se R è commutativo, allora

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

In particolare, per $a \in R$, l'ideale

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

è detto *ideale principale* generato da a.

(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) Se un ideale I di un anello R contiene un elemento invertibile $a \in R^*$, allora $I = R$. Infatti:

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

In particolare, ogni campo possiede soltanto gli ideali banali 0 e K.

4.2 Esempi.

(1) Gli ideali di $\mathbb{Z}$ sono tutti principali.
Infatti:

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

(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.

4.3 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

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

Si ha che $\overline{a} = \overline{a'}$ 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:

$$\overline{a} + \overline{b} = \overline{a + b}$$
$$\overline{a} \cdot \overline{b} = \overline{ab}$$

Le operazioni sono ben definite:

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

Con queste operazioni R/I diventa un anello detto l'*anello quoziente di R modulo I*.
Si ha $0_{R/I} = \overline{0} = 0 + I = I$ e $\cdot$ è $1_{R/I} = \overline{1} = 1 + I$.

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

Sia $n \in \mathbb{N}$. Allora l'anello $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ delle classi di resto modulo n è l'anello quoziente di $\mathbb{Z}$ rispetto all'ideale $I = n\mathbb{Z}$. Infatti $[a] = \{x \in \mathbb{Z} \mid x \equiv a \bmod n\} = \{x \in \mathbb{Z} \mid x - a \in n\mathbb{Z}\} = \overline{a}$.

Abbiamo $\mathbb{Z}/n\mathbb{Z}^* = \{[a] \mid 0 < a < n, \text{ MCD}(a, n)\text{=}1\ \}$.
Quindi $\mathbb{Z}/n\mathbb{Z}$ è un campo se e solo se n è un numero primo.

<u>B. Ideali massimali.</u>

4.5 Insiemi ordinati

(1) Sia $\mathcal{M}$ un insieme. Un *ordine* (parziale) su $\mathcal{M}$ è una relazione $\leq$ con le proprietà

- riflessiva,
- antisimmetrica: se $x \leq y$ e $y \leq x$, allora $x = y$,
- transitiva.

Diremo che $(\mathcal{M}, \leq)$ è un *insieme parzialmente ordinato.* Se per $x, y \in \mathcal{M}$ si ha sempre $x \leq y$ oppure $y \leq x$, allora $\leq$ è detto *ordine totale* e $(\mathcal{M}, \leq)$ è *totalmente ordinato.*

(2) Sia $\mathcal{M}$ un insieme ordinato. Un elemento $y \in \mathcal{M}$ è detto

- *massimo* di $\mathcal{M}$ se $x \leq y$ per ogni $x \in \mathcal{M}$.
- *elemento massimale* di $\mathcal{M}$ se non esiste elemento $y' \in \mathcal{M}$ tale che $y \leq y'$ e $y \neq y'$.
- *maggiorante* di un sottoinsieme $\mathcal{N} \subset \mathcal{M}$ se $x \leq y$ per ogni $x \in \mathcal{N}$.

4.6 Esempi.

(1) $(\mathbb{R}, \leq)$ ‘e un insieme totalmente ordinato.

(2) 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 $A = R$.

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

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

4.7 Lemma di Zorn.

Sia $(\mathcal{M}, \leq)$ un insieme ordinato non vuoto. Se ogni sottoinsieme totalmente ordinato di $\mathcal{M}$ possiede un maggiorante in $\mathcal{M}$, allora $\mathcal{M}$ possiede un elemento massimale.

<u>OSSERVAZIONE:</u> L’enunciato del Lemma di Zorn è equivalente a:

- l’Assioma di Scelta: il prodotto cartesiano di una famiglia non vuota di insiemi non vuoti non è vuoto.

- Il Teorema sugli Insiemi Ben Ordinati: ogni insieme può essere ben ordinato, cioè esiste un ordine rispetto al quale ogni sottoinsieme non vuoto possiede un minimo.

4.8 Teorema: esistenza di ideali massimali.

Sia R un anello. Ogni ideale proprio di R è contenuto in un ideale massimale.
In particolare, ogni anello $R \neq 0$ possiede un ideale massimale.

DIMOSTRAZIONE:

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

C. IDEALI PRIMI.

4.9 Definizione di ideale primo.

Un ideale proprio $P \subset R$ di un anello R si dice *ideale primo* se per tutti gli elementi $x, y \in R$ con $x \cdot y \in P$ si ha $x \in P$ oppure $y \in P$.

4.10 Proposizione.

Sia R un anello commutativo.

(1) Un ideale P di R è primo se e solo se R/P è un dominio.

(2) Un ideale I di R è massimale se e solo se R/I è un campo.

<u>*DIMOSTRAZIONE :*</u>

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

4.11 Esempi.

(1) Se R è un dominio, allora 0 è un ideale primo.

(2) Gli ideali primi di $\mathbb{Z}$ sono 0 e gli ideali $p\mathbb{Z}$ con p primo.

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

5 Omomorfismi

5.1 Definizione.

Siano R e S due anelli.
Un'applicazione $\varphi : R \to S$ 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; in tal caso si dice che R e S sono isomorfi e si scrive $R \cong S$.

5.2 Nucleo e immagine.

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

1. Se $I \subset S$ è un ideale di S (rispettivamente, se $S' \subset S$ è un sottoanello di S), allora $\varphi^{-1}(I)$ è un ideale di R (rispettivamente, $\varphi^{-1}(S')$ è un sottoanello di R).
   In particolare, l'insieme $\mathrm{Ker}\varphi = \{a \in R \mid \varphi(a) = 0\}$ è un ideale di R, detto il *nucleo* di φ.

2. Se $R' \subset R$ è un sottoanello di R, allora $\varphi(R')$ è un sottoanello di S. In particolare, l'immagine $Im\varphi = \{\varphi(a) \mid a \in R\}$ è un sottoanello di S.

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

DIMOSTRAZIONE

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

5.3 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 $\mathrm{Im}\varphi = \mathbb{Z}$ non è un ideale di $\mathbb{Q}$.
(2) Sia R un dominio. L'applicazione

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

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

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

(3) Siano K un campo ed R un anello. Ogni omomorfismo di anelli $K \to R$ è iniettivo oppure nullo.
Infatti

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

(4) L'applicazione

$$\nu : R \to R/I,\ x \mapsto \overline{x} = x + I$$

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

5.4 Teorema di Fattorizzazione di Omomorfismi

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

$$\overline{f}\,\nu = f.$$

Si ha $\mathrm{Ker}\overline{f} = \mathrm{Ker}f/I = \{\overline{x} \mid x \in \mathrm{Ker}f\}$ e $\mathrm{Im}\overline{f} = \mathrm{Im}f$.
<u>*DIMOSTRAZIONE*</u>

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

5.5 Teorema Fondamentale dell'Omomorfismo

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

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

5.6 Esempi

(1) Se R è un dominio, allora l'ideale (x) è un ideale primo di $R[x]$.
Infatti
$\vdots$
$\vdots$
$\vdots$
$\vdots$
(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, vedi Esercizio 2.

6 Divisibilità

In questo paragrafo sia R *sempre un dominio.*

A. Domini a ideali principali.

6.1 Domini a ideali principali. Definizione.

(1) Si dice che R è un *dominio a ideali prinicipali*, ovvero un *PID* (principal ideal domain), se tutti gli ideali di R sono principali.
(2) 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 $y \in (x)$.
(3) Due elementi $x, y \in R$ di un dominio R si dicono *associati* se $x \mid y$ e $y \mid x$. Scriveremo $x \sim y$.

OSSERVAZIONE: Sono equivalenti i seguenti enunciati:

(i) $x \sim y$

(ii) Esiste $r \in R^*$ tale che $y = rx$

(iii) $(x) = (y)$

DIMOSTRAZIONE:
$\vdots$
$\vdots$

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

6.2 Elementi irriducibili.

Un elemento $p \in R$ di un dominio R si dice *irriducibile* se

(i) p non è invertibile

(ii) p possiede soltanto i divisori banali, ovvero se $xy = p$, allora $x \in R^*$ oppure $y \in R^*$.

OSSERVAZIONE: Un elemento $p \in R$ è irriducibile se (p) è un ideale primo. Non vale il converso (vedi Esercizi, Foglio 2).

6.3 Proposizione.

Sia R un PID e sia $0 \neq p \in R$ un elemento non invertibile. Sono equivalenti i seguenti enunciati:

1. p è irriducibile.
2. (p) è un ideale primo.
3. (p) è un ideale massimale.

In particolare, un ideale di un PID è primo se e solo se è zero oppure massimale.

DIMOSTRAZIONE:

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

B. Domini a fattorizzazione unica.

6.4 Domini a fattorizzazione unica. Definizione.

(1) Si dice che R è un *dominio a fattorizzazione unica*, ovvero un *UFD* (unique factorization domain), se ogni elemento non invertibile $a \in R$ con $a \neq 0$ può essere scritto come prodotto di elementi irriducibili e questa scomposizione è unica a meno dell'ordine e di associazione. Più precisamente:

(i) Esistono elementi irriducibili $p_1, \dots, p_n \in R$ tali che $a = p_1 \cdot \ldots \cdot p_n$.

(ii) Se anche $q_1, \dots, q_m \in R$ sono elementi irriducibili tali che $a = q_1 \cdot \ldots \cdot q_m$, allora $m = n$ ed esiste una permutazione $\sigma \in S_n$ tale che $p_i \sim q_{\sigma(i)}$ per ogni $1 \leq i \leq n$.

OSSERVAZIONE (Teorema Fondamentale dell'Aritmetica). L'anello $\mathbb{Z}$ è un UFD.

6.5 Anelli noetheriani.

Teorema. Sono equivalenti i seguenti enunciati (per un qualsiasi anello R):

(1) Ogni ideale I di R è finitamente generato: esiste un insieme finito $A = \{a_1, \dots, a_n\}$ tale che $I = (A)$.

(2) Ogni catena ascendente di ideali

$$I_1 \subset I_2 \subset I_3 \subset \ldots R$$

è stazionaria, cioè esiste $n \in \mathbb{N}$ tale che $I_n = I_{n+1} = I_{n+2} = \ldots$.

(3) Ogni insieme non vuoto di ideali di R possiede un elemento massimale rispetto a "$\subset$".

Un anello con queste proprietà è detto *noetheriano*[1].

DIMOSTRAZIONE:

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

OSSERVAZIONE: Ovviamente ogni PID è un anello noetheriano.

[1] questi anelli furono introdotti da Emmy Noether (1882-1935)

6.6 Ogni PID è un UFD.

Teorema: Ogni dominio a ideali principali è un dominio a fattorizzazione unica.

DIMOSTRAZIONE:

$\vdots$

6.7 Massimo comun divisore e minimo comune multiplo.

Siano $a_1, \dots, a_r \in R \setminus \{0\}$.

1. Un elemento $d \in R$ è detto *massimo comun divisore* di $a_1, \dots, a_r$ se soddisfa
   (a) $d \mid a_i$ per ogni $1 \leq i \leq r$,
   (b) se $t \mid a_i$ per ogni $1 \leq i \leq r$, allora $t \mid d$;
2. Un elemento $m \in R$ è detto *minimo comune multiplo* di $a_1, \dots, a_r$ se soddisfa
   (a) $a_i \mid m$ per ogni $1 \leq i \leq r$,
   (b) se $a_i \mid c$ per ogni $1 \leq i \leq r$, allora $m \mid c$.

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

<u>OSSERVAZIONI:</u>

1. Massimo comun divisore e minimo comune multiplo esistono sempre quando R è un UFD.

   Infatti

⋮

2. Massimo comun divisore e minimo comune multiplo, quando esistono, sono unici a meno di associazione.

6.8 Elementi coprimi.

Siano $a_1, \dots, a_r \in R$. Si dice che $a_1, \dots, a_r$ sono *coprimi* se ciascun comun divisore di $a_1, \dots, a_r$ è invertibile, ovvero se $1 = MCD(a_1, \dots, a_r)$.

<u>OSSERVAZIONI:</u>

1. Siano $b_1, \dots, b_r \in R \setminus \{0\}$ con $d = MCD(b_1, \dots, b_r)$ e $b_i = d \cdot a_i$ per $1 \leq i \leq r$. Allora $a_1, \dots, a_r$ sono coprimi.
2. Lemma di Euclide: Siano R un UFD, $x, a \in R$ elementi coprimi, e sia $b \in R$. Se $x \mid ab$, allora $x \mid b$.
3. Identità di Bézout: Se R è un PID, allora a, b sono coprimi se e solo se esistono $r, s \in R$ tali che $1 = ra + sb$.

<u>DIMOSTRAZIONE:</u> Esecizi Foglio 3.

B. ANELLI EUCLIDEI.

6.9 Anelli euclidei. Definizione.

Un *anello euclideo* è costituito da una coppia (R, δ) dove R è un dominio e $\delta : R \setminus \{0\} \to \mathbb{N}_0$ è una funzione con la proprietà che per tutti gli elementi $a, b \in R \setminus \{0\}$ esistono $q, r \in R$ tali che

(i) $a = qb + r$ (*divisione col resto*)

(ii) $r = 0$ oppure $\delta(r) < \delta(b)$

OSSERVAZIONE: Ogni anello euclideo è un PID.
Infatti
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$

6.10 L'Algoritmo Euclideo.

In un anello euclideo (R, δ) possiamo calcolare il massimo comun divisore di $a, b \in R \setminus \{0\}$ tramite divisioni successive come segue:
Se $b \mid a$, allora $b = MCD(a, b)$. Altrimenti poniamo $r_0 = b$ e eseguiamo divisioni col resto:

$$\begin{array}{llllll}
a = q_1\, r_0 + r_1 & \text{con} & q_1, r_1 \in R & \text{e} & \delta(r_1) < \delta(r_0) \\
r_0 = q_2\, r_1 + r_2 & \text{con} & q_2, r_2 \in R & \text{e} & \delta(r_2) < \delta(r_1) \\
\vdots & & \vdots & & \vdots \\
r_{n-1} = q_{n+1}\, r_n + r_{n+1} & \text{con} & q_{n+1}, r_{n+1} \in R & \text{e} & r_{n+1} = 0.
\end{array}$$

Allora

$$r_n = MCD(a, b) \quad \text{e} \quad \frac{ab}{r_n} = mcm(a, b).$$

DIMOSTRAZIONE:
$\vdots$

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

6.11 Esempi.

(1) $(\mathbb{Z}, |\cdot|)$ è un anello euclideo.
(2) $(\mathbb{Z}[i], \delta)$ è un anello euclideo, vedi Esercizio 5.

6.12 Proposizione

1. Sia R un anello commutativo e siano $f, g \in R[x]$ due polinomi non nulli. Se g è monico, allora esistono $q, r \in R[x]$ tali che
   (i) $f = qg + r$
   (ii) $\deg(r) < \deg(g)$
2. Se K è un campo, allora $(K[x], \deg)$ è un anello euclideo, e in particolare un PID (e un UFD).

<u>DIMOSTRAZIONE:</u>
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$

<u>OSSERVAZIONE:</u> $R[x]$ è un PID se e solo se R è un campo (vedi Esercizi, Foglio 2).

Parte III

POLINOMI

Menzioniamo due risultati importanti senza dimostrazione.

Teorema di Gauss.

Se R è un UFD, anche l'anello dei polinomi $R[x]$ è un UFD.

Teorema della Base di Hilbert.

Se un anello commutativo R è noetheriano, anche l'anello dei polinomi $R[x]$ è noetheriano.

7 Zeri di polinomi

7.1 Polinomi irriducibili su un campo.

Teorema: Sia K un campo e sia $f \in K[x]$ un polinomio. Sono equivalenti i seguenti enunciati:

1. f è un elemento irriducibile di $K[x]$.
2. $\deg f = n > 0$ e f non può essere scritto come prodotto di due polinomi di grado $< n$.
3. L'anello quoziente $K[x]/(f)$ è un campo.

DIMOSTRAZIONE

$\vdots$

7.2 Estensione di un campo, grado dell'estensione

Siano K, F campi. Se $K \subset F$ è un sottocampo, si dice che F è un'*estensione* di K. In tal caso F è anche uno spazio vettoriale su K. La dimensione di F come spazio vettoriale su K è detta *grado* dell'estensione e si indica con $[F : K] = \dim_K F$.
Un'estensione si dice *finita* se $[F : K] < \infty$.

7.3 L'estensione di campi $K \subset F = K[x]/(f)$

Sia K un campo e sia $f \in K[x]$ un polinomio irriducibile di grado n. Allora l'applicazione

$$\varphi : K \to K[x]/(f) = F,\ a \mapsto \overline{a} = a + (f)$$

è un monomorfismo e $K \subset F$ è un'estensione di campi di grado $[F : K] = n$. Gli elementi

$$\overline{1}, \overline{x}, \overline{x}^2, \ldots, \overline{x}^{n-1}$$

formano una base di F su K.

<u>*DIMOSTRAZIONE*</u> :

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

7.4 Definizione

Sia R commutativo, e sia $f \in R[x]$, $f = \sum_{i=0}^n a_i x^i$. Per $\alpha \in R$ poniamo

$$f(\alpha) = \sum_{i=0}^n a_i \alpha^i.$$

L'elemento $\alpha \in R$ è detto *zero* (oppure *radice*) di f se $f(\alpha) = 0$.

7.5 Teorema di Kronecker

Sia K un campo e sia $f \in K[x]$ di grado $n > 0$. Allora esiste un'estensione $K \subset F$ di grado $[F : K] \leq n$ nella quale f possiede uno zero $\alpha \in F$.

<u>*DIMOSTRAZIONE*</u> :

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

7.6 Teorema di Ruffini

Sia R un anello commutativo. Per $\alpha \in R$ l'applicazione

$$\varepsilon_\alpha : R[x] \to R,\ f \mapsto f(\alpha)$$

è un epimorfismo con nucleo $\mathrm{Ker}\varepsilon_\alpha = (x - \alpha)$. In particolare, $\alpha \in R$ è uno zero di un polinomio $f \in R[x]$ se e solo se il polinomio $x - \alpha$ divide f. Inoltre, $R[x]/(x - \alpha) \cong R$.

DIMOSTRAZIONE

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

7.7 Corollario

Sia R un dominio e sia $f \in R[x]$ un polinomio di grado $n \geq 0$. Allora f possiede al più n zeri in R.

DIMOSTRAZIONE

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

7.8 Polinomi irriducibili di grado ≤ 3.

Sia K un campo.

(1) Ogni polinomio $f = a_0 + a_1 x$ di grado 1 è irriducibile e ammette l'unico zero $\alpha = -a_1^{-1} a_0 \in K$.

(2) Se $f \in K[x]$ è un polinomio irriducibile di grado $\deg f > 1$ allora f non ammette zeri.

(3) Un polinomio $f \in K[x]$ di grado $\deg f \in \{2, 3\}$ è irriducibile se e solo se non ammette zeri.

DIMOSTRAZIONE

$\vdots$

$\vdots$

$\vdots$

$\vdots$

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

7.9 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 $f = a(x - \alpha_1)(x - \alpha_2)...(x - \alpha_n)$ con a, α_1,...,$\alpha_n \in \mathbb{C}$.

(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

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

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

Infatti
$\vdots$
$\vdots$
$\vdots$
$\vdots$

(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
$\vdots$
$\vdots$
$\vdots$
$\vdots$

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

(5) $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$ (vedi Esercizi, Foglio 3).

(6) 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 $f = 2x + 2$ è irriducibile in $\mathbb{Q}[x]$, ma non in $\mathbb{Z}[x]$. Il polinomio $6x^2 + 5x + 1 \in \mathbb{Z}[x]$ è riducibile di grado 2, pur non avendo zeri in $\mathbb{Z}$ (vedi Esercizi, Foglio 3). Dunque l'ipotesi "campo" in 7.8 è essenziale !

8 Criteri di irriducibilità

In questo paragrafo sia R *sempre un dominio.*

8.1 Polinomi primitivi.

Un polinomio $f \in R[x] \setminus \{0\}$ è detto *primitivo* se i suoi coefficienti sono coprimi.

8.2 Esempi.

(1) Ogni polinomio monico è primitivo.
(2) Se R è un campo, ogni polinomio $f \in R[x] \setminus \{0\}$ è primitivo.
(3) Ogni polinomio irriducibile di grado $n > 0$ è primitivo:

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

(4) $2 \in \mathbb{Z}[x]$ è irriducibile ma non primitivo.

8.3 Lemma 1 (Riduzione modulo I)

Sia I un ideale di R. L'applicazione

$$\rho : R[x] \to R/I[x],\ \sum_{i=0}^{n} a_i\, x^i \mapsto \sum_{i=0}^{n} \overline{a_i}\, x^i$$

è un epimorfismo con nucleo $IR[x] = \{f \in R[x] \mid \text{tutti i coefficienti di } f \text{ appartengono ad } I\}$.

8.4 Lemma di Gauss.

Sia R un UFD. Se $f, g \in R[x]$ sono polinomi primitivi, anche il prodotto fg è primitivo.

<u>*DIMOSTRAZIONE*</u>

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

8.5 Il campo dei quozienti.

Sia $S = R \setminus \{0\}$.
(1) Sul prodotto cartesiano $R \times S$ definiamo la relazione

$$(a, s) \sim (b, t) \quad \text{se} \quad at = sb$$

$\sim$ è una relazione di equivalenza. Scriviamo $\frac{a}{s}$ per la classe di equivalenza di (a, s) rispetto a $\sim$.
(2) Sull'insieme

$$Q = Q(R) = \{\frac{a}{s} \;\mid\; a \in R, s \in S\}$$

delle classi di equivalenza rispetto a $\sim$ definiamo le operazioni

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$$

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

Le operazioni sono ben definite:

$\vdots$

$\vdots$

$\vdots$

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

(3) $(Q, +, \cdot)$ è un campo con $0 = \frac{0}{1}$ e $1 = \frac{1}{1}$, detto *campo dei quozienti* di R.

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

(4) L'applicazione $\varphi : R \to Q$, $a \mapsto \frac{a}{1}$ è un monomorfismo. Quindi possiamo identificare R con un sottoanello di Q.

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

(5) (Q, φ) hanno la proprietà universale seguente: per ogni campo K e ogni monomorfismo $\psi : R \to K$ esiste uno e un solo monomorfismo $\tilde{\psi} : Q \to K$ tale che $\tilde{\psi}\,\varphi = \psi$.
Dimostrazione:

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

8.6 Lemma 2

Sia R un UFD e sia Q il campo dei quozienti di R.

1. Per ogni $0 \neq g \in Q[x]$ esiste $\alpha \in Q \setminus \{0\}$ tale che $\alpha\, g \in R[x]$ sia primitivo.
2. Se $g \in R[x]$ è primitivo, e se $\alpha \in Q$ soddisfa $\alpha\, g \in R[x]$, allora $\alpha \in R$.

DIMOSTRAZIONE

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

$\vdots$

8.7 Proposizione

Sia R un UFD e sia $0 \neq f \in R[x]$.

1. Esistono $d \in R \setminus \{0\}$ e un polinomio primitivo $\tilde{f} \in R[x]$ tali che $f = d\,\tilde{f}$.
2. Se f è primitivo, allora f è irriducibile in $R[x]$ se e solo se lo è in $Q[x]$.

<u>*DIMOSTRAZIONE*</u>

$\vdots$

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

8.8 Riduzione modulo p.

Sia $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ un polinomio primitivo di grado $n > 0$. Siano inoltre P un ideale primo di R e $\rho : R[x] \to R/P[x]$, $\sum_{i=0}^{n} a_i\, x^i \mapsto \sum_{i=0}^{n} \overline{a_i}\, x^i$ come in 8.3. Se $a_n \notin P$ e $\rho(f)$ è irriducibile in $R/P[x]$, allora f è irriducibile in $R[x]$.

DIMOSTRAZIONE

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

8.9 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,...,a_{n-1}

(iii) p^2 non divide a_0.

<u>*DIMOSTRAZIONE*</u>

$\vdots$

8.10 Esempi

(1) $f = x^5 - x^2 + 1 \in \mathbb{Z}[x]$ è irriducibile. Riduzione modulo 2:

$\vdots$

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

8.11 Sostituzione

Sia K un campo, $f = \sum_{i=0}^{n} a_i x^i \in K[x]$. Sostituiamo 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 :

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

8.12 Esempio.

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

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

Nota (per l'anno accademico 2009/2010): Termina qui la parte sulla quale verterà *l'esame integrativo* (per chi, nel passaggio al nuovo ordinamento, desidera farsi riconoscere i crediti di *Elementi di Algebra* come crediti di *Algebra*).

Parte IV

CAMPI

9 Estensioni algebriche

9.1 Aggiunzioni, elementi algebrici, elementi trascendenti.

Sia $K \subset F$ un'estensione.

1. Dato un sottoinsieme $A \subset F$, il campo

$$K(A) = \bigcap \{L \mid L \text{ è un sottocampo di } F \text{ contenente } K \text{ e } A\}$$

si dice *aggiunzione* di A a K.

2. Un elemento $\alpha \in F$ si dice *algebrico* su K se esiste un polinomio $0 \neq f \in K[x]$ tale che $f(\alpha) = 0$. Altrimenti α è detto *trascendente* su K.

3. Se tutti gli elementi di F sono algebrici su K, si dice che $K \subset F$ è un'*estensione algebrica*.

OSSERVAZIONE: Ogni estensione finita è algebrica.
Infatti
$\vdots$

9.2 Il polinomio minimo

Sia $K \subset F$ un'estensione, e sia $\alpha \in F$ un elemento algebrico su K.

1. Esiste uno e un solo polinomio $h \in K[x]$ monico e irriducibile tale che $h(\alpha) = 0$, detto *polinomio minimo* di α su K.

2. Per ogni $g \in K[x]$ si ha $g(\alpha) = 0$ se e solo se $h \mid g$.

3. Se $\deg h = n$, allora $K \hookrightarrow K[x]/(h) \cong K(\alpha)$ è un'estensione di grado n con K- base $1, \alpha, \alpha^2,\ldots,\alpha^{n-1}$.

<u>*DIMOSTRAZIONE*</u> :

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

9.3 Esempi

(1) Il polinomio minimo di i su $\mathbb{R}$ è x^2+1.

(2) Il polinomio minimo di $\sqrt{2} \in \mathbb{R}$ su $\mathbb{Q}$ è x^2-2.

(3) In 9.1(2) il polinomio minimo di $\overline{x} \in F$ su $K = \mathbb{Z}/2\mathbb{Z}$ è x^2+x+1.

(4) Il polinomio minimo di $\alpha = -\frac{1}{2} + i\frac{1}{2}\sqrt{3} \in \mathbb{C}$ su $\mathbb{Q}$ è x^2+x+1.

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

9.4 Lemma sul grado

Siano $K \subset F$ un'estensione finita e sia L un *campo intermedio*, cioè $K \subset L \subset F$ dove $K \subset L$ e $L \subset F$ sono estensioni di campi. Allora

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

<u>*DIMOSTRAZIONE*</u> :

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

9.5 Corollario.

Sia $K \subset F$ un'estensione.

1. Se $[F : K]$ è un numero primo, allora non esistono campi intermedi propri.
2. $K \subset F$ è un'estensione finita se e solo se esistono elementi algebrici $\alpha_1, \ldots, \alpha_n \in F$ tali che $F = K(\alpha_1, \ldots, \alpha_n)$.
3. Sia $K \subset L \subset F$ un campo intermedio. Allora $K \subset F$ è un'estensione algebrica se e solo se $K \subset L$ e $L \subset F$ sono estensioni algebriche.
4. Sia $\overline{K}$ l'insieme degli elementi di F che sono algebrici su K. Allora $K \subset \overline{K}$ è un'estensione algebrica, detta *chiusura algebrica* di K in F (Esercizio 14).

DIMOSTRAZIONE :

$\vdots$

9.6 Esempi.

(1) La chiusura algebrica $\mathbb{Q} \subset \overline{\mathbb{Q}}$ di $\mathbb{Q}$ in $\mathbb{C}$ è un'estensione algebrica di grado infinito (Esercizi, Foglio 5).
(2) π è trascendente su $\mathbb{Q}$ (Lindemann 1882).

10 Campi di riducibilità completa.

10.1 Teorema e Definizione.

Sia K un campo e sia $f \in K[x]$ un polinomio di grado $n > 0$. Allora esiste un'estensione $K \subset F$ di grado $[F : K] \leq n!$ tale che

1. $f = a(x - \alpha_1)(x - \alpha_2)...(x - \alpha_n)$ con $a \in K$, $\alpha_1, \alpha_2, ..., \alpha_n \in F$.
2. Se $K \subset F' \subset F$ è un campo intermedio contenente $\alpha_1, \ldots, \alpha_n$, allora $F' = F$.

F è detto *campo di riducibilità completa* (oppure *campo di spezzamento*) di f su K.
Si ha $F = K(\alpha_1, \ldots, \alpha_n)$.

<u>*DIMOSTRAZIONE*</u> :

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

10.2 Esempi

(1) Il campo di riducibilità completa di $f = x^3 - 1$ su $\mathbb{Q}$:

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

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

(2) Il campo di riducibilità completa di $g = x^3 - 2$ su $\mathbb{Q}$:

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

(3) Il campo di riducibilità completa di $x^4 - x$ su $K = \mathbb{Z}/2\mathbb{Z}$:

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

10.3 Lemma.

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

DIMOSTRAZIONE : Per 9.5(2) esistono elementi algebrici $\alpha_1, \ldots, \alpha_n \in F$ tali che $F = K(\alpha_1, \ldots, \alpha_n)$. Procediamo per induzione su n.
$n = 0$: Allora $F = K$ e possiamo sceglere $\tau = \sigma$.
$n > 0$: σ induce un omomorfismo di anelli

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

Sia f il polinomio minimo di α_1 su K e sia $f' = \tilde{\sigma}(f) \in K'[x]$. Sappiamo che $(f) = \mathrm{Ker}\varepsilon$ dove $\varepsilon : K[x] \to K(\alpha_1) \subset F$, $h \mapsto h(\alpha_1)$ per la definizione 9.2. Sia g' un fattore irriducibile di f', e consideriamo

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

Per 7.3 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 $\mathrm{Ker}\varepsilon = (f) \subset \mathrm{Ker}\nu\tilde{\sigma}$. Per il Teorema 5.4 possiamo fattorizzare $\nu\tilde{\sigma} : K[x] \to F_1$ attraverso ε, cioè esiste $\tau_1 : K(\alpha_1) \cong K[x]/\mathrm{Ker}\varepsilon \to F_1$ tale che

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

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

10.4 Unicità del campo di riducibilità completa.

Teorema: Siano K, K' campi con un isomorfismo $\sigma : K \to K'$. 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 $\tau : F \to F'$ 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 $\tau : F \to L$ 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 5.3(3) che τ è iniettivo. Resta da dimostrare $\mathrm{Im}\tau = F'$.
Sappiamo che $f = a(x - \alpha_1) \ldots (x - \alpha_n)$ dove $a \in K$ e $\alpha_1, \ldots, \alpha_n$ sono gli zeri di f in F. Abbiamo $F = K(\alpha_1, \ldots, \alpha_n)$ e $\mathrm{Im}\tau = K'(\tau(\alpha_1), \ldots, \tau(\alpha_n))$. Come nel Lemma, σ e τ inducono omomorfismi di anelli

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

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

10.5 Estensioni normali.

Un'estensione $K \subset F$ è detta *normale* se

1. $K \subset F$ è un'estensione algebrica;
2. per ogni $\alpha \in F$ il polinomio minimo $f \in K[x]$ di α su K è prodotto di fattori lineari in $F[x]$, cioè

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

   con $a \in K, \alpha_1, \ldots, \alpha_n \in F$.

10.6 Esempi.

(1) Ogni estensione di grado 2 è normale.
Infatti
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮

(2) Sia p un numero primo. Allora $\mathbb{Q} \subset \mathbb{Q}(\sqrt{p})$ e $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\sqrt[4]{p})$ sono estensioni normali, ma $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{p})$ non è normale.
Infatti
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮

(3) Se $K \subset F$ è un'estensione normale e $K \subset L \subset F$ è un campo intermedio, allora $L \subset F$ è normale. (Esercizio 17)

10.7 Teorema.

Sia $K \subset F$ un'estensione. $K \subset F$ è un'estensione finita e normale se e solo se F è campo di riducibilità completa di un polinomio non costante $f \in K[x]$.

<u>*DIMOSTRAZIONE*</u> :
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮

10.8 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 $\tau : F \to F$ tale che $\tau(\alpha) = \beta$ e $\tau\,|_K = \mathrm{id}_K$.

<u>*DIMOSTRAZIONE*</u> :

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

11 Separabilità

<u>A. La caratteristica di un campo.</u>

11.1 La caratteristica di un campo.

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

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

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

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

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

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

<u>OSSERVAZIONE:</u> 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 $\varphi : K \to K$, $x \mapsto x^p$ è un monomorfismo, detto *omomorfismo di Frobenius*.
Infatti

⋮
⋮
⋮
⋮
⋮
⋮
⋮

11.2 Esempi

(1) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ hanno caratteritica 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 $p \neq 0$.

11.3 Teorema

Per un campo K consideriamo il più piccolo sottocampo di K

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

Si ha $P = \{ (n \cdot 1_K)(m \cdot 1_K)^{-1} \mid n, m \in \mathbb{Z} \}$. Inoltre
$\operatorname{char} K = 0$ se e solo se $P \cong \mathbb{Q}$,
$\operatorname{char} K = p$ se e solo se $P \cong \mathbb{Z}/p\mathbb{Z}$.

DIMOSTRAZIONE :

⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮
⋮

11.4 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 :

⋮
⋮
⋮
⋮
⋮

B. MOLTEPLICITÀ DEGLI ZERI.

11.5 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 $(x-\alpha)^{n+1}$.

11.6 La derivata formale di un polinomio.

Sia K un campo. L'applicazione

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

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. $D(fg) = D(f)g + fD(g)$

11.7 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 $D(f)$.

<u>*DIMOSTRAZIONE*</u> : $\Rightarrow$: 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 $(x-\alpha)^2$. $\square$

11.8 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) $D(f) \neq 0$.

<u>*DIMOSTRAZIONE*</u> :

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

11.9 Polinomi separabili.

Siano K un campo e $f \in K[x]$ un polinomio di grado $n > 0$. Se f è irriducibile, diremo che f è *separabile* quando soddisfa gli enunciati equivalenti del Teorema 11.8. In generale, diremo che f è *separabile* se lo sono tutti i suoi fattori irriducibili.

11.10 Esempi.

(1) L'ipotesi "irriducibile" in 11.8 è indispensabile: ad esempio, il polinomio $f = (x-1)^2 \in \mathbb{Q}[x]$ soddisfa $Df = 2(x-1) \neq 0$ pur avendo uno zero di molteplicità 2.
(2) Su un campo K di caratteristica zero ogni polinomio non costante è separabile:
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$

(3) Il polinomio $x^2 - 1 = (x-1)(x+1) \in \mathbb{Q}[x]$ è separabile. Ma in $\mathbb{Z}/2\mathbb{Z}[x]$ abbiamo $x^2 - 1 = (x-1)^2$ con uno zero di molteplicità 2, e infatti $D(x^2-1) = 2x = 0$.

(4) Se $f_1, \ldots, f_n \in K[x]$ sono polinomi non costanti, allora $f = f_1 \cdot \ldots \cdot f_n$ è separabile se e solo se lo sono tutti gli f_i, vedi Esercizio 21.

(5) Un polinomio separabile $f \in K[x]$ è separabile anche in qualsiasi estensione $K \subset F$.
Infatti se $f = f_1 \cdot \ldots \cdot f_n$ è una scomposizione in fattori irriducibili in $K[x]$ e g è un fattore irriducibile di f in $F[x]$, allora $f_1 \cdot \ldots \cdot f_n \in (g)$ ed, essendo (g) un ideale primo di $F[x]$ per 6.3 e 6.12, possiamo dedurre che esitste un i tale che $f_i \in (g)$, cioè $g \mid f_i$ in $F[x]$. Ma allora non può esistere un'estensione di F in cui g abbia zeri di molteplicità > 1. Quindi g è separabile in $F[x]$ e concludiamo che f è separabile in $F[x]$.

C. ESTENSIONI SEPARABILI.

11.11 Campi perfetti.

Un campo K è detto *perfetto* se ogni polinomio non costante $f \in K[x]$ è separabile.

11.12 Teorema.

Un campo K di caratterstica $p \neq 0$ è perfetto se e solo se l'omomorfismo di Frobenius

$$\varphi : K \to K,\ x \mapsto x^p$$

è suriettivo (e quindi biiettivo).
DIMOSTRAZIONE :
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

11.13 Estensioni separabili.

Sia $K \subset F$ un'estensione. Un *elemento* $\alpha \in F$ è *separabile* su K se α è algebrico su K e il suo polinomio minimo su K è separabile. Se ogni $\alpha \in F$ è separabile su K, diremo che l'*estensione* $K \subset F$ è *separabile*.

<u>OSSERVAZIONI:</u>
(1) Ogni estensione algebrica di un campo perfetto è separabile.
(2) Ogni campo di caratteristica zero è perfetto (vedi 11.10 (2)).
(3) Ogni campo finito è perfetto per il Teorema 11.12.
(4) Dato un campo intermedio $K \subset L \subset F$, si ha che $K \subset F$ è separabile se e solo se lo sono $K \subset L$ e $L \subset F$ (Esercizio 21).

11.14 Esempio: un'estensione algebrica non separabile

Per un numero primo p consideriamo il campo delle funzioni razionali $K = \mathbb{Z}/p\mathbb{Z}(x)$ su $\mathbb{Z}/p\mathbb{Z}$. Sappiamo che K è un campo infinito di caratteristica p.
Verifichiamo che K non è perfetto: Prendiamo il polinomio $f = y^p - x \in K[y]$, interpretato quindi come polinomio primitivo nell'indeterminata y sull'anello K. Poiché x è un elemento irriducibile di $\mathbb{Z}/p\mathbb{Z}[x]$, si vede con un argomento analogo a 8.10(3) che f è irriducibile su $\mathbb{Z}/p\mathbb{Z}[x]$, e quindi per 8.7 anche sul campo dei quozienti $K = Q(\mathbb{Z}/p\mathbb{Z}[x])$. 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.

Parte V

<u>TEORIA DI GALOIS</u>

12 Campi intermedi e sottogruppi

12.1 Il campo fisso.

Sia F un campo.
(1) L'insieme degli automorfismi $\varphi : F \to F$ forma un gruppo $\mathrm{Aut}F$ rispetto alla composizione di applicazioni, detto *gruppo degli automorfismi* di F.
(2) Se $G \leq \mathrm{Aut}F$ è un sottogruppo, allora l'insieme

$$\mathrm{Fix}_F(G) = \{a \in F \mid \varphi(a) = a \text{ per ogni } \varphi \in G\}$$

è un sottocampo di F, detto *campo fisso* di G in F.
<u>*DIMOSTRAZIONE*</u> :
Verifichiamo (2):

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

<u>*OSSERVAZIONE*</u> : Sia $K = \mathrm{Fix}_F(G) \subset F$. Per ogni sottogruppo $H \leq G$ si ottiene un campo intermedio $K \subset L = \mathrm{Fix}_F(H) \subset F$.

12.2 Lemma.

Dati due campi K, F, l'insieme K^F di tutte le applicazioni $F \to K$ forma uno spazio vettoriale su K rispetto alla somma di applicazioni e alla moltiplicazione per uno scalare

$$k \cdot f : F \to K,\ x \mapsto k \cdot f(x).$$

I monomorfismi $F \to K$ formano un insieme linearmente indipendente di K^F.
<u>*DIMOSTRAZIONE*</u> :

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

12.3 Lemma di Dedekind.

Siano K, F due campi con n monomorfismi distinti $\varphi_1, \ldots, \varphi_n : F \to K$. Allora

$$L = \{a \in F \mid \varphi_1(a) = \varphi_2(a) = \ldots = \varphi_n(a)\}$$

è un sottocampo di F con $[F : L] \geq n$.

<u>*DIMOSTRAZIONE*</u> :

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

12.4 La traccia di un gruppo finito.

Siano F un campo e $G \leq \mathrm{Aut}F$ un sottogruppo finito. L'applicazione

$$\tau : F \to F,\ a \mapsto \sum_{\varphi \in G} \varphi(a)$$

è detta *traccia* di G in F. Si ha $\mathrm{Im}\tau = \mathrm{Fix}_F(G)$.

<u>*DIMOSTRAZIONE*</u> :

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

12.5 Teorema di Artin.

Siano F un campo e $G \leq \mathrm{Aut}F$ un sottogruppo finito di n elementi. Allora

$$[F : \mathrm{Fix}_F(G)] = n.$$

<u>*DIMOSTRAZIONE*</u> :

$\vdots$
$\vdots$

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

12.6 Il gruppo di Galois.

Sia $K \subset F$ un'estensione di campi. Allora l'insieme

$$\mathrm{Gal}(F/K) = \{\varphi \in \mathrm{Aut}F \mid \varphi(a) = a \text{ per ogni } a \in K\} = \{\varphi \in \mathrm{Aut}F \mid \varphi\,|_K = \mathrm{id}\}$$

è un sottogruppo di$\mathrm{Aut}F$, detto *gruppo di Galois* di F su K.

OSSERVAZIONI
(1) Per ogni estensione finita $K \subset F$ si ha che $\mid \mathrm{Gal}(F/K) \mid$ divide $[F : K]$.
(2) Se $K \subset L \subset F$ è un campo intermedio, allora $\mathrm{Gal}(F/L) \leq \mathrm{Gal}(F/K)$.
DIMOSTRAZIONE :
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$

12.7 Esempi.

(0) Sia F un campo e sia $P = \bigcap\{L \mid L \text{ è un sottocampo di } F\}$ il più piccolo sottocampo di F come in 11.3. Allora $\mathrm{Gal}(F/P) = \mathrm{Aut}F$.
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
(1) Sia $d \in \mathbb{Z} \setminus \{0, 1\}$ prodotto di numeri primi distinti e sia $F = \mathbb{Q}(\sqrt{d})$. Allora $\mathrm{Gal}(F/\mathbb{Q}) = \mathrm{Aut}F$ è un gruppo di ordine 2.

$\vdots$

(2) Sia $F = \mathbb{Q}(\sqrt[3]{2})$. Allora $\mathrm{Aut}F = \{\mathrm{id}\}$.

$\vdots$

12.8 Teorema.

Siano F un campo e $G \leq \mathrm{Aut}F$ un sottogruppo finito. Allora

$$\mathrm{Gal}(F/\mathrm{Fix}_F(G)) = G.$$

<u>*DIMOSTRAZIONE*</u> :

$\vdots$

13 Estensioni di Galois

13.1 Teorema e Definizione.

Per un'estensione di campi sono equivalenti i seguenti enunciati:

1. Esiste un sottogruppo finito $G \leq \mathrm{Aut}F$ tale che $K = \mathrm{Fix}_F(G)$.
2. $K \subset F$ è un'estensione finita con $\mathrm{Fix}_F(\mathrm{Gal}(F/K)) = K$.
3. $K \subset F$ è un'estensione finita di grado $[F : K] = \mid \mathrm{Gal}(F/K) \mid$.

Un'*estensione di Galois* è un'estensione $K \subset F$ che soddisfa queste proprietà.

<u>*DIMOSTRAZIONE*</u> :

⋮

⋮

⋮

⋮

13.2 Esempi

(1) Se $d \in \mathbb{Z}$ è prodotto di primi distinti, allora $\mathbb{Q} \subset \mathbb{Q}(\sqrt{d})$ è un'estensione di Galois.
(2) $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ non è un'estensione di Galois.
(3) Se F è un campo finito e P è il più piccolo sottocampo di F, allora $P \subset F$ è un'estensione di Galois e $\mathrm{Aut}F$ è generato dall'omomorfismo di Frobenius.
Infatti

⋮

⋮

⋮

⋮

⋮

⋮

⋮

⋮

⋮

13.3 Calcolo del polinomio minimo

Sia $K \subset F$ un'estensione di Galois con gruppo di Galois $G = \mathrm{Gal}(F/K)$, e sia $\alpha \in F$. Siano $a_1, \ldots, a_r \in F$ gli elementi distinti dell'insieme $\{\varphi(\alpha) \mid \varphi \in G\}$. Allora

$$f = \prod_{i=1}^{r}(x - a_i)$$

è il polinomio minimo di α su K.

<u>*DIMOSTRAZIONE*</u> :

⋮

⋮

⋮

⋮

⋮

⋮

$\vdots$

13.4 Teorema

Sono equivalenti i seguenti enunciati per un'estensione $K \subset F$.

1. $K \subset F$ è un'estensione di Galois.
2. $K \subset F$ è un'estensione finita, normale e separabile.
3. F è campo di riducibilità completa di un polinomio separabile f su K.

<u>*DIMOSTRAZIONE*</u> :

$\vdots$

⋮

13.5 Lemma

Sia $K \subset F$ un'estensione di Galois con $G = \mathrm{Gal}(F/K)$. Se $K \subset L \subset F$ è un campo intermedio, allora anche $L \subset F$ è un'estensione di Galois e per $H = \mathrm{Gal}(F/L)$ si ha $[\,L : K\,] = [\,G : H\,]$, dove $[\,G : H\,]$ è l'indice di H in G, ovvero il numero di laterali di G modulo H.

<u>*DIMOSTRAZIONE*</u> :

⋮

13.6 Teorema Fondamentale della Teoria di Galois

Sia $K \subset F$ un'estensione di Galois con $G = \mathrm{Gal}(F/K)$. Siano inoltre
$\mathcal{L}$ l'insieme di tutti i campi intermedi $K \subset L \subset F$ e
$\mathcal{H}$ l'insieme di tutti i sottogruppi $H \leq G$.
Le applicazioni

$$\mathrm{Gal} : \mathcal{L} \to \mathcal{H},\ L \mapsto \mathrm{Gal}(F/L)$$

$$\mathrm{Fix} : \mathcal{H} \to \mathcal{L},\ H \mapsto \mathrm{Fix}_F(H)$$

definiscono corrispondenze biunivoche reciprocamente inverse tra $\mathcal{L}$ e $\mathcal{H}$ che invertono l'ordine dato dall'inclusione. Inoltre, per ogni campo intermedio $K \subset L \subset F$ si ha

(a) $L \subset F$ è un'estensione di Galois.

(b) Se $H = \mathrm{Gal}(F/L)$, allora $[\,L : K\,] = [\,G : H\,]$, e i seguenti enunciati sono equivalenti:

  (c) $K \subset L$ è un'estensione di Galois.

  (a) H è un sottogruppo normale di G.

  (b) $\varphi(L) \subset L$ per ogni $\varphi \in G$.

  Se valgono (a) - (c), allora $\mathrm{Gal}(L/K) \cong G/H$.

<u>*DIMOSTRAZIONE*</u> :

⋮

⋮

⋮

13.7 Esempio

Siano p, q due primi distinti. Sappiamo per l'Esercizio 20 che $F = \mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\alpha)$ con $\alpha = \sqrt{p} + \sqrt{q}$ è un'estensione di Galois di grado 4 con $\mathrm{Aut}F = \mathrm{Gal}(F/\mathbb{Q}) = \{\mathrm{id}, \varphi_1, \varphi_2, \varphi_3\}$ isomorfo al gruppo di Klein.
Abbiamo
$\varphi_1(\sqrt{p}) = -\sqrt{p}$ e $\varphi_1 \mid_{\mathbb{Q}(\sqrt{q})} = \mathrm{id}$,
$\varphi_2(\sqrt{q}) = -\sqrt{q}$ e $\varphi_2 \mid_{\mathbb{Q}(\sqrt{p})} = \mathrm{id}$, e
$\varphi_3(\sqrt{p}) = -\sqrt{p}$ e $\varphi_3(\sqrt{q}) = -\sqrt{q}$.
$\mathrm{Aut}F$ ha esattamente tre sottogruppi non banali

$$H_i = < \varphi_i >, \; i = 1, 2, 3.$$

Questi sottogruppi corrispondono per 13.6 a tre campi intermedi $L_i = \mathrm{Fix}_F(H_i)$, che sono precisamente

$$L_1 = \mathbb{Q}(\sqrt{q}), \; L_2 = \mathbb{Q}(\sqrt{p}), \; L_3 = \mathbb{Q}(\sqrt{pq})$$

e $L_i \subset F$ sono estensioni di Galois di grado $[\, G : H_i \,] = 2$.
Possiamo usare 13.3 per calcolare i polinomi minimi di α su L_i.
Per $i = 1$ si ha $x^2 - 2\sqrt{q}\, x + q - p$,
per $i = 2$ si ha $x^2 - 2\sqrt{p}\, x + p - q$,
per $i = 3$ si ha $x^2 - (p + q + 2\sqrt{pq})$.

Si noti che $\mathrm{Aut}F$ è un gruppo abeliano, quindi gli H_i sono suoi sottogruppi normali e pertanto $\mathbb{Q} \subset \mathbb{Q}(\sqrt{p})$, $\mathbb{Q} \subset \mathbb{Q}(\sqrt{q})$, $\mathbb{Q} \subset \mathbb{Q}(\sqrt{pq})$ sono estensioni di Galois.

Parte VI

<u>APPLICAZIONI DELLA TEORIA DI GALOIS</u>

14 Campi finiti

14.1 Lemma

Sia F un campo finito. Allora esistono un numero primo p e un numero naturale $n \in \mathbb{N}$ tali che F possiede p^n elementi e $x^{p^n} = x$ per ogni $x \in F$.

<u>*DIMOSTRAZIONE*</u>

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

14.2 Teorema di classificazione dei campi finiti

1. Per ogni numero primo p e ogni $n \in \mathbb{N}$ esiste un campo F di p^n elementi.

   $F = GF(p^n)$ è detto *campo di Galois* di ordine p^n e si ottiene come campo di riducibilità completa del polinomio $f = x^{p^n} - x$ su $\mathbb{Z}/p\mathbb{Z}$.

2. Ogni campo finito è isomorfo a un campo di Galois $GF(p^n)$.

<u>*DIMOSTRAZIONE*</u>

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

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

14.3 Lemma

Ogni sottogruppo finito del gruppo moltiplicativo $(F \setminus \{0\}, \cdot)$ di un campo F è ciclico.

DIMOSTRAZIONE

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

14.4 Teorema dell'elemento primitivo

Per ogni estensione finita e separabile $K \subset F$ esiste $\alpha \in F$ tale che

$$F = K(\alpha)$$

In particolare, per ogni campo finito $F = GF(p^n)$ esiste $\alpha \in F$ tale che

$$F = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{p^n-2}\}$$

DIMOSTRAZIONE
Per il caso in cui K è un campo infinito si veda l'Esercizio 28.
Il caso in cui K è un campo finito:

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

15 Risolubilità per radicali

Motivazione

Gli zeri di un polinomio

$$f = x^2 + a_1\,x + a_0$$

di grado 2 su $\mathbb{Q}$ si determinano con una formula

$$\alpha_1 = -\frac{a_1}{2} + \sqrt{\frac{{a_1}^2}{4} - a_0}$$

$$\alpha_2 = -\frac{a_1}{2} - \sqrt{\frac{{a_1}^2}{4} - a_0}$$

in cui intervengono solo le quattro operazioni e radici quadrate.
Formule analoghe, anche se più complicate, si hanno per i polinomi di grado 3 e 4.
Vedremo però che ciò non vale per i polinomi di grado $n \geq 5$ (Teorema di Abel e Ruffini, 1826).

15.1 Lemma e Definizione

Siano $n \in \mathbb{N}$ e K un campo la cui caratteristica non divide n. Sia inoltre K_n il campo di riducibilità completa di $f = x^n - 1$ su K. Gli zeri di f si chiamano *radici n-sime dell'unità* e formano un sottogruppo ciclico $E_n(K)$ di $(K_n \setminus \{0\},\,\cdot)$ di ordine n.

DIMOSTRAZIONE

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

$\vdots$

15.2 Lemma e Definizione

Siano $n \in \mathbb{N}$ e K un campo la cui caratteristica non divide n. Sia inoltre $a \in K \setminus \{0\}$ e sia F il campo di riducibilità completa di $f = x^n - a$ su K. Gli zeri di f si chiamano *radici n-sime di a*.
Sia α una radice n-sima di a. Allora

1. F contiene $E_n(K) = \{z_0 = 1,\, z_1,\, \ldots,\, z_{n-1}\}$ e quindi un campo di riducibilità completa K_n di $x^n - 1$ su K.

2. $\{\alpha,\, z_1\,\alpha,\, \ldots, z_{n-1}\,\alpha\}$ è l'insieme delle radici n-sime di a.

3. $F = K_n(\alpha)$ e $K \subset F$ è un'estensone di Galois.

4. Se $E_n(K) \subset K$, allora $F = K(\alpha)$ e $\mathrm{Gal}(F/K)$ è un gruppo ciclico.

DIMOSTRAZIONE

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

15.3 Lemma e Definizione

Siano $n \in \mathbb{N}, n > 1$, e sia K un campo la cui caratteristica non divide n.
(1) Le radici n-sime dell'unità che generano il gruppo ciclico $E_n(K)$ si chiamano *radici primitive.* Se z è una radice primitiva, allora $E_n(K) = \{z^m \mid m = 0, 1, \ldots, n-1\}$, e un elemento di forma z^m con $0 < m < n$ è una radice primitiva se e solo se m e n sono coprimi.
(2) $K \subset K_n$ è un'estensione di Galois il cui gruppo di Galois $\mathrm{Gal}(K_n/K)$ è isomorfo a un sottogruppo del gruppo moltiplicativo $(\mathbb{Z}/n\mathbb{Z}^*, \cdot)$ ed è in particolare un gruppo abeliano.

DIMOSTRAZIONE

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

15.4 Osservazione

Possiamo assumere senza perdita di generalità che K è un campo la cui caratteristica non divide n. Infatti se K è un campo la cui caratteristica p divide n, allora possiamo scrivere $n = p^\alpha m$, dove $\alpha \in \mathbb{N}$ e p non divide m. Poiché $x^n - 1 = (x^m - 1)^{p^\alpha}$, dove $x^m - 1$ è un polinomio separabile su K, vediamo che $E_n(K) = E_m(K)$ è un gruppo ciclico di ordine m.

Da ora in avanti supponiamo per semplicità che K sia un campo di caratteristica 0
(ma gli enunciati che seguono valgono in qualsiasi caratteristica!)

15.5 Definizione

Un'estensione di campi $K \subset F$ è detta *estensione per radicali* se esiste una catena di campi intermedi

$$K = L_0 \subset L_1 \subset L_2 \subset \ldots L_n = F$$

tali che ogni L_i è 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}.

15.6 Osservazioni

(1) Nella definizione 15.5 possiamo assumere senza perdita di generalità che $K \subset F$ sia anche un'estensione di Galois.

$\vdots$

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

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

formano una catena finita di sottogruppi

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

Inoltre, se $L_i = L_{i-1}(\alpha_i)$ dove α_i è una radice n_i-sima di un elemento di L_{i-1} e L_{i-1} contiene tutte le radici n_i-sime ell'unità, allora segue da 15.2 che H_i è un sottogruppo normale di H_{i-1} e il gruppo quoziente $H_{i-1}/H_i \cong \mathrm{Gal}(L_i/L_{i-1})$ è ciclico (e quindi abeliano).

$\vdots$

15.7 Definizione

Un gruppo G si dice *risolubile* se esiste una catena finita di sottogruppi

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

con le proprietà

1. N_i è sottogruppo normale di N_{i-1},
2. il gruppo quoziente N_{i-1}/N_i è abeliano.

15.8 Definizione

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 $\mathrm{Gal}(f/K) = \mathrm{Gal}(F/K)$ dove F è un campo di riducibilità completa di f su K.

15.9 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. $\mathrm{Gal}(f/K)$ è un gruppo risolubile.

DIMOSTRAZIONE
(1) $\Rightarrow$ (2) : Per 15.6 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

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

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}.

Per (i) sappiamo che F contiene un campo di riducibilità completa L di f su K. Poiché K è un campo perfetto ($\mathrm{char}K = 0$), 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

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

per il Teorema Fondamentale 13.6, e quindi basta verificare che $\mathrm{Gal}(F/K)$ è risolubile, vedi 16.5.

Procediamo per induzione su m.
$m = 0$: in questo caso $F = K$, quindi $\mathrm{Gal}(F/K) = \{\mathrm{id}\}$ è risolubile.
$m \to m + 1$: 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 15.6(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) Si dimostra che $K \subset F$, $K \subset K'$, $F \subset F'$ e $K' \subset F'$ sono tutte estensioni di Galois.
⋮
⋮
⋮
⋮
⋮
⋮
⋮

(b) Considerando il campo intermedio $K \subset F \subset F'$, deduciamo da (a) con 13.6 che

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

quindi sempre per 16.5 basta dimostrare che

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

è risolubile.
(c) Dalla catena di campi intermedi

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

si ottiene una catena di campi intermedi

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

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

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

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 $\mathrm{Gal}(L/K')$ ciclico (vedi 15.2),
• $K \subset K' = K_n$ è un'estensione di Galois con gruppo di Galois $\mathrm{Gal}(K'/K)$ abeliano (vedi 15.3).
(d) Applicando il Teorema Fondamentale 13.6 a

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

si ottiene che

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

ha un quoziente $G'/H \cong \mathrm{Gal}(L/K')$ ciclico e pertanto risolubile. Poiché anche H è risolubile, deduciamo da 16.5 che G' è risolubile. Applicando il Teorema Fondamentale 13.6 a

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

vediamo che $G/G' \cong \mathrm{Gal}(K'/K)$ è abeliano e pertanto risolubile, e per 16.5 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 ($\mathrm{char} K = 0$), il polinomio f è separabile e quindi $K \subset L$ è un'estensione di Galois. Per ipotesi $G = \mathrm{Gal}(L/K)$ è risolubile.
(a) Si dimostra che la catena di sottogruppi normali di G con quozienti abeliani

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

può essere scelta tale che ogni quoziente N_{i-1}/N_i sia addirittura ciclico di ordine primo p_i.
(b) Ponendo $L_i = \mathrm{Fix}_L(N_i)$ si ottiene una catena di campi intermedi

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

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 13.6 che anche ogni $L_{i-1} \subset L_i$ è un'estensione di Galois il cui gruppo di Galois $\mathrm{Gal}(L_i/L_{i-1}) \cong N_{i-1}/N_i$ è ciclico di ordine primo p_i.
(c) Si dimostra che ogni estensione di Galois $L'' \subset L'$ il cui gruppo di Galois $\mathrm{Gal}(L''/L')$ 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. $\square$

16 Gruppi risolubili

16.1 Esempi

(1) Ogni gruppo abeliano è risolubile: si scelga $\{e\} \leq G$.

(2) S_3 è risolubile:

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

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:

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

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.

16.2 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

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

ed è detto *sottogruppo commutatore* di G.
Per iterazione definiamo

$$K^2(G) = K(K(G))$$
$$K^{i+1}(G) = K(K^i(G))$$

16.3 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 $f : G \to G'$ e per ogni $n \in \mathbb{N}$ si ha $f(K^n(G)) \subset K^n(G')$. Se f è suriettivo si ha addirittura $f(K^n(G)) = K^n(G')$.
3. $K^n(G)$ è un sottogruppo normale di G per ogni $n \in \mathbb{N}$.
4. $K(G)$ è il più piccolo sottogruppo normale N di G tale che G/N sia abeliano.

<u>DIMOSTRAZIONE</u>
(1) per definizione.
(2) Basta dimostrare l'enunciato per n=1. Un elemento di K(G) è di forma

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

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 $f : G \to G$, $x \mapsto axa^{-1}$ abbiamo $a\,K^n(G)\,a^{-1} = f(K^n(G)) = K^n(G)$ per (2), quindi $K^n(G)$ è un sottogruppo normale di G.
(4) $G/K(G)$ è abeliano: poichè $ab(ba)^{-1} = [a, b] \in K(G)$ si ha $aK(G)\,bK(G) = bK(G)\,aK(G)$ per tutti gli elementi $a, b \in G$. Se inoltre N è un sottogruppo normale tale che G/N sia abeliano, allora per tutti gli elementi $a, b \in G$ abbiamo $aN\,bN = b\,NaN$ in G/N, ovvero $[a, b] = ab(ba)^{-1} \in N$, che dimostra $K(G) \subset N$.

16.4 Teorema

Un gruppo G è risolubile se e solo se esiste un $n \in \mathbb{N}_0$ tale che $K^nG = \{e\}$.

DIMOSTRAZIONE
$\Leftarrow$: Per 16.3 (3) e (4)

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

è una catena di sottogruppi normali con quozienti abeliani.
$\Rightarrow$: Sia

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

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 $K(G) = \{e\}$.
$n \to n + 1$: 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 16.3 (2) all'omomorfismo $\nu : G \to G/N_1$ vediamo che $\nu(K(G)) = \{e_{G/N_1}\}$, quindi $K(G) \subset \operatorname{Ker}\nu = N_1$ e perciò $K^{m+1}(G) \subset K^m(N_1) = \{e\}$.

16.5 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 16.3 (2) all'immersione $H \hookrightarrow G$ e all'epimorfismo canonico $\nu : G \to G/N$ 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 16.4 per concludere che G è risolubile.

16.6 Corollario

Per $n \geq 5$ il gruppo S_n non è risolubile.

DIMOSTRAZIONE

(i) Verifichiamo che se N è un sottogruppo normale di S_n che contiene tutti i 3-cicli, anche $K(N)$ contiene tutti i 3-cicli: infatti N deve contenere $a = (123)$ e $b = (145)$ (stiamo usando $n \geq 5$), quindi $K(N)$ contiene $[a, b] = (123)\,(145)\,(321)\,(541) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \ldots & n \\ 2 & 4 & 3 & 1 & 5 & \ldots & n \end{pmatrix} = (124)$. Inoltre, 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 $x, y, z \in \{1, \ldots, n\}$ 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 Esercizio 19 (a).
(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 $K^3(G)$,..., anche $K^n(G)$ per qualsiasi $n \in N$. Da 16.4 segue che G non è risolubile.

17 Risolubilità del polinomio generale di grado n

Sia K un campo di *caratteristica* 0.

17.1 Proposizione

Se $f \in K[x]$ un polinomio di grado $n > 0$, allora $\mathrm{Gal}(f/K)$ è isomorfo a un sottogruppo di S_n.

DIMOSTRAZIONE

$\vdots$

17.2 Teorema

Per qualsiasi polinomio non costante $f \in K[x]$ di grado ≤ 4 l'equazione $f(x) = 0$ è risolubile per radicali.

DIMOSTRAZIONE

$\vdots$

17.3 Esempi

(1) Il polinomio $f = x^5 - 1 \in \mathbb{Q}[x]$ è risolubile per radicali, poiché $\mathrm{Gal}(f/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}_5/\mathbb{Q})$ è abeliano e quindi risolubile, vedi 15.3.

(2) Il polinomio $f = x^5 - 10x^4 + 27x^3 - 18x^2 + 30x + 50 = (x-5)^2(x^3 + 2x + 2)$ è risolubile per radicali, poiché $\mathrm{Gal}(f/\mathbb{Q}) = \mathrm{Gal}(x^3 + 2x + 2/\mathbb{Q})$ è isomorfo a un sottogruppo di S_3 ed è pertanto risolubile.

(3) Il polinomio $f = x^5 - 4x + 2 \in \mathbb{Q}[x]$ non è risolubile per radicali. Per verificarlo notiamo che f è irriducibile su $\mathbb{Q}$ con tre zeri reali e due zeri coniugati complessi $\alpha, \overline{\alpha}$ (si usi che f ha un massimo in $-\sqrt[4]{\frac{4}{5}}$ e un minimo in $\sqrt[4]{\frac{4}{5}}$). Vediamo dunque che il campo di riducibilità completa E di f su $\mathbb{Q}$ contiene un campo intermedio $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset E$ con $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$, e l'ordine di $G = \mathrm{Gal}(f/\mathbb{Q})$ è pertanto un multiplo di 5. Quindi G contiene un elemento di ordine 5 (per un risultato noto come Teorema di Cauchy). Inoltre G contiene anche la trasposizione $\tau \in G$ data dalla coniugazione di numeri complessi, che è un elemento di ordine 2. Poiché si dimostra che ogni sottogruppo di S_5 che contenga un elemento di ordine 5 e un elemento di ordine 2 deve coincidere con S_5, concludiamo dunque che $G \cong S_5$ non è risolubile.

17.4 Definizione

(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:

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

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

17.5 Esempio

Sia $n = 2$, quindi $R = K[x, y]$, $\quad F = K(x, y)$, e $S_2 = \{\mathrm{id},\, (12)\}$.
Per $\sigma = (12) \in S_2$ si ha $\hat{\sigma}(\frac{x+2y}{x+y}) = \frac{y+2x}{x+y}$, quindi $\frac{x+2y}{x+y} \notin \mathrm{Fix}_F(S_2)$, mentre $\hat{\sigma}(\frac{xy}{x+y}) = \frac{xy}{x+y}$, quindi $\frac{xy}{x+y} \in \mathrm{Fix}_F(S_2)$.

17.6 Definizione

I seguenti polinomi in R

$$s_0 = 1$$

$$s_1 = x_1 + \ldots + x_n$$

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

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

$$\vdots$$

$$s_n = x_1 \ldots x_n$$

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

17.7 Proposizione

Consideriamo il polinomio

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

Allora

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

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

17.8 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

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

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

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

17.9 Il 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 $G = \mathrm{Gal}(f/K) = \mathrm{Gal}(E/K)$ 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 $\alpha_1, \ldots, \alpha_n$. Identifichiamo quindi G con un sottogruppo di S_n, vedi 17.1.
Poniamo

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

e chiamiamo *discriminante* di f l'elemento

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

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 $\{\alpha_1, \alpha_2\} = \{\frac{-p+\delta}{2}, \frac{-p-\delta}{2}\}$.
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 $x - \frac{1}{3}a_2 \ldots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
$\vdots$
(2) $\Delta = -4p^3 - 27q^2$
Infatti $\delta = -\det\begin{pmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{pmatrix}$, 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 $i = 1, 2, 3$).

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 $G = \mathrm{Gal}(g/K) \cong \mathbb{Z}/2\mathbb{Z}$.
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* (Esercizio 32):
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

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

(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 33).

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 $x - \frac{1}{4}a_3 \ldots$

⋮
⋮
⋮
⋮

(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

$$u_1 u_2 u_3 = -q$$

si ha

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

18 Costruzioni con riga e compasso

18.1 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 in 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 $M = \{0, 1\}$.

18.2 Esempi

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

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

(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.

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

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

18.3 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

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

18.4 Lemma

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

<u>*DIMOSTRAZIONE*</u>

$\vdots$

18.5 Teorema.

Sono equivalenti i seguenti enunciati per $a \in \mathbb{C}$.

1. $a \in \mathbb{K}$.
2. Esiste una catena finita di campi intermedi
$$\mathbb{Q} = L_0 \subset L_1 \subset \ldots \subset L_m \subset \mathbb{C}$$
tali che
$$[L_{i+1} : L_i] = 2 \quad \text{e} \quad a \in L_m.$$
3. a è un elemento algebrico su $\mathbb{Q}$ e per il polinomio minimo f di a su $\mathbb{Q}$ esiste $m \in \mathbb{N}$ tale che
$$\mid \mathrm{Gal}(f/\mathbb{Q}) \mid = 2^m.$$

In particolare, se $a \in \mathbb{C}$ è costruibile, allora $[\mathbb{Q}(a) : \mathbb{Q}]$ è una potenza di 2.

<u>*DIMOSTRAZIONE*</u>

$\vdots$

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

18.6 Corollario (costruzioni impossibili).

(1) La quadratura del cerchio è impossibile: non esiste un quadrato il cui lato $a \in \mathbb{K}$ sia costruibile e la cui area coincida con l'area del cerchio di centro 0 e raggio 1.
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 9.6 e 18.5.

(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 18.5.

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

$\vdots$
$\vdots$

Quindi $[\mathbb{Q}(z) : \mathbb{Q}] = \deg \Phi_9 = 6$ non sarebbe una potenza di 2, contraddicendo 18.5.

18.7 Costruzione del poligono regolare.

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

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

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 4.4.

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

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

Inoltre si dimostra che nel Lemma 15.3(2) con $K = \mathbb{Q}$ si ha addirittura $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong \mathbb{Z}/n\mathbb{Z}^*$.
Quindi $[\mathbb{Q}(z) : \mathbb{Q}] = \varphi(n)$ e pertanto il Teorema è un'applicazione di 18.5. $\square$

19 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