Appunti del corso di Elementi di Algebra e Teoria di Galois

Lorenzo Molena

Lezioni dal 07/03/2023 al 25/05/2023

Indice

Parte I.

Gruppi

1. Richiamo sui gruppi

1.1. Definizione

Un gruppo $(G, \cdot)$ è costituito da un insieme non-vuoto G e un'operazione
$\cdot : G \times G \to G$, $(a, b) \mapsto a \cdot b = ab$, che gode delle seguenti proprietà:

(G1) **associativa**: $a(bc) = (ab)c$ per $a, b, c \in G$

(G2) **elemento neutro**: esiste un $e = e_G \in G$ tale che
$ae = ea = a$ per ogni $a \in G$

(G3) **elementi inversi**: per ogni $a \in G$ esiste un $b \in G$ tale che $ab = ba = e$

G è un gruppo *abeliano* se vale inoltre la proprietà:

(G4) **commutatività**: $ab = ba$ per $a, b \in G$

1.2. Osservazioni

1. L'elemento neutro e è univocamente determinato :
   se e, e' soddisfano $(G2)$, allora
   $e = ee' = e'$.
   L'elemento inverso di $a \in G$ è univocamente determinato e si indica con a^{-1}

2. Per $a, b \in G$ si ha $(ab)^{-1} = b^{-1}a^{-1}$

3. **proprietà cancellativa**: se $a, x, y \in G$ e soddisfano $ax = ay$, allora $x = y$

4. Si usa anche la notazione additiva $(G, +)$.
   In tal caso l'elemento neutro si indica con 0_G e l'inverso con $-a$

Esempi

1. $(\mathbb{Z},+)$, $(\mathbb{R},+)$, $(\mathbb{Q},+)$, $(\mathbb{R}\setminus\{0\},\cdot)$, $(\mathbb{Q}\setminus\{0\},\cdot)$ sono gruppi abeliani.
   $\mathrm{Gl}(n,K):$ le matrici invertibili su campo K di ordine $n\in\mathbb{N}$ formano un gruppo rispetto alla moltiplicazione di matrici, che non è abeliano per $n\geq 2$.

2. Dati $n\in\mathbb{N}$ e due interi $z,z'\in\mathbb{Z}$, si ha che $n\mid z-z'$ se e solo se z e z' hanno lo stesso resto della divisione per n.
   Per $0\leq r<n$ chiamiamo *classe di resto* modulo n, l'insieme
   $$\begin{aligned}\overline{r} &:= \{z\in\mathbb{Z}\mid \text{il resto della divisione di } z \text{ per } n \text{ è } r\}\\ &= \{nq+r\mid q\in\mathbb{Z}\}\end{aligned}$$
   Abbiamo che $n\mid z-z'$ se e solo se z e z' appartengono alla stessa classe di resto.
   Le classi di resto $\overline{0}$, $\overline{1}$, …, $\overline{n-1}$ formano un gruppo abeliano $(\mathbb{Z}/n\mathbb{Z},+)$ rispetto all'operazione $\overline{a}+\overline{b}:=\overline{a+b}$

3. Sia A un insieme non-vuoto. Le applicazioni *biiettive* $f:A\to A$ formano un gruppo $(\mathrm{S}(A),\circ)$ rispetto alla composizione, detto *gruppo simmetrico* su A.
   In particolare per $A=\{1,\dots,n\}$ si ha $S_n:=\mathrm{S}(A)$ il gruppo simmetrico delle permutazioni di n elementi.
   Per $n=3$
   $$S_3=\{\mathrm{id},\begin{pmatrix}1&2\end{pmatrix},\begin{pmatrix}1&3\end{pmatrix},\begin{pmatrix}2&3\end{pmatrix},\begin{pmatrix}1&2&3\end{pmatrix},\begin{pmatrix}1&3&2\end{pmatrix}\}$$
   non è abeliano:
   $$\begin{pmatrix}1&2\end{pmatrix}\begin{pmatrix}1&3\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\begin{pmatrix}1&3&2\end{pmatrix}$$
   $$\begin{pmatrix}1&3\end{pmatrix}\begin{pmatrix}1&2\end{pmatrix}=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\end{pmatrix}$$

1.3. Sottogruppi

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

Osservazione

$H \leq G$ se e solo se per tutti gli $a, b \in H$ si ha $ab^{-1} \in H$.

1.4. Esempi

1. Ogni gruppo $(G, \cdot)$ possiede i sottogruppi banali G, $\{e\}$
2. I numeri dispari **non** formano un sottogruppo di $(\mathbb{Z}, +)$
3. Dato un gruppo $(G, \cdot)$ e un elemento $a \in G$, poniamo per $n \in \mathbb{Z}$

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

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

$$a^n \cdot (a^m)^{-1} = a^n \cdot a^{-m} = a^{n-m} \in \langle a \rangle$$

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

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

   Tutti i sottogruppi di $(\mathbb{Z}, +)$ hanno questa forma:
   Sia $H \leq (\mathbb{Z}, +)$, se $H = 0$, allora $H = 0\mathbb{Z}$, altrimenti esiste un $0 \neq m \in H$. Possiamo assumere $m > 0$.
   Sia $n > 0$ il minimo intero positivo in H. Allora $H = n\mathbb{Z}$:
   Ovviamente $n\mathbb{Z} \subset H$.
   Sia adesso $a \in H$.
   Eseguiamo la divisione con resto:

$$a = nq + r \text{ con } q \in \mathbb{Z},\ 0 \leq r < n.$$

   Abbiamo $r = \underset{\substack{\cap \\ H}}{a} - \underset{\substack{\cap \\ H}}{nq} \in H$ e per la minimalità di n, si ha che $r = 0$ e $a \in n\mathbb{Z}$.

$\square$

1.5. Definizione

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

Esempio

$\mathbb{Z} = \langle 1 \rangle$, $\mathbb{Z}/n\mathbb{Z} = \langle \overline{1} \rangle$

1.6. Definizione

Dati due gruppi $(G, \cdot)$ e $(G', *)$, un'applicazione $f : G \to G'$ è detta

- **omomorfismo** se $f(a \cdot b) = f(a) * f(b)$
- **isomorfismo** se è un omomorfismo biiettivo.

Diciamo che G e G' sono *isomorfi* e scriviamo $G \cong G'$ se esiste un isomorfismo $f : G \to G'$.

1.7. Classificazione dei gruppi ciclici

Sia $(G, \cdot)$ un gruppo ciclico.
Se $|G| = \infty$, allora $(G, \cdot) \cong (\mathbb{Z}, +)$.
Se $|G| = n$, allora $(G, \cdot) \cong (\mathbb{Z}/n\mathbb{Z}, +)$

1.8. Esempio

L'insieme $\mathcal{V} = \{\mathrm{id}, \begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}, \begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}2 & 4\end{pmatrix}, \begin{pmatrix}1 & 4\end{pmatrix}\begin{pmatrix}2 & 3\end{pmatrix}\} \subset S_4$ è un sottogruppo di S_4 , detto *gruppo di Klein*.
I suoi elementi hanno tutti ordine ≤ 2.
Quindi $\mathcal{V}$ è abeliano, ma non ciclico.

Richiamo sull'ordine

L'ordine di un elemento $a \in G$ è $\mathrm{ord}(a) := |\langle a \rangle|$, ovvero $\mathrm{ord}(a) = \infty$ oppure è il minimo intero positivo m tale che $a^m = e$.

Lemma

Un gruppo G i cui elementi hanno tutti ordine ≤ 2 è sempre abeliano.

Dimostrazione.
In G si ha $a^2 = e$ per ogni $a \in G$.
Ma allora per $a, b \in G$ si ha $e = a^2 = b^2 = (ab)^2$, in particolare $a^2 = baba$ e per la proprietà cancellativa $a = bab$, quindi $ab^2 = bab$ e perciò $ab = ba$.

$\square$

Tornando all'esempio $\mathcal{V} \leq S_4$ vediamo che:

$$\left(\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}\right)^2 = \begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix} = \begin{pmatrix}1 & 2\end{pmatrix}^2\begin{pmatrix}3 & 4\end{pmatrix}^2 = \mathrm{id}$$

e analogamente per gli altri elementi.
Per il Lemma $\mathcal{V}$ è abeliano.
$\mathcal{V}$ non è ciclico perché non possiede elementi di ordine 4.

2. Laterali

Le classi di resto $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ di $\mathbb{Z}$ modulo n sono disgiunte a due a due e $\mathbb{Z} = \overline{0} \,\dot\cup\, \overline{1} \,\dot\cup\, \ldots \,\dot\cup\, \overline{n-1}$.

2.1. Richiamo sulle partizioni di un insieme

Sia A un insieme con una relazione di equivalenza $\sim$ (cioè $\sim$ è riflessiva, simmetrica e transitiva).
Per $a, b \in A$ si ha

$$a \sim b \Leftrightarrow \overline{a} = \overline{b} \Leftrightarrow \overline{a} \cap \overline{b} \neq \varnothing$$

dove $\overline{a} = \{x \in A \mid x \sim a\}$ indica la classe di equivalenza di a modulo $\sim$.
In particolare $\sim$ induce una partizione su A :
l'insieme A è unione di classi di equivalenza disgiunte a due a due.

2.2. Lemma e definizione

Ogni sottogruppo H di un gruppo $G, \cdot$ definisce una relazione di equivalenza su G

$$a \sim b \text{ se } ab^{-1} \in H$$

Le classi di equivalenza di G modulo $\sim$

$$\overline{a} = \{x \in G \mid xa^{-1}\} = \{ha \mid h \in H\} = Ha$$

si chiamano *laterali* (destri) di G modulo H (con rappresentante a). L'insieme di tutti i laterali si indica con

$$G/H = \{\overline{a} \mid a \in G\}$$

L'ordine di G/H, cioè il numero di laterali di G modulo H, è detto *indice* di H in G e si indica con

$$[G : H] = |G/H|$$

Dimostrazione.
$\sim$ relazione di equivalenza:
riflessiva: $a \sim a$ perché $aa^{-1} = e \in H$.
simmetrica: se $a \sim b$, allora $ab^{-1} \in H$, perciò $ba^{-1} = (ab^{-1})^{-1} \in H$ e $b \sim a$.
transitiva: se $a \sim b$ e $b \sim c$, allora $ab^{-1}, bc^{-1} \in H$, perciò $ac^{-1} = ab^{-1}bc^{-1} \in H$ e $a \sim c$.

Il laterale destro di $a \in G$ è

$$\overline{a} = \{x \in G \mid x \sim a\} = \{x \in G \mid xa^{-1} \in H\}$$

dunque

$$x \in \overline{a} \Leftrightarrow x = \underbrace{xa^{-1}}_{\substack{\cap \\ H}} a \text{ è di forma } x = ha \text{ con } h \in H$$

Perciò $\overline{a} = \{ha \mid h \in H\} = Ha$.

$\square$

Esempio

$G = (\mathbb{Z}, +)$, $H \leq G$, allora $H = n\mathbb{Z}$ con $n \in \mathbb{Z}$ e per $a, b \in \mathbb{Z}$ si ha:

$$\begin{aligned} a \sim b &\Leftrightarrow a - b \in H = n\mathbb{Z} \\ &\Leftrightarrow n \mid a - b \\ &\Leftrightarrow a \text{ e } b \text{ appartengono alla stessa classe di resto modulo } n. \end{aligned}$$

I laterali di $\mathbb{Z}$ modulo $H = n\mathbb{Z}$ sono esattamente le classi di resto $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ di $\mathbb{Z}$ modulo n.

2.3. Teorema di Lagrange

Sia $(G, \cdot)$ un gruppo finito e sia $H \leq G$, allora $|G| = |H| \cdot [G : H]$.
In particolare $|H|$ divide $|G|$.

Dimostrazione.
Poniamo $n := |G|$, $m := |H| \leq n$.

$$H = \{h_1, \ldots, h_m\}$$

Ogni laterale $\overline{a} = \{h_1 a, \ldots, h_m a\}$ possiede esattamente m elementi (proprietà cancellativa).
Per il Lemma 2.2, i laterali danno luogo ad una partizione di G, quindi il numero dei laterali è finito. Poniamo $r := [G : H]$.

$$G/H = \{\overline{a_1}, \ldots, \overline{a_r}\}$$

Abbiamo quindi

$$G = \dot{\bigcup_{i=1}^{r}} \overline{a_i}$$

e perciò

$$|G| = \sum_{i=1}^{r} |\overline{a_i}| = m \cdot r = |H| \cdot [G : H]$$

$\square$

Corollario

Se G è un gruppo di orine n e $a \in G$, allora $\text{ord}(a)$ divide n e $a^n = e$.

Dimostrazione.
$m := \text{ord}(a) = |\langle a \rangle|$ divide $|G|$ per il Teorema di Lagrange ed è il minimo intero positivo tale che $a^m = e$.
Scriviamo $n = mq$ con $q \in \mathbb{Z}$ e otteniamo $a^n = a^{mq} = (a^m)^q = e^q = e$

$\square$

3. Il gruppo quoziente

Siano $(G, \cdot)$ un gruppo e $H \leq G$.
Vogliamo definire un'operazione su G/H tale che

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

ovvero

$$Ha \cdot Hb = Hab$$

Affinché l'operazione sia ben definita, dobbiamo garantire:

$$\text{Se } \overline{a} = \overline{a'} \text{ e } \overline{b} = \overline{b'}, \text{ allora } \overline{ab} = \overline{a'b'}.$$

Ciò significa:

$$\text{Se } aa'^{-1} \in H \text{ e } bb'^{-1} \in H, \text{ allora } (ab)(a'b')^{-1} \in H.$$

In generale

$$(ab)(a'b')^{-1} = abb'^{-1}a'^{-1} = a\underbrace{bb'^{-1}}_{\substack{\cap \\ H}}a^{-1}\underbrace{aa'^{-1}}_{\substack{\cap \\ H}}$$

Quindi serve la condizione seguente:

3.1. Definizione

Un sottogruppo H di un gruppo $(G, \cdot)$ si dice **normale**, e in tal caso si scrive $H \lhd G$, se per ogni $a \in G$ si ha

$$aha^{-1} \in H$$

Osservazione

$H \lhd G$ se e solo se $Ha = aH$ per ogni $a \in G$.
Infatti se $H \lhd G$, allora $Ha \subset aH$ poiché

$$ha = a\underbrace{a^{-1}ha}_{\substack{\cap \\ H}} \in aH$$

Analogamente le altre implicazioni.

Esempi

1. Ogni sottogruppo di un gruppo abeliano è normale
2. In S_3 il sottogruppo $H = \langle\begin{pmatrix}1 & 2\end{pmatrix}\rangle = \{\mathrm{id}, \begin{pmatrix}12\end{pmatrix}\}$ **non** è normale:

$$\begin{aligned}\begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}1 & 3\end{pmatrix}^{-1} &= \begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}1 & 3\end{pmatrix}\\ &= \begin{pmatrix}13\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}\\ &= \begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}1 & 3 & 2\end{pmatrix}\\ &= \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix} = \begin{pmatrix}2 & 3\end{pmatrix} \notin H\end{aligned}$$

3.2. Lemma e definizione

Sia $(G, \cdot)$ un gruppo e sia $H \lhd G$.
Allora l'insieme dei laterali G/H è un gruppo rispetto all'operazione

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

con elemento neutro $\overline{e} = H$, detto *gruppo quoziente* di G modulo H.
Per $a \in G$ si ha $\overline{a} = \overline{e}$ se e solo se $a \in H$.

Dimostrazione.
L'operazione è ben definita perché $H \lhd G$.

(G1) Per $\overline{a}, \overline{b}, \overline{c} \in G/H$

$$(\overline{a} \cdot \overline{b})\overline{c} = \overline{ab} \cdot \overline{c} = \overline{(ab)c} = \overline{a(bc)} = \overline{a}(\overline{b} \cdot \overline{c})$$

(G2) Per $\overline{a} \in G/H$

$$\overline{a} \cdot \overline{e} = \overline{ae} = \overline{a} = \overline{e} \cdot \overline{a}$$

(G3) Dato $\overline{a} \in G/H$

$$\overline{a} \cdot \overline{a^{-1}} = \overline{aa^{-1}} = \overline{e} = \overline{a^{-1}} \cdot \overline{a}$$

quindi $\overline{a}^{-1} = \overline{a^{-1}}$

Inoltre $x \in \overline{e}$ se e solo se $x \sim e$, ovvero

$$xe^{-1} = xe = x \in H$$

e ciò equivale a dire che $\overline{x} = \overline{e}$.

□

Esempio

$G = \mathbb{Z}$, $H = n\mathbb{Z}$.
L'elemento neutro di $G/H = (\mathbb{Z}/n\mathbb{Z}, +)$ è $\overline{0} = n\mathbb{Z}$.

3.3. Lemma e definizione

Siano $(G, \cdot)$ e $(G', *)$ due gruppi con un omomorfismo $f : G \to G'$.
Allora

1. $\ker f = \{a \in G \mid f(a) = e\} \lhd G$
   è un sottogruppo normale, detto *nucleo* di f.

2. L'immagine $\operatorname{im} f = \{f(a) \mid a \in G\} \leq G'$
   è un sottogruppo di G'.

3. $e_G \in \ker f$, e l'applicazione f è iniettiva se e solo se $\ker f = \{e_G\}$.

4. Se $H \lhd G$, allora l'applicazione

$$\nu : G \to G/H, a \mapsto \overline{a} = Ha$$

   è un omomorfismo suriettivo con nucleo $\ker \nu = H$, detto **epimorfismo canonico**.

Dimostrazione.

1. $\ker f \leq G$:
   Siano $a, b \in \ker f$. Allora $ab^{-1} \in \ker f$ perché

$$f(ab^{-1}) = f(a) * f(b)^{-1} = e_{G'} * e_{G'} = e_{G'}$$

   Infatti:

   - $f(e_G) = e_{G'}$ poiché

$$f(e_G) * f(a) = f(e_g \cdot a) = f(a) = e_{G'} * f(a)$$

   - Per $b \in G$

$$f(b) * f(b^{-1}) = f(bb^{-1}) = f(e_G) = e_{G'}$$

     quindi $f(b)^{-1} = f(b^{-1})$

$\ker f \lhd G$:
Sia $a \in G$ e $h \in \ker f$.
Allora $aha^{-1} \in \ker f$, perché

$$f(aha^{-1}) = f(a)\underbrace{f(h)}_{=e_{G'}}f(a)^{-1} = f(a)f(a)^{-1} = e_{G'}$$

2. Siano $f(a), f(b) \in \operatorname{im} f$. Allora

$$f(a)f(b)^{-1} = f(ab^{-1}) \in \operatorname{im} f$$

quindi $\operatorname{im} f \leq G'$.

3. Se f è iniettiva e $a \in \ker f$ allora $f(a) = e_{G'} = f(e_G)$, perciò $a = e_G$.
Viceversa se $\ker f = \{e_G\}$ e $a, b \in G$ soddisfano $f(a) = f(b)$, allora

$$e_{G'} = f(a) * f(b)^{-1} = f(ab^{-1})$$

dunque $ab^{-1} \in \ker f$, perciò $ab^{-1} = e_G$, ovvero $a = b$.

4. ν omomorfismo: se $a, b \in G$

$$\nu(ab) = \overline{ab} = \overline{a} \cdot \overline{b} = \nu(a) \cdot \nu(b)$$

ν è suriettivo per definizione.

$$\begin{aligned}\ker \nu &= \{a \in G \mid \nu(a) = e_{G/H}\} \\ &= \{a \in G \mid \overline{a} = \overline{e_G}\} \\ &= \{a \in G \mid a \in H\} = H\end{aligned}$$

□

3.4. Teorema di fattorizzazione di omomorfismi

Sia $(G, \cdot)$ un gruppo e sia $H \leq G$.
Sia inoltre $f : G \to G'$ un omomorfismo di gruppi tale che $H \subseteq \ker f$.
Allora esiste uno e un solo omomorfismo $\overline{f} : G/H \to G'$ tale che $\overline{f} \circ \nu = f$, ovvero il seguente diagramma

$$\begin{tikzcd} G \arrow[r, "\nu"] \arrow[d, "f"'] & G/H \arrow[dl, dashed, "\overline{f}"] \\ G' & \end{tikzcd}$$

è commutativo.
Si ha che $\ker \overline{f} = \ker f/H$ e $\operatorname{im} \overline{f} = \operatorname{im} f$

Dimostrazione.
Se esiste una tale $\overline{f}$, allora deve soddisfare $\overline{f}(\overline{a}) = f(a)$.
Poniamo quindi $\overline{f} : G/H \to G', \overline{a} \mapsto f(a)$.
Ben definita:
Se $\overline{a} = \overline{a'}$, allora $aa'^{-1} \in H$ e quindi

$$f(a)f(a')^{-1} = f(aa'^{-1}) = e_{G'} \text{ perciò } f(a) = f(a')$$

$\overline{f}$ omomorfismo:

$$\overline{f}(\overline{a} \cdot \overline{b}) = \overline{f}(\overline{ab}) = f(ab) = f(a) \cdot f(b) = \overline{f}(\overline{a}) \cdot \overline{f}(\overline{b})$$

$\overline{f} \circ \nu = f$:

$$(\overline{f} \circ \nu)(a) = \overline{f}(\nu(a)) = \overline{f}(\overline{a}) = f(a) \text{ per ogni } a \in G$$

Unicità:
Se $g : G/H \to G'$ soddisfa $g \circ \nu = f$, allora per $\overline{a} \in G/H$ si ha $g(\overline{a}) = g(\nu(a)) = f(a) = \overline{f}(\overline{a})$, quindi $g = \overline{f}$.

$$\begin{aligned} \ker \overline{f} &= \{\overline{a} \in G/H \mid \overline{f}(\overline{a}) = e_{G'}\} \\ &= \{\overline{a} \in G/H \mid f(a) = e_{G'}\} \\ &= \{\overline{a} \in G/H \mid a \in \ker f\} = \ker f/H \end{aligned}$$

(si noti che $H \lhd \ker f$, infatti $H \leq \ker f$ e per $a \in \ker f$, $h \in H$ si ha $aha^{-1} \in H$)

$$\operatorname{im} \overline{f} = \{\overline{f}(\overline{a}) \mid \overline{a} \in G/H\} = \{f(a) \mid a \in G\} = \operatorname{im} f$$

$\square$

3.5. Teorema fondamentale dell'omomorfismo

Sia $f : G \to G'$ un omomorfismo di gruppi.
Allora esiste uno e un solo omomorfismo $\overline{f} : G/\ker f \to G'$, tale che $\overline{f} \circ \nu = f$, ovvero il diagramma

$$\begin{tikzcd} G \arrow[r, "\nu"] \arrow[d, "f"'] & G/\ker f \arrow[dl, dashed, "\overline{f}"] \\ G' & \end{tikzcd}$$

è commutativo.
In particolare $G/\ker f \cong \operatorname{im} f$.

Dimostrazione.
Caso particolare di 3.4 con $H = \ker f$.
In questo caso $\ker \overline{f} = \{e_{G/\ker f}\}$, perciò $\overline{f}$ è iniettiva e induce un isomorfismo $G/\ker f \to \operatorname{im} f$. Perciò $G/\ker f \cong \operatorname{im} f$.

□

4. Gruppi risolubili

4.1. Definizione

Sia G un gruppo. Per $a, b \in G$ poniamo

$$[a, b] := aba^{-1}b^{-1} = (ab)(ba)^{-1}$$

detto il *commutatore* di a e b.
Il sottogruppo $\mathrm{K}(G)$ di G generato da tutti i commutatori $[a, b]$ è detto **sottogruppo commutatore** di G.
(Dato un sottoinsieme $A \subset G$ possiamo sempre considerare l'intersezione di tutti i sottogruppi di G che contengono A, ovvero il più piccolo sottogruppo di G che contiene A, detto il *sottogruppo di G generato da A*).
Per iterazione consideriamo

$$\mathrm{K}^2(G) = \mathrm{K}(\mathrm{K}(G))$$
$$\mathrm{K}^i(G) = \mathrm{K}(\mathrm{K}^{i-1}(G))$$

4.2. Proprietà

Sia G un gruppo.

1. G è abeliano se e solo se $\mathrm{K}(G) = \{e_G\}$

2. Ogni elemento di $\mathrm{K}(G)$ è di forma

$$[a_1, b_1] \cdot \ldots \cdot [a_n, b_n] \text{ con } a_1, \ldots, a_n, b_1, \ldots, b_n \in G$$

3. Se $f : G \to G'$ è un omomorfismo allora $f(\mathrm{K}(G)) \subseteq \mathrm{K}(G')$
   e si ha $f(\mathrm{K}(G)) = \mathrm{K}(G')$ quando f è suriettivo.

4. $\mathrm{K}(G) \lhd G$. Più in generale se $N \lhd G$, allora $\mathrm{K}(N) \lhd G$.

5. $\mathrm{K}(G)$ è il più piccolo sottogruppo normale N di G tale che G/N sia abeliano.

Dimostrazione.

1. G è abeliano $\iff$ $[a,b] = e_G$ per tutti gli elementi $a, b \in G$ $\iff$ $\mathrm{K}(G) = \{e_G\}$

2. Gli elementi di $\mathrm{K}(G)$ sono prodotti di un numero finito di commutatori e loro inversi.
   Ma $[a,b]^{-1} = ((ab)(ba)^{-1})^{-1} = (ba)(ab)^{-1} = [b,a]$

3. $f([a,b]) = f((ab)(ba)^{-1}) = f(a)f(b)f(a)^{-1}f(b)^{-1} = [f(a), f(b)]$
   Dunque $f(\mathrm{K}(G)) \subseteq \mathrm{K}(G')$, con "=" quando f è suriettivo.

4. Sia $N \lhd G$. Allora $aNa^{-1} = N$ per ogni $a \in G$ e $f_a : N \to N, x \mapsto axa^{-1}$ è un isomorfismo$^{(*)}$ con $f_a^{-1} = f_{a^{-1}}$.
   Dunque
   $$a\,\mathrm{K}(N)a^{-1} = f_a(\mathrm{K}(N)) = \mathrm{K}(N) \text{ per } (3)$$
   $$f_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = f_a(x)f_a(y) \tag{$*$}$$
   Concludiamo quindi che $\mathrm{K}(N) \lhd G$.

5. $G/\,\mathrm{K}(G)$ è abeliano: poiché per $a, b \in G$ $(ab)(ba)^{-1} = [a,b] \in \mathrm{K}(G)$, si ha
   $$\overline{a} \cdot \overline{b} = \overline{ab} = \overline{ba} = \overline{b} \cdot \overline{a} \text{ in } G/\,\mathrm{K}(G)$$
   Sia adesso $N \lhd G$ tale che G/N è abeliano.
   Allora per $a, b \in G$ si ha
   $$Nab = Na \cdot Nb = Nb \cdot Na = Nba$$
   perciò $[a,b] = (ab)(ba)^{-1} \in N$. Dunque $\mathrm{K}(G) \subseteq N$.

□

4.3. Lemma e definizione

Per un gruppo $(G, \cdot)$ sono equivalenti i seguenti enunciati:

1. Esiste un $n \in \mathbb{N}$ tale che $\mathrm{K}^n(G) = \{e_G\}$
2. G possiede una catena di sottogruppi

   $$\{e_G\} = N_m \leq \ldots \leq N_2 \leq N_1 \leq N_0 = G$$

   con le seguenti proprietà per ogni $1 \leq i \leq m$:

   (i) $N_i \lhd N_{i-1}$

   (ii) N_{i-1}/N_i è abeliano.

   Se valgono 1 e 2, il gruppo G è detto **risolubile**.

Dimostrazione.
(1) ⇒ (2):
Consideriamo la catena

$$\{e_G\} = \mathrm{K}^n(G) \leq \ldots \leq \mathrm{K}^2(G) \leq \mathrm{K}(G) \leq G =: \mathrm{K}^0(G)$$

Abbiamo

(i) $\mathrm{K}^i(G) = \mathrm{K}(\mathrm{K}^{i-1}(G)) \lhd \mathrm{K}^{i-1}(G)$

(ii) $\mathrm{K}^{i-1}(G)/\,\mathrm{K}^i(G)$ è abeliano per 4.2.

(2) ⇒ (1):
Procediamo per induzione su m:

$\underline{m = 1}$:

$$\{e_G\} = N_1 \leq G, \text{ con } N_1 \lhd G \text{ e } G/N \text{ abeliano.}$$

Poiché $G/N_1 = G/\{e_G\} \cong G$, concludiamo che G è abeliano e pertanto $\mathrm{K}(G) = \{e_G\}$.

$\underline{m \to m+1}$:
Sia

$$\{e_G\} = N_{m+1} \leq N_m \leq \ldots \leq N_1 \leq G$$

una catena con (i) e (ii).
Per ipotesi induttiva esiste un $n \in \mathbb{N}$ tale che $\mathrm{K}^n(N_1) = \{e_G\}$.

Inoltre $\mathrm{K}(G/N_1) = \{e_{G/N_1}\}$ perché G/N_1 è abeliano per (i).
Consideriamo l'epimorfismo canonico $\nu : G \to G/N_1$, vediamo che:

$$\nu(\mathrm{K}(G)) = \mathrm{K}(G/N_1) = \{e_{G/N_1}\}$$

Perciò $\mathrm{K}(G) \subseteq \ker \nu = N_1$.
Segue che $\mathrm{K}^{n+1}(G) \subseteq \mathrm{K}^n(N_1) = \{e_G\}$ considerando l'omomorfismo dato dall'inclusione di $\mathrm{K}(G) \subseteq N_1$ ecc.

□

4.4. Corollario

Sia G un gruppo risolubile.
Allora sono risolubili anche tutti i suoi sottogruppi normali N e tutti i quozienti G/N.
Inoltre G è risolubile se e solo se esiste un sottogruppo normale $N \lhd G$ tale che N e G/N sono risolubili.

Dimostrazione.
Se G è risolubile, allora $\mathrm{K}^n(G) = \{e_G\}$ per un $n \in \mathbb{N}$ opportuno, e applicando la 4.2 all'immersione $N \hookrightarrow G$ abbiamo $\mathrm{K}^n(N) = \{e_G\}$.
Inoltre considerando $\nu : G \to G/N$ abbiamo

$$\mathrm{K}^n(G/N) = \nu(\mathrm{K}^n(G)) = \{e_{G/N}\}$$

Per il secondo enunciato si procede come nella dimostrazione di 4.3 (2) $\Rightarrow$ (1)

□

4.5. Richiamo sul segno di una permutazione

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

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

è detto **segno** della permutazione σ.
Si dice che σ è *pari* se $\varepsilon(\sigma) = 1$, altrimenti σ è *dispari*.

Dimostrazione.
$(-1)^r = \prod_{1 \leq i < j \leq n} \frac{\sigma(i)-\sigma(j)}{i-j}$ con ($r = \#$ inversioni):

$$\begin{aligned}
\prod_{i<j}(\sigma(i) - \sigma(j)) &= \prod_{\substack{i<j \\ \sigma(i)<\sigma(j)}} (\sigma(i) - \sigma(j)) \cdot \prod_{\substack{i<j \\ \sigma(i)>\sigma(j)}} (\sigma(i) - \sigma(j)) \text{ (scambio)} \\
&= \prod_{\substack{i<j \\ \sigma(i)<\sigma(j)}} (\sigma(i) - \sigma(j)) \cdot \prod_{\substack{i<j \\ \sigma(i)>\sigma(j)}} (\sigma(j) - \sigma(i)) \cdot (-1)^r \text{ (rinomino)} \\
&= \prod_{\substack{i<j \\ \sigma(i)<\sigma(j)}} (\sigma(i) - \sigma(j)) \cdot \prod_{\substack{j<i \\ \sigma(j)>\sigma(i)}} (\sigma(i) - \sigma(j)) \cdot (-1)^r \\
&= \prod_{\sigma(i)<\sigma(j)} (\sigma(i) - \sigma(j)) \cdot (-1)^r \\
\underset{\{\sigma(1),\dots,\sigma(n)\}=\{1,\dots,n\} \nearrow}{\text{(rinomino)}} &= \prod_{i<j}(i-j) \cdot (-1)^r, \text{ quindi } \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i-j} = (-1)^r
\end{aligned}$$

$\square$

4.6. Lemma e definizione

L'applicazione

$$\begin{aligned}
\varepsilon : S_n &\longrightarrow (\{-1, 1\}, \cdot) \\
\sigma &\longmapsto \varepsilon(\sigma)
\end{aligned}$$

è un omomorfismo suriettivo. Il suo nucleo A_n è formato dalle permutazioni pari. In particolare $A_n \lhd S_n$ con $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$.
Il sottogruppo A_n è detto **gruppo alterno**.
Si ha $|A_n| = \frac{n!}{2}$

Dimostrazione.
$\varepsilon : S_n \to (\{-1,1\},\cdot), \sigma \mapsto \varepsilon(\sigma)$ è un omomorfismo:
Siano $\sigma, \tau \in S_n$. Dobbiamo mostrare che $\varepsilon(\sigma \circ \tau) = \varepsilon(\sigma) \cdot \varepsilon(\tau)$

$$\begin{aligned}
\varepsilon(\sigma \circ \tau) &= \prod_{i<j} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{i-j} \\
&= \underbrace{\prod_{i<j} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\sigma(i) - \sigma(j)}}_{\substack{\shortparallel \\ (*)}} \cdot \underbrace{\prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i-j}}_{\substack{\shortparallel \\ \varepsilon(\tau)}}
\end{aligned}$$

Resta da verificare che $(*) = \varepsilon(\sigma)$.
Abbiamo

$$\begin{aligned}
(*) &= \prod_{\substack{i<j \\ \tau(i)>\tau(j)}} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} \cdot \prod_{\substack{i<j \\ \tau(i)<\tau(j)}} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} \\
&= \prod_{\substack{i<j \\ \tau(i)>\tau(j)}} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} \cdot \prod_{\substack{i<j \\ \tau(i)<\tau(j)}} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \begin{matrix}\text{(scambio)} \\ \text{(scambio)}\end{matrix} \\
&= \prod_{\substack{i<j \\ \tau(i)>\tau(j)}} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} \cdot \prod_{\substack{j<i \\ \tau(j)<\tau(i)}} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} \quad \text{(rinomino)} \\
&= \prod_{\tau(i)>\tau(j)} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} \\
\underset{\{\tau(1),\dots,\tau(n)\}=\{1,\dots,n\} \nearrow}{\text{(rinomino)}} \quad &= \prod_{i>j} \frac{\sigma(i) - \sigma(j)}{i-j} \underset{\substack{\uparrow \\ \text{(doppio scambio)}}}{=} \prod_{j>i} \frac{\sigma(j) - \sigma(i)}{j-i} = \varepsilon(\sigma)
\end{aligned}$$

In particolare, se σ è composizione di r trasposizioni $\sigma = \tau_1 \circ \ldots \circ \tau_2$, allora

$$\varepsilon(\sigma) = \varepsilon(\tau_1) \cdot \ldots \cdot \varepsilon(\tau_r) = (-1)^r$$

Ovviamente ε è suriettivo (ad esempio si ha $\varepsilon(\mathrm{id}) = 1$ e $\varepsilon(\begin{pmatrix}1 & 2\end{pmatrix}) = -1$).
Per il Teorema fondamentale dell'omomorfismo

$$S_n/A_n \cong \underset{\substack{\text{gruppo di} \\ \text{due elementi}}}{(\{-1,1\},\cdot)} \cong (\mathbb{Z}/2\mathbb{Z}, +)$$

Infine $[S_n : A_n] = \frac{|S_n|}{|A_n|}$, dunque

$$|A_n| = \frac{|S_n|}{[S_n : A_n]} = \frac{n!}{2}$$

$\square$

4.7. Risolubilità di S_n

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

Dimostrazione.

1. Ogni sottogruppo abeliano è risolubile, perciò S_1 e S_2 sono risolubili.
2. $\{\mathrm{id}\} \leq A_3 \leq S_3$ è una catena di sottogruppi normali con quozienti $A_3 \cong \mathbb{Z}/3\mathbb{Z}$, $S_3/\mathbb{Z}/2\mathbb{Z}$ abeliani.
3. $\{\mathrm{id}\} \leq \mathcal{V} \leq A_4 \leq S_4$ è una catena di sottogruppi normali con quozienti $\mathcal{V}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ abeliani. Infatti
$$\mathcal{V} = \{\mathrm{id}, \begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}, \begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}2 & 4\end{pmatrix}, \begin{pmatrix}1 & 4\end{pmatrix}\begin{pmatrix}2 & 3\end{pmatrix}\} \subset A_4$$
Resta da verificare che $\mathcal{V} \lhd S_4$.
Usiamo la formula 4.8:
$$\begin{aligned}\sigma\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}\sigma^{-1} &= \sigma\begin{pmatrix}1 & 2\end{pmatrix}\sigma^{-1}\sigma\begin{pmatrix}3 & 4\end{pmatrix}\sigma^{-1}\\ &= \underbrace{\begin{pmatrix}\sigma(1) & \sigma(2)\end{pmatrix}\circ\begin{pmatrix}\sigma(3) & \sigma(4)\end{pmatrix}}_{\in \mathcal{V}}\end{aligned}$$
Analogamente per gli altri elementi di $\mathcal{V}$.
4. Sia adesso $n > 4$.
   (i) Verifichiamo che se $N \lhd S_n$
   contiene tutti i 3-cicli, allora anche $\mathrm{K}(N)$ contiene tutti i 3-cicli:
   Sappiamo che $\mathrm{K}(N) \lhd S_n$ contiene $a = \begin{pmatrix}1 & 2 & 3\end{pmatrix}$, $b = \begin{pmatrix}1 & 4 & 5\end{pmatrix}$
   (stiamo usando $n \geq 5$).
   Quindi $\mathrm{K}(N)$ contiene
   $$\begin{aligned}[a,b] = aba^{-1}b^{-1} &= \begin{pmatrix}1 & 2 & 3\end{pmatrix}\begin{pmatrix}1 & 4 & 5\end{pmatrix}\begin{pmatrix}3 & 2 & 1\end{pmatrix}\begin{pmatrix}5 & 4 & 1\end{pmatrix}\\ &= \begin{pmatrix}1 & 2 & 3 & 4 & 5 & \dots & n\\ 2 & 4 & 3 & 1 & 5 & \dots & n\end{pmatrix} = \begin{pmatrix}1 & 2 & 4\end{pmatrix}\end{aligned}$$
   Dunque $\mathrm{K}(N)$ contiene anche tutti gli elementi $\sigma\begin{pmatrix}1 & 2 & 4\end{pmatrix}\sigma^{-1}$ per $\sigma \in S_n$, quindi $\begin{pmatrix}\sigma(1) & \sigma(2) & \sigma(4)\end{pmatrix}$ per 4.8.
   Se $\begin{pmatrix}x & y & z\end{pmatrix} \in S_n$ è un 3-ciclo, scegliamo un $\sigma \in S_n$ tale che $\sigma(1) = x$, $\sigma(2) = y$, $\sigma(4) = z$, e vediamo che
   $$\begin{pmatrix}x & y & z\end{pmatrix} = \sigma\begin{pmatrix}1 & 2 & 4\end{pmatrix}\sigma^{-1} \in \mathrm{K}(N)$$
   (ii) Poiché S_n contiene tutti i 3-cicli, concludiamo che anche $\mathrm{K}(S_n), \mathrm{K}^2(S_n), \mathrm{K}^3(S_n), \dots$ contengono tutti i 3-cicli.
   Perciò S_n non è risolubile.

$\square$

4.8. Lemma

Dati $\sigma \in S_n$ e $x_1, \ldots, x_m \in \{1, \ldots, n\}$ si ha

$$\sigma \circ \big(x_1 \quad \ldots \quad x_m\big) \circ \sigma^{-1} = \big(\sigma(x_1) \quad \ldots \quad \sigma(x_m)\big)$$

Dimostrazione.
Sia $j \in \{1, \ldots, n\}$,

$$\sigma \circ \big(x_1 \quad \ldots \quad x_m\big) \circ \sigma^{-1} \qquad\qquad \big(\sigma(x_1) \quad \ldots \sigma(x_m)\big)$$

$$j \mapsto \begin{cases} \sigma(x_{i+1}) & \text{se } j = \sigma(x_i), i < m \\ \sigma(x_1) & \text{se } j = \sigma(x_m) \\ j & \text{se } j \notin \{\sigma(x_1), \ldots, \sigma(x_m)\} \end{cases} \qquad j \mapsto \begin{cases} \sigma(x_{i+1}) & \text{se } j = \sigma(x_i), i < m \\ \sigma(x_1) & \text{se } j = \sigma(x_m) \\ j & \text{se } j \notin \{\sigma(x_1), \ldots, \sigma(x_m)\} \end{cases}$$

$\square$

5. Azioni di un gruppo

5.1. Osservazione

Siano $(G, \cdot)$ un gruppo e X un insieme non-vuoto.
Supponiamo che esista un omomorfismo

$$G \to \mathrm{S}(X), a \mapsto \sigma_a$$

Abbiamo quindi $\sigma_e = \mathrm{id}_X$ e $\sigma_{a \cdot b} = \sigma_a \circ \sigma_b$.
Possiamo definire un'applicazione

$$G \times X \to X, (a, x) \mapsto \sigma_a(x)$$

con le proprietà

$$\begin{aligned} \sigma_e(x) &= x \\ \sigma_{ab}(x) &= \sigma_a(\sigma_b(x)) \end{aligned}$$

per ogni $x \in X, a, b \in G$.

5.2. Definizione

Dati un gruppo $(G, \cdot)$ e un insieme $X \neq \varnothing$, si dice che G *agisce* su X se esiste un'applicazione

$$G \times X \to X, (a, x) \mapsto a(x)$$

detta **azione** di G su X, con le seguenti proprietà per ogni $x \in X$:

(*A*1) $e(x) = x$

(*A*2) $ab(x) = a(b(x))$ per $a, b \in G$

5.3. Osservazione

Abbiamo visto che ogni omomorfismo $G \to \mathrm{S}(X)$ da luogo ad un'azione G su X.
Viceversa data un'azione

$$G \times X \to X, (a, x) \mapsto a(x)$$

per ogni elemento $a \in G$ si ottiene un'applicazione

$$f_a : X \to X, x \mapsto a(x)$$

Per la proprietà $(A1)$ si si ha $f_e = \mathrm{id}_X$ e per $(A2)$ si ha

$$f_{ab}(x) = f_a(f_b(x)) \tag{$*$}$$

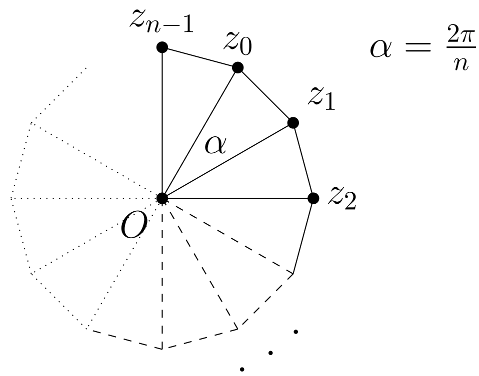
Quindi f_a è invertibile, con applicazione inversa $f_{a^{-1}}$, perciò $f_a \in \mathrm{S}(X)$.
Dunque otteniamo un'applicazione

$$f : G \to \mathrm{S}(X), a \mapsto f_a$$

che è un omomorfismo per $(*)$.
Concludiamo quindi che le azioni di G su X corrispondono biunivocamente agli omomorfismi $G \to \mathrm{S}(X)$.

5.4. Esempi

1. Sia $n \in \mathbb{N}$. Consideriamo il poligono regolare di n vertici



Il gruppo $(\mathbb{Z}/n\mathbb{Z}, +)$ agisce sull'insieme dei vertici $X = \{z_0, \ldots, z_{n-1}\}$ tramite

$$\begin{array}{rcl} \mathbb{Z}/n\mathbb{Z} \times X & \longrightarrow & X \\ (\overline{r}, z_i) & \longmapsto & \rho^r(z_i) \end{array}$$

dove ρ è la rotazione di angolo α e centro O.
Infatti:

- poiché $\rho^n = \mathrm{id}_X$, vediamo che ρ^r non dipende dalla scelta del rappresentante di $\overline{r}$, quindi l'applicazione è ben definita.
- $(A1)$ $(\overline{0}, x) \mapsto \rho^0(x) = x$

  $(A2)$ $(\overline{r+s}, x) = (\overline{r} + \overline{s}, x) \mapsto \rho^{r+s}(x) = \rho^r(\rho^s(x))$

2. Siano K un campo, $n \in N$. Il gruppo delle matrici invertibili $G = \mathrm{Gl}(n, K)$ agisce sullo spazio vettoriale $V = K^n$ tramite

$$G \times V \to V, (A, v) \mapsto Av$$

3. Ogni gruppo G agisce su se stesso tramite il *coniugio*

$$G \times G \to G, (a, x) \mapsto axa^{-1}$$

Infatti ogni elemento $a \in G$ definisce un automorfismo di G (cioè un isomorfismo $G \to G$) detto *automorfismo interno*

$$\mathrm{int}_a : G \to G, x \mapsto axa^{-1}$$

(int_a omomorfismo:

$$\mathrm{int}_a(xy) = axya^{-1} = axa^{-1}aya = \mathrm{int}_a(x) \cdot \mathrm{int}_a(y)$$

int_a invertibile con inversa $\mathrm{int}_{a^{-1}}$)
Dunque abbiamo un omomorfismo

$$\mathrm{int} : G \to \mathrm{S}(G), a \mapsto \mathrm{int}_a$$

Infatti:

$$\begin{aligned}\mathrm{int}_{ab}(x) &= (ab)xab^{-1}\\ &= a(bxb^{-1})a^{-1}\\ &= \mathrm{int}_a(\mathrm{int}_b(x))\end{aligned}$$

perciò $\mathrm{int}_{ab} = \mathrm{int}_a \circ \mathrm{int}_b$.
Se G è abeliano, l'azione del coniugio è banale.
Ogni gruppo $(G, \cdot)$ agisce su se stesso anche tramite la moltiplicazione (a sinistra):

$$G \times G \to G, (a, x) \mapsto a \cdot x$$

Infatti ogni elemento di G definisce una biiezione

$$\mathrm{t}_a : G \to G, x \mapsto a \cdot x$$

detta *traslazione*, con $\mathrm{t}_a^{-1} = \mathrm{t}_{a^{-1}}$ e $\mathrm{t}_{ab}(x) = a(b \cdot x) = \mathrm{t}_a(\mathrm{t}_b(x))$.
In altre parole

$$\mathrm{t} : G \to \mathrm{S}(G), a \mapsto \mathrm{t}_a$$

è un omomorfismo di gruppi. Inoltre t è iniettivo:
se $\mathrm{t}_a = \mathrm{id}_G$, allora $ax = x$ per ogni $x \in G$, perciò $a = e_G$.
Abbiamo dimostrato

5.5. Teorema di Cayley

Ogni gruppo G è isomorfo ad un sottogruppo del gruppo simmetrico $(\mathrm{S}(G), \circ)$

5.6. Lemma e definizione

Sia $G \times X \to X$ un'azione di un gruppo G su un insieme X. Per ogni elemento $x \in X$ consideriamo l'insieme

$$\mathrm{O}(x) := \{a(x) \mid a \in G\}$$

detto l'**orbita** di x attraverso l'azione di G.
Le orbite degli elementi di X inducono una partizione di X, cioè X è l'unione di orbite disgiunte a due a due.

Dimostrazione.
Consideriamo la relazione di equivalenza su X data da

$$x \sim y \text{ se } x \in \mathrm{O}(y)$$

riflessiva: $x \sim x$ poiché $x = e(x) \in \mathrm{O}(x)$
simmetrica: se $x \sim y$, allora $x = a(y)$ per un $a \in G$, dunque

$$y = e(y) \underset{(A1)}{=} (a^{-1}a)(y) \underset{(A2)}{=} a^{-1}(a(y)) = a^{-1}(x) \in \mathrm{O}(x)$$

transitiva: se $x \in \mathrm{O}(y)$ e $y \in \mathrm{O}(z)$, allora $x = a(y)$ e $y = b(z)$ per $a, b \in G$ opportuni, quindi

$$x = a(b(z)) \underset{(A2)}{=} (ab)(z) \in \mathrm{O}(z)$$

e pertanto $x \sim z$.
Adesso si applichi 2.1.

$\square$

5.7. Lemma e definizione

Sia $G \times X \to X$ un'azione di un gruppo G su un insieme X. Per ogni elemento $x \in X$ lo **stabilizzatore** di x è il sottogruppo di G dato da

$$G_x := \{a \in G \mid a(x) = x\}$$

Dimostrazione.
Se $a, b \in G_x$, allora $a(x) = x = b(x)$, perciò

$$b^{-1}(x) = b^{-1}(b(x)) \underset{(A2)}{=} e(x) \underset{(A1)}{=} x \quad \text{e} \quad ab^{-1}(x) = a(b^{-1}(x)) = a(x) = x$$

Dunque $ab^{-1} \in G_x$.

$\square$

5.8. Esempio

Ogni $\sigma \in S_n$ induce un'azione del gruppo $G = \langle\sigma\rangle \leq S_n$ sull'insieme $X = \{1, \ldots, n\}$ attraverso $G \times X \to X, (\sigma^m, i) \to \sigma^m(i)$.
Per 5.6 le orbite di questa azione inducono una partizione $X = \mathrm{O}(x_1) \cupdot \cdots \cupdot \mathrm{O}(x_r)$.
Ogni orbita è di forma

$$\mathrm{O}(x_i) = \{x_i, \sigma(x_i), \ldots, \sigma^{m_i}(x_i)\}$$

per un certo $m_i < \mathrm{ord}(\sigma)$.
$m_i = 0$ se e solo se $\mathrm{O}(x_i) = \{x_i\}$, ovvero $\sigma(x_i) = x_i$. In tal caso sia $\tau_i = \mathrm{id}_X$.
Per $m_i > 0$ consideriamo il ciclo

$$\tau_i = \begin{pmatrix} x_i & \sigma(x_i) & \ldots & \sigma^{m_i}(x_i) \end{pmatrix} \in S_n$$

Poiché le orbite sono disgiunte, i cicli $\tau_1, \ldots, \tau_r$ sono disgiunti.
E poiché $X = \mathrm{O}(x_1) \cupdot \cdots \cupdot \mathrm{O}(x_r)$, abbiamo

$$\sigma = \tau_1 \circ \ldots \circ \tau_r$$

Tale scomposizione è unica, a meno dell'ordine:
Se anche $\sigma = \rho_1 \circ \ldots \circ \rho_s$ con cicli disgiunti $\rho_1, \ldots, \rho_s$, allora gli insiemi $\{x \in X \mid \rho_i(x) \neq x\}$ per $1 \leq i \leq s$, determinano le orbite dell'azione di G su X.
Pertanto $r = s$ e $\{\rho_1, \ldots, \rho_s\} = \{\tau_1, \ldots, \tau_r\}$.
Abbiamo dimostrato

5.9. Teorema

Ogni permutazione è prodotto di cicli disgiunti. Tale scomposizione è unica a meno dell'ordine.

Esempio

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 6 & 1 & 8 & 7 & 3 & 4 \end{pmatrix}$$

Le orbite di $G = \langle \sigma \rangle$ sono:

$$\mathrm{O}(1) = \{1, 2, 5, 8, 4\} \, \mathrm{O}(3) = \{3, 6, 7\}$$

$\sigma = \begin{pmatrix} 1 & 2 & 5 & 8 & 4 \end{pmatrix} \begin{pmatrix} 3 & 6 & 7 \end{pmatrix}$.
$\mathrm{ord}(\sigma) = 15 = |G|$.
Mentre gli stabilizzatori di G sono:

$$\begin{array}{ll} G_1 = \{\mathrm{id}, \sigma^5, \sigma^1 0\} & [G : G_1] = 5 \\ G_3 = \{\mathrm{id}, \sigma^3, \sigma^6, \sigma^9, \sigma^1 2\} & [G : G_3] = 3 \end{array}$$

Osserviamo che $|\,\mathrm{O}(1)| = [G : G_1]$ e $|\,\mathrm{O}(3)| = [G : G_3]$.

5.10. Equazioni delle orbite

Sia $G \times X \to X$ un'azione di un gruppo G su un insieme X. Per ogni elemento $x \in X$ si ha

$$|\,\mathrm{O}(x)| = [G : G_x]$$

Dimostrazione.
In $\mathrm{O}(x)$ si ha:

$$\begin{aligned} a(x) = b(x) &\text{ se e solo se } x = a^{-1}b(x) \\ &\text{ se e solo se } a^{-1}b \in G_x \\ &\text{ se e solo se } \overline{a} = \overline{b} \text{ in } G/G_x \end{aligned}$$

Possiamo quindi definire

$$\begin{array}{rcl} \mathrm{O}(x) & \longrightarrow & G/G_x \\ a(x) & \longmapsto & \overline{a} \end{array}$$

Che è ben-definita, iniettiva e ovviamente anche suriettiva.
Perciò

$$|\,\mathrm{O}(x)| = |G/G_x| = [G : G_x]$$

□

5.11. Lemma e definizione

Siano $(G, \cdot)$ un gruppo e $x \in G$.
Consideriamo l'azione del coniugio.
Lo stabilizzatore di x è

$$\mathrm{Z}(x) = \{a \in G \mid axa^{-1} = x\} = \{a \in G \mid ax = xa\}$$

detto **centralizzatore** di x in G.
Inoltre

$$\begin{aligned} \mathrm{O}(x) = \{x\} \text{ se e solo se } & \mathrm{Z}(x) = G \\ & \text{se e solo se } ax = xa \text{ per ogni } a \in G. \end{aligned}$$

In altre parole $\mathrm{O}(x) = \{x\}$ se e solo se x appartiene al **centro** di G:

$$\begin{aligned} \mathrm{Z}(G) &:= \{a \in G \mid ay = ya \text{ per ogni } y \in G\} \\ &= \bigcap_{y \in G} \mathrm{Z}(y) \end{aligned}$$

Corollario

Per $x \in G$ si ha $\mathrm{O}(x) = \{x\}$ se e solo se $G = G_x$.

$\square$

5.12. Equazione delle classi

Sia G un gruppo finito e siano $\mathrm{O}(x_1), \dots, \mathrm{O}(x_m)$ le orbite distinte di G rispetto all'azione del coniugio.
Possiamo supporre che esista un $1 \le r \le m$, tale che $x_1, \dots, x_r \in \mathrm{Z}(G)$,
e $x_{r+1}, \dots, x_m \notin \mathrm{Z}(G)$.
Allora

$$|G| = |\,\mathrm{Z}(G)| + \sum_{i=r+1}^{r} [G : \mathrm{Z}(x_i)]$$

Dimostrazione.
Poiché $G = \bigcup_{i=1}^{m} \mathrm{O}(x_i)$, abbiamo

$$|G| = \sum_{i=1}^{m} |\,\mathrm{O}(x_i)|$$

Inoltre $\bigcup_{i=1}^{r} \mathrm{O}(x_i) = \{x_1, \dots, x_r\} = \mathrm{Z}(G)$:
$\supseteq$:
Se $x \in \mathrm{Z}(G)$ allora $x \in \mathrm{O}(x_i)$ con $1 \le i \le m$, ovvero $\{x\} = \mathrm{O}(x) = \mathrm{O}(x_i)$, perciò $x = x_i$ e $1 \le r \le r$.

Dunque $G = \mathrm{Z}(G) \cup\!\!\!\cdot\; \bigcup_{i=r+1}^{m} \mathrm{O}(x_i)$ e

$$\begin{aligned} |G| &= |\,\mathrm{Z}(G)| + \sum_{i=r+1}^{m} |\,\mathrm{O}(x_i)| \\ &\underset{5.10}{=} |\,\mathrm{Z}(G)| + \sum_{i=r+1}^{m} [G : G_{x_i}] \end{aligned}$$

$\square$

5.13. Lemma e definizione

Ogni gruppo G agisce sull'insieme $\mathcal{H}$ dei suoi sottogruppi, tramite coniugio

$$G \times \mathcal{H} \to \mathcal{H}, (a, H) \mapsto aHa^{-1}$$

Infatti $aHa^{-1} \in \mathcal{H}$, ovvero $aHa^{-1} \leq G$:
Se $axa^{-1}, aya^{-1} \in aHa^{-1}$, allora

$$(axa^{-1})(aya^{-1})^{-1} = axa^{-1}ay^{-1}a^{-1} = a\underbrace{xy^{-1}}_{\substack{\cap \\ H}}a^{-1} \in aHa^{-1}$$

L'orbita di H è l'insieme di tutti i sottogruppi di G che sono coniugati ad H e il suo stabilizzatore è il **normalizzante**

$$\begin{aligned} \mathrm{N_G}(H) &= \{a \in G \mid aHa^{-1} = H\} \\ &= \{a \in G \mid aH = Ha\} \end{aligned}$$

Per 5.10 il numero dei sottogruppi di G coniugati ad H è $[G : \mathrm{N_G}(H)]$

6. Teoremi di Sylow

Il Teorema di Lagrange afferma che l'ordine di ogni sottogruppo di un gruppo G di ordine n divide n.
In generale però possono esistere divisori m di n tali che G non possiede sottogruppi di ordine m.

6.1. Esempio

Il gruppo alterno A_4 ha 12 elementi e non possiede sottogruppi di ordine 6.
Per verificarlo procediamo per assurdo e supponiamo che esista $H \leq A_4$ con $|H| = 6$.

1. Poiché $[G : A_4] = 2$, si ha $H \lhd G$.

2. Inoltre l'intersezione $H \cap \mathcal{V}$ con il gruppo di Klein $\mathcal{V}$ deve avere $|H \cap \mathcal{V}| = 2$.
   Infatti $|H \cap \mathcal{V}|$, per il Teorema di Lagrange, divide sia $|H| = 6$ che $|\mathcal{V}| = 4$, perciò $|H \cap \mathcal{V}| \in \{1, 2\}$.
   Ma se $|H \cap \mathcal{V}| = 1$, ovvero $H \cap \mathcal{V} = \{\mathrm{id}\}$, allora l'applicazione
   $$H \times \mathcal{V} \to A_4, (h, v) \mapsto hv$$
   sarebbe iniettiva:
   se (h_1, v_1) e (h_2, v_2) soddisfano $h_1v_1 = h_2v_2$, allora $h_2^{-1}h_1 = v_2v_1^{-1} \in H \cap \mathcal{V}$, perciò $h_2^{-1}h_1 = v_2v_1^{-1} = \mathrm{id}$ e $h_1 = h_2$, $v_1 = v_2$, quindi $(h_1, v_1) = (h_2, v_2)$.
   Ma ciò è impossibile poiché $|H \times \mathcal{V}| = 24$ e $|A_4| = 12$.

3. Sappiamo per (2) che $H \cap \mathcal{V} = \{\mathrm{id}, v\}$ per un $v \in \mathcal{V} \setminus \{\mathrm{id}\}$.
   Perciò $v = \begin{pmatrix} i & j \end{pmatrix} \begin{pmatrix} k & l \end{pmatrix}$ con $\{i, j, k, l\} = \{1, 2, 3, 4\}$.
   Poniamo $\sigma = \begin{pmatrix} i & j & k \end{pmatrix}$ e calcoliamo
   $$\begin{aligned} \sigma v \sigma^{-1} &= \begin{pmatrix} \sigma(i) & \sigma(j) \end{pmatrix} \begin{pmatrix} \sigma(k) & \sigma(l) \end{pmatrix} \\ &= \begin{pmatrix} j & l \end{pmatrix} \begin{pmatrix} i & l \end{pmatrix} \neq v \end{aligned}$$
   Perciò $\sigma v \sigma^{-1} \notin H \cap \mathcal{V}$, quindi $\sigma v \sigma^{-1} \notin H$.
   Ma ciò contraddice $H \lhd A_4$.

6.2. Definizione

Dato un numero primo p diciamo che un gruppo è un *p-gruppo* se il suo ordine è di forma p^k con $k > 0$.

6.3. Osservazione

Se p è primo e G è un gruppo con $|G| = p$, allora G è ciclico (per $a \in G \setminus \{\text{id}\}$, si ha $1 < \text{ord}(a) \mid p$, perciò $\text{ord}(a) = p$ e $G = \langle a \rangle$) e pertanto è abeliano.

6.4. Proposizione

Sia p primo e sia G un p-gruppo con $|G| = p^k$, $k \in \mathbb{N}$.
Allora p divide $|\,\mathrm{Z}(G)|$.

Dimostrazione.
Usiamo l'equazione delle classi 5.12

$$|G| = |\,\mathrm{Z}(G)| + \sum_{i=r+1}^{m} [G : G_{x_i}]$$

Dove $x_{r+1}, \ldots, x_m$ sono i rappresenti delle orbite di G attraverso l'operazione del coniugio che non sono elementi del centro $\mathrm{Z}(G)$.
Sappiamo che $[G : G_{x_i}] \mid |G|$ per ogni $r < i \leq m$ e $[G : G_{x_i}] > 1$, poiché
$[G : G_{x_i}] = |\,\mathrm{O}(x_i)|$ e $\mathrm{O}(x) = \{x\}$ se e solo se $x \in \mathrm{Z}(G)$.
Dunque ogni $[G : G_{x_i}]$ è una potenza non banale di p.
Poiché p divide $|G|$ e ciascun $[G : G_{x_i}]$, concludiamo che $p \mid |\,\mathrm{Z}(G)|$.

□

6.5. Corollario

Se p è primo e G è un gruppo con $|G| = p^k$, $k \in \mathbb{N}$, allora G è risolubile ed esiste una catena di sottogruppi

$$\{e\} = N_0 \leq N_1 \leq N_2 \leq \ldots \leq N_k = G$$

tale che per ogni $1 \leq i \leq k$

(i) $N_{i-1} \lhd N_i$

(ii) $|N_i| = p^i$

Dimostrazione.
La dimostrazione è lasciata per esercizio.

□

6.6. Definizione

Sia G un gruppo e p un numero primo. I sottogruppi di G che sono p-gruppi si dicono *p-sottogruppi*.
Inoltre $H \leq G$ è detto **p-sottogruppo di Sylow** se è massimale, cioè non esiste un p-sottogruppo di G che contenga propriamente H.

6.7. Esempi

Sia G un gruppo finito e p primo.

1. Se p non divide $|G|$, allora $\{e\}$ è l'unico p-sottogruppo (di Sylow) di G.

2. Se G è abeliano, allora

$$G_p = \{a \in G \mid \mathrm{ord}(a) \text{ è una potenza di } p\}$$

   è l'unico p-sottogruppo di Sylow di G
   (da dimostrare per esercizio)

3. $G = S_4$ con $|G| = 24 = 2^3 \cdot 3$.
   I 3-sottogruppi non banali di G sono tutti di ordine 3, perciò isomorfi a $\mathbb{Z}/3\mathbb{Z}$.
   I 2-sottogruppi non banali di G possono avere ordine 2,4 oppure 8.

   - ordine 2: generati da trasposizioni, sono isomorfi a $\mathbb{Z}/2\mathbb{Z}$.
   - ordine 4: $\mathcal{V}$, oppure sottogruppi generati da cicli di lunghezza 4, quindi isomorfi a $\mathbb{Z}/4\mathbb{Z}$.
   - ordine 8: abbiamo D_4, altri ?
     Vediamo che questi sono i 2-sottogruppi di Sylow e sono tutti coniugati (e quindi isomorfi) tra loro.

6.8. Teorema(Wielandt)

Sia G un gruppo finito e sia p un numero primo tale che p^k con $k \in \mathbb{N}$ opportuno divide l'ordine di G.
Allora G possiede un sottogruppo di ordine p^k.

Dimostrazione.
$n = |G| = p^l m$ dove $k < l$ e p e m sono coprimi.
Poniamo $t = p^k$ e consideriamo l'insieme $\mathcal{A}$ di tutti i sottoinsiemi di G che hanno esattamente t elementi.
Vogliamo mostrare che $\mathcal{A}$ contiene un sottogruppo di G.
Innanzitutto, si ricordi che per $X \in \mathcal{A}$ e per $a \in G$ si ha che

$$aX = \{ax \mid x \in X\} \text{ ha nuovamente cardinalità } t$$

Abbiamo quindi un'azione

$$G \times \mathcal{A} \to \mathcal{A}, (a, X) \mapsto aX$$

che induce una partizione di $\mathcal{A}$.
Siano $\mathrm{O}(x_1), \ldots, \mathrm{O}(x_r)$ le orbite distinte di $\mathcal{A}$ e siano $G_{x_1}, \ldots, G_{x_r}$ i loro stabilizzatori.
Per 5.10

$$|\mathcal{A}| = \sum_{i=1}^{r} |\,\mathrm{O}(x_i)| = \sum_{i=1}^{r} [G : G_{x_i}]$$

Abbiamo

$$\begin{aligned} |\mathcal{A}| = \binom{n}{t} = \frac{n!}{t!(n-t)!} &= \frac{n(n-1)\cdots(n-t+1)}{t(t-1)\cdots 1} \\ &= \prod_{i=0}^{t-1} \frac{n-i}{t-i} = \binom{n-1}{t-1}\frac{n}{t} \end{aligned}$$

dove $\frac{n}{t} = p^{l-k}m$ e per il Lemma 6.9 concludiamo che $|\mathcal{A}|$ è divisibile per p^{l-k}, ma non per p^{l-k+1}.
Quindi deve esistere un $1 \leq i \leq r$ tale che $[G : G_{x_i}]$ non è divisibile per p^{l-k+1}.
Resta da verificare che $|G_{x_i}| = t$.

$$G_{x_i} = \{a \in G \mid aX_i = X_i\}$$

Se $x \in X_i$, allora possiamo definire

$$\mathrm{t}_x : G_{x_i} \to X_i, a \mapsto ax$$

che è iniettiva.

Dunque $|G_{x_i}| \leq |X_i| = t$.
Inoltre

$$\underbrace{|G|}_{\substack{\| \\ p^l m}} = |G_{x_i}| \cdot \underbrace{[G : G_{x_i}]}_{\substack{\uparrow \\ \text{non è divisibile} \\ \text{per } p^{l-k+1}}}$$

$\Rightarrow p^k \mid |G_{x_i}|$
Quindi $t \leq |G_{x_i}|$, perciò G_{x_i} ha ordine t.

$\square$

6.9. Lemma

Siano p un numero primo , $k, n \in \mathbb{N}$. Se $t = p^k$ divide n, allora p non divide $\binom{n-1}{t-1}$

Dimostrazione.
Sia $n = p^k m$. Per ogni $1 \leq i \leq t-1$ scriviamo $i = p^{k_i} m_i$ con $0 \leq k_i < k$, $m_i \in \mathbb{N}$ tali che p e m_i siano coprimi.
Abbiamo

$$\frac{n-i}{t-i} = \frac{p^k m - p^{k_i} m_i}{p^k - p^{k_i} m_i} = \frac{p v_i - m_i}{p w_i - m_i}$$

per $v_i, w_i \in \mathbb{N}$ opportuni, perciò

$$\binom{n-1}{t-1} = \prod_{i=1}^{t-1} \frac{n-i}{t-1} = \frac{pv - m'}{pw - m'}$$

dove $m' = \prod_{i=1}^{t-1}(-m_i)$.
Dunque, se p dividesse $\binom{n-1}{t-1}$, allora $\frac{pv-m'}{pw-m'} = p \cdot q$ con $q \in \mathbb{N}$ opportuno, perciò $pv - m' = p \cdot q(pw - m')$ e p divide m'.
Ma ciò è impossibile poiché ogni m_i è coprimo con p.

$\square$

6.10. Lemma

Siano G un gruppo finito, p un numero primo e sia $|G| = p^k m$ dove $k, m \in \mathbb{N}$ e p non divide m.
Sia P un p-sottogruppo di G di ordine p^k.
Per ogni p-sottogruppo H di G, esiste un $x \in G$ tale che $H \subseteq xPx^{-1}$.

Dimostrazione.
Il sottogruppo H di G agisce sull'insieme G/P dei laterali di G modulo P tramite

$$H \times G/P \to G/P, (h, \overline{x}) \mapsto \overline{hx}$$

Abbiamo $|G/P| = \frac{|G|}{|P|} = m$.
Se $\mathrm{O}(\overline{x_1}), \ldots, \mathrm{O}(\overline{x_r})$ sono le orbite di G/P, abbiamo

$$m = |G/P| = \sum_{i=1}^{r} [H : H_{\overline{x_i}}] \qquad \text{per 5.10}$$

Dove ogni addendo $[H : H_{\overline{x_i}}]$ divide $|H|$ per il Teorema di Lagrange e pertanto è una potenza di p. Perciò deve esistere un addendo con esponente nullo, altrimenti $p \mid m$, ovvero esiste un i con $[H : H_{\overline{x_i}}] = 1$.
Ciò significa

$$H = H_{\overline{x_i}} = \{h \in H \mid \overline{hx_i} = \overline{x_i} \text{ in } G/P\}$$

Dunque per ogni $h \in H$ abbiamo

$$\overline{hx_i} = \overline{x_i} \qquad \text{in } G/P$$

ovvero $x_i^{-1} h x_i \in P$, cioè $h \in x_i P x_i^{-1}$.
Dunque $H \subseteq x_i P x_i^{-1}$.

$\square$

6.11. Teoremi di Sylow

Sia G un gruppo finito di ordine n e sia p un numero primo.
Supponiamo che $n = p^k m$, dove $k, m \in \mathbb{N}$ e p non divide m.

1. G possiede p-sottogruppi di Sylow. Essi sono precisamente i sottogruppi di ordine p^k.

2. I p-sottogruppi di Sylow sono coniugati tra loro:
   se P_1, P_2 sono p-sottogruppi di Sylow, allora esiste un $x \in G$ tale che
   $P_1 = xP_2x^{-1}$.

3. Il numero s_p dei sottogruppi di Sylow di G è un divisore di m di forma

$$s_p = 1 + zp \quad \text{con } z \in \mathbb{N}_0$$

Dimostrazione.
Per il Teorema di Wielandt esiste un sottogruppo di ordine p^i per ogni $1 \leq i \leq k$.
Se $P \leq G$ ha ordine p^k, allora P non può essere contenuto propriamente in un p-sottogruppo di G, perciò P è un sottogruppo di Sylow.
Viceversa se H è un p-sottogruppo di Sylow, allora per 6.10 esiste un $x \in G$ tale che $H \subseteq xPx^{-1}$, quindi $H = xPx^{-1}$, e $|H| = |P| = p^k$. Abbiamo dimostrato (1) e (2).
Prima di continuare, notiamo

6.12. Corollario

Sia G un gruppo di ordine $n = p^k m$ come nel Teorema.

1. Ogni p-sottogruppo è contenuto in un p-sottogruppo di Sylow

2. Un p-sottogruppo di Sylow è normale se e solo se è l'unico p-sottogruppo di Sylow.

3. Se P è un p-sottogruppo di Sylow, allora il normalizzante
   $\mathrm{N_G}(P) = \{a \in G \mid aP = Pa\}$ ha ordine $|\mathrm{N_G}(P)| = p^k m'$ per un divisore m' di m e P è l'unico sottogruppo di Sylow di $\mathrm{N_G}(P)$.
   (Si rammenti che $P \lhd \mathrm{N_G}(P)$)

Riprendiamo la dimostrazione di 6.11

3. Se H è un p-sottogruppo di Sylow, allora s_p è il numero dei sottogruppi di G che sono coniugati ad H e per 5.13

$$s_p = [G : \mathrm{N_G}(H)]$$

Per il Teorema di Lagrange $s_p|\operatorname{N_G}(H)| = |G|$, ovvero $s_p(p^k m') = p^k m$.
Perciò $s_p \mid m$.
Si noti che H agisce sull'insieme $\mathcal{P}$ di tutti i p-sottogruppi di Sylow tramite

$$H \times \mathcal{P} \to \mathcal{P}, (a, P) \mapsto aPa^{-1}$$

ed è l'unico elemento di $\mathcal{P}$ con orbita banale:
certamente $\mathrm{O}(H) = \{aHa^{-1} \mid a \in H\} = \{H\}$, viceversa se $\mathrm{O}(P) = \{P\}$, allora aPa^{-1} per ogni $a \in H$, perciò $H \subseteq \operatorname{N_G}(P)$.
Quindi H è un p-sottogruppo di Sylow di $\operatorname{N_G}(P)$ e per 6.12(3) segue $H = P$.
Dunque se $\mathrm{O}(P_1), \ldots \mathrm{O}(P_r)$ sono le orbite di $\mathcal{P}$ attraverso questa azione e $H_{P_1}, \ldots, H_{P_r}$ i relativi stabilizzatori, allora

$$s_p = |\mathcal{P}| = \sum_{i=1}^{r} |\,\mathrm{O}(P_i)| = \sum_{i=1}^{r} [H : H_{P_i}]$$

dove ogni addendo divide $|H| = p^k$, quindi è una potenza di p e un unico addendo ha esponente nullo.
Concludiamo che $s_p = 1 + zp$ con $z \in \mathbb{N}_0$ opportuno.

$\square$

7. Conseguenze dei teoremi di Sylow

7.1. Teorema di Cauchy

Sia G un gruppo e sia p un numero primo.
Se $p \mid |G|$, allora G possiede un elemento di ordine p.

Dimostrazione.
Teorema di Wielandt per $k = 1$.

$\square$

7.2. Corollario

Se p è primo, allora un gruppo finito è un p-gruppo se e solo se l'ordine di ogni suo elemento è una potenza di p.

Dimostrazione.

"$\Rightarrow$" : per il Teorema di Lagrange

"$\Leftarrow$" : se q fosse un numero primo con $q \neq p$ e $q \mid |G|$, allora G avrebbe un elemento di ordine q. $\lightning$

$\square$

7.3. Richiamo

Dati due gruppi G_1 e G_2, il **prodotto diretto** (o *somma diretta*) di G_1 e G_2 è l'insieme $G_1 \times G_2$ con l'operazione $(a_1, a_2) \cdot (b_1, b_2) = (a_1 \cdot b_1, a_2 \cdot b_2)$ ed elemento neutro (e_1, e_2), ed è abeliano se e solo se lo sono G_1 e G_2.
Se $a_1 \in G_1$ e $a_2 \in G_2$ sono elementi di ordine m_1 e m_2 rispettivamente, allora $\mathrm{ord}((a_1, a_2)) = \mathrm{mcm}(m_1, m_2)$.

7.4. Teorema

Sia p un numero primo. Se G è un gruppo di ordine p^2, allora $G \cong \mathbb{Z}/p^2\mathbb{Z}$ oppure $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Dimostrazione.
Se G è un gruppo ciclico, allora $G \cong \mathbb{Z}/p^2\mathbb{Z}$.
Supponiamo che G non sia ciclico.
Poiché $p \mid |G|$ per 6.4 abbiamo $|G/\operatorname{Z}(G)| \in \{1, p\}$.
Perciò $G/\operatorname{Z}(G)$ è ciclico, quindi G è abeliano (esercizio), inoltre G possiede un elemento a di ordine p per 7.1.
Prendiamo $b \in G \setminus \langle a \rangle$. Allora $\operatorname{ord}(b) \in \{1, p, p^2\}$, ma $\operatorname{ord}(b) \neq 1$, altrimenti $b = e \in \langle a \rangle$, e inoltre $\operatorname{ord}(b) \neq p^2$, altrimenti G sarebbe ciclico. Dunque $\operatorname{ord}(b) = p$.
Consideriamo

$$\begin{array}{rcl} f : \langle a \rangle \times \langle b \rangle & \longrightarrow & G \\ (x, y) & \longmapsto & xy \end{array}$$

f omomorfismo:

$$f((x,y) \cdot (x',y')) = f((xx', yy')) = xx'yy' \underset{\substack{\uparrow \\ G \text{ abeliano}}}{=} (xy)(x'y') = f((x,y))f((x',y'))$$

f iniettivo:
se $f((x,y)) = e$, allora $xy = e$, perciò $x = y^{-1} \in \langle a \rangle \cap \langle b \rangle = \{e\}$ poiché $b \notin \langle a \rangle$ implica che $\langle a \rangle \cap \langle b \rangle \subsetneq \langle b \rangle$.
Dunque $f((x,y)) = e$ implica $x = y = e$ e $(x,y) = (e,e)$.
Poiché $|\langle a \rangle \times \langle b \rangle| = |G|$, concludiamo che f è un isomorfismo.
Quindi $G \cong \langle a \rangle \times \langle b \rangle \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

□

7.5. Teorema

Siano p, q numeri primi tali che $p < q$ e p non divida $q - 1$.
Ogni gruppo di ordine pq è ciclico (e isomorfo a $\mathbb{Z}/pq\mathbb{Z}$)

Dimostrazione.
Siano P un p-sottogruppo di Sylow e Q un q-sottogruppo di Sylow. Allora

$$P \cong \mathbb{Z}/p\mathbb{Z} \text{ e } Q \cong \mathbb{Z}/q\mathbb{Z} \text{ e } P \cap Q = \{e\}$$

Inoltre $s_q = 1 + zq$ con $z \in \mathbb{N}_0$ e divide p.
Poiché $p < q$, segue $z = 0$ e $s_q = 1$, perciò $Q \lhd G$.
Inoltre $s_p = 1 + z'p$ con $z' \in \mathbb{N}_0$ e divide q. Se $s_p \neq 1$, allora $s_p = q$ e $p \mid q - 1$ ↯
Perciò anche $s_p = 1$ e $P \lhd G$.

Consideriamo
$$f : P \times Q \to G, (x, y) \mapsto xy$$
Per verificare che f sia un omomorfismo basta mostrare che $xx'yy' = xyx'y'$ per tutti gli elementi $x, x' \in P$, $y, y' \in Q$, ovvero basta vedere che $xy = yx$ per $x \in P$ e $y \in Q$.
Ma si ha che
$$xy(yx)^{-1} = xyx^{-1}y^{-1} \in P \cap Q$$
Infatti $xyx^{-1} \in Q$ poiché $P \lhd G$, perciò $(xyx^{-1})y^{-1} \in Q$,
e $yx^{-1}y^{-1} \in P$ poiché $Q \lhd G$, quindi $x(yx^{-1}y^{-1}) \in P$.
Poiché $P \cap Q = \{e\}$, segue che $xy = yx$.
Concludiamo che f è un omomorfismo, e come in 7.4 vediamo che è un isomorfismo.
Perciò
$$G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$
Prendendo $a \in \mathbb{Z}/p\mathbb{Z}$ di ordine p e $b \in \mathbb{Z}/q\mathbb{Z}$ di ordine q vediamo che $\mathrm{ord}((a, b)) = pq$ (vedi 7.3).
Perciò $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$

□

7.6. Esempi

1. Ogni gruppo di ordine 15 è ciclico ($15 = 3 \cdot 5$ e 3 non divide 4)

2. Ogni gruppo G di 200 elementi ha un sottogruppo normale abeliano.
   Infatti $200 = 2^3 5^2$ con $s_5 = 1 + 5z \in \{1, 6, 11, \ldots\}$ e $s_5 \mid 8$, perciò $s_5 = 1$.
   Dunque c'è un unico 5-sottogruppo di Sylow P di ordine $|P| = 5^2$. Perciò
   $$P \lhd G \text{ è abeliano}$$

3. I gruppi di ordine < 10, a meno di isomorfismo

$\lvert G\rvert$	
2	$\mathbb{Z}/2\mathbb{Z}$
3	$\mathbb{Z}/3\mathbb{Z}$
4	$\mathbb{Z}/4\mathbb{Z}, \mathcal{V} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
5	$\mathbb{Z}/5\mathbb{Z}$
6	$\mathbb{Z}/6\mathbb{Z}, S_3$
7	$\mathbb{Z}/7\mathbb{Z}$
8	$\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, D_4, Q$
9	$\mathbb{Z}/9\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

Caso $|G| = 6$:
Se G non è ciclico, consideriamo $a, b \in G$ con $\operatorname{ord}(a) = 3$, $\operatorname{ord}(b) = 2$.
Allora $\operatorname{ord}(ab) \neq 6$, perciò $ab \neq ba$, quindi $bab = a^2$.
Infatti $\langle a \rangle$ ha indice 2 in G, ed è pertanto normale, dunque $bab \in \langle a \rangle = \{e, a, a^2\}$ e $bab \neq e$ poiché $a \neq e$ e $bab \neq a$ perché $ba \neq ab$.
Segue che $(ba)^2 = (ab)^2 = a^3 = e$.
Inoltre $|G/\langle a \rangle| = 2$ implica

$$G = \{e, a, a^2\} \cup \{b, ab, a^2b\} = \{ \underbrace{e, a, a^2}_{\substack{\text{ordine 3} \\ \updownarrow \\ \text{cicli di lunghezza 3}}} \quad , \quad \underbrace{b, ab, a^2b}_{\substack{\text{ordine 2} \\ \updownarrow \\ \text{trasposizioni}}} \}$$

Parte II.

Anelli

8. Il concetto di anello

8.1. Definizione

Un anello $(R, +, \cdot)$ è dato da un insieme non vuoto R e due operazione $+, \cdot : R \times R \to R$ che godono delle proprietà seguenti:

$(R1)$ $(R, +)$ 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

$$a(b + c) = ab + ac$$
$$(a + b)c = ac + bc \qquad \text{per } a, b \in R$$

R è detto *commutativo* se $(R, \cdot)$ gode della proprietà commutativa.

Osservazioni

1. $a \cdot 0_R = 0_R = 0_R \cdot a$ per ogni $a \in R$
   Infatti $a \cdot 0_R + a \cdot a \underset{(R3)}{=} a(0_R + a) = a \cdot a$
   perciò $a \cdot 0_R = 0_R$

2. $(-a)b = -ab = a(-b)$ per $a, b \in R$
   Infatti $(-a)b + ab \underset{(R3)}{=} (-a + a)b = 0_R \cdot b = 0_R$
   perciò $(-a)b = -ab$

3. 0_R e 1_R sono univocamente determinati.
   $0_R = 1_R$ se e solo se $R = \{0_R\}$.
   Infatti se $a \in R$, allora $a = a \cdot 1_R = a \cdot 0_R = 0_R$.
   In questo corso supponiamo sempre $R \neq \{0_R\}$

8.2. Lemma e definizione

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

1. Un elemento di $a \in R$ si dice **invertibile** se esiste un $b \in R$ 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 di R. Allora $1_R \in R^* \subseteq R \setminus \{0_R\}$ e $(R^*, \cdot)$ è un gruppo con elemento neutro 1_R.

3. Un **campo** è un anello commutativo tale che $R^* = R \setminus \{0_R\}$. In altre parole , $(R \setminus \{0_R\}, \cdot)$ è un gruppo abeliano.

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

8.3. Definizione

Sia $(R, +, \cdot)$ un anello (campo).
Un sottoinsieme non vuoto $S \subset R$ si dice *sottoanello (sottocampo)* se $(S, +, \cdot)$ è un anello (campo).

Osservazione

1. $S \subset R$ è un sottoanello se e solo se
   - $(S, +) \leq (R, +)$
   - $1_R \in S$ e $ab \in S$ per tutti gli elementi $a, b \in S$

2. $S \subset R$ è un sottocampo se e solo se

$$(S, +) \leq (R, +) \quad \text{e} \quad (S \setminus \{0_R\}, \cdot) \leq (R \setminus \{0_R\}, \cdot)$$

8.4. Esempi

1. $(\mathbb{Z}, +, \cdot)$ è un dominio, con $\mathbb{Z}^* = \{1, -1\}$
2. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sono campi.
   Si ha una catena di sottocampi
   $$\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$
   $\mathbb{Z}$ è un sottoanello si $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
3. Ogni campo è un dominio:
   se $a, b \in R$ con $ab = 0_R$ e $a \neq 0_R$, allora $b = a^{-1}ab = a^{-1} \cdot 0_R = 0_R$.
4. L'insieme $\mathrm{M}_{n\times n}(K)$ delle matrici quadrate di ordine n su un campo K è un anello rispetto all'addizione e moltiplicazione di matrici. Non è commutativo e ha divisori di zero.
   $$\begin{pmatrix}1 & 2\\ 0 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix} = \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}$$
   $$\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}\begin{pmatrix}1 & 2\\ 0 & 0\end{pmatrix} = \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$$
5. Se $R_1, \ldots, R_n$ sono anelli, allora $R = R_1 \times \cdots \times R_n$ è un anello rispetto all'addizione e moltiplicazione per componenti.
   $$(a_1, \ldots, a_n) \dot{+} (b_1, \ldots, b_n) = (a_1 \dot{+} b_1, \ldots, a_n \dot{+} b_n)$$
   con
   $$0_R = (0_{R_1}, \ldots, 0_{R_n})$$
   $$1_R = (1_{R_1}, \ldots, 1_{R_n})$$
6. Sia I un insieme non vuoto e sia R un anello.
   L'insieme R^I di tutte le funzioni $f : I \to R$ è un anello rispetto a
   $$f + g : I \to R, x \mapsto f(x) + g(x)$$
   $$\text{e } f \cdot g : I \to R, x \mapsto f(x) \cdot g(x)$$
   con
   $$0_{R^I} : I \to R, x \mapsto 0_R$$
   $$1_{R^I} : I \to R, x \mapsto 1_R$$
   Se $I = [0, 1]$, $R = \mathbb{R}$, allora l'insieme $\mathcal{C}^0(I, \mathbb{R})$ delle funzioni continue è un sottoanello di $\mathbb{R}^I$.
   Se $I = \mathbb{N}_0$, allora $\mathbb{R}^{\mathbb{N}_0}$ è l'anello delle successioni di numeri reali.

8.5. Lemma e definizione

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

$$(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) = (a_0 + b_0, a_1 + b_1, a_2 + a_2, \ldots)$$

$$(a_0, a_1, a_2, \ldots) \cdot (b_0, b_1, b_2, \ldots) = (a_0b_0, a_0b_1 + a_1b_0, a_0b_2 + a_1b_1 + a_2b_0, \ldots, \underset{\substack{\uparrow \\ k}}{\sum_{i=0}^{k} a_i b_{k-1}}, \ldots)$$

con

$$0 = (0_R, 0_R, 0_R, \ldots)$$

$$1 = (1_R, 0_R, 0_R, \ldots)$$

Sia $x = (0_R, 1_R, 0_R, \ldots)$, allora

$$x^2 = (0_R, 0_R, 1_R, 0_R, \ldots), \quad x^i = (0_R, 0_R, \ldots, \underset{\substack{\uparrow \\ i}}{1_R}, 0_R, \ldots)$$

Perciò

$$(a_0, a_1, a_2, \ldots) = a_0 1 + a_1 x + a_2 x^2 + \ldots = \sum_{i=0}^{n} a_i x^i$$

dove a_n è l'ultima componente non nulla.

Diremo che $f = \sum_{i=0}^{n} a_i x^i$ è un *polinomio* su R nell'incognita x con i coefficienti $a_0, \ldots, a_n$, dove a_n è detto **coefficiente conducente** e $n = \deg f$ è il **grado** di f.
Il polinomio nullo $0 = (0_R, 0_R, 0_R, \ldots)$ per convenzione ha grado -1.
L'anello $R^{(\mathbb{N}_0)}$ con queste operazioni è detto **anello dei polinomi** e si indica con $R[x]$.
Identificando gli elementi $a \in R$ con i polinomi costanti $(a, 0_R, 0_R, \ldots)$ (di grado ≤ 0) possiamo identificare R con un sottoanello di $R[x]$.

Le definizioni di somma e prodotto tra polinomi sono giustificate da

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i = \sum_{i=0}^{\max(n,m)} (a_i + b_i) x^i$$

$$\sum_{i=0}^{n} a_i x^i \cdot \sum_{i=0}^{m} b_i x^i = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 +$$

$$+ \ldots + (\sum_{i=0}^{k} a_i b_{k-i}) x^k + \ldots + a_n b_m x^{n+m}$$

Osservazione

Sia R un dominio, allora

1. $R[x]$ è un dominio
2. $\deg(fg) = \deg(f) + \deg(g)$ per $f, g \in R[x]$ (non nulli)
3. $R[x]^* = R^*$

Dimostrazione.
Siano $f = \sum_{i=0}^{n} a_i x^i, g = \sum_{i=0}^{m} b_i x^i$ due polinomi in $R[x]$, con $\deg f = n \geq 0$, $\deg g = m \geq 0$, allora

$$fg = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \ldots + a_n b_m x^{n+m}$$

con $fg \neq 0$ di grado $n + m$.
Per (3) ovviamente $a \in R^*$ è un polinomio invertibile con elemento inverso a^{-1}.
$\subseteq$:
Siano $f, g \in R[x]$ tali che $fg = 1_{R[x]} = 1_R$.
Allora

$$\underset{\substack{\vee| \\ 0}}{\deg f} + \underset{\substack{\vee| \\ 0}}{\deg g} = \deg(f + g) = 0$$

perciò $\deg f = \deg g = 0$ e $f = a_0$, $g = b_0$ con $a_0 b_0 = 1$.

$\square$

9. Ideali

9.1. Definizione

Dato un anello R, un sottoinsieme non vuoto $I \subset R$ è un **ideale (bilatero)** di R se gode delle proprietà

(i) se $a, b \in I$, allora $a + b \in I$

(ii) se $a \in I$ e $r \in R$, allora $ra, ar \in I$.

Osservazioni

1. Ogni anello possiede gli ideali banali $0 = \{0_R\}$ e R
2. Se I contiene un elemento invertibile, allora $I = R$:
   Se $a \in R^*$ e $a \in I$, allora per ogni $r \in R$ si ha
   $$r = r \cdot 1_R = (\underset{\substack{\pitchfork \\ R}}{r \cdot a^{-1}}) \cdot \underset{\substack{\pitchfork \\ I}}{a} \in I$$
3. Ogni ideale è un sottogruppo di $(R, +)$:
   Se $a, b \in I$, allora
   $$a - b = a + \underbrace{(\underset{\substack{\pitchfork \\ R}}{-1_R})\underset{\substack{\pitchfork \\ I}}{b}}_{\substack{\pitchfork \\ I}} \in I$$
4. Data una famiglia di ideali $(A_j)_{j \in J}$ di R, sono ideali anche
   $$\sum_{j \in J} A_j := \{\sum_{j \in J_0} a_j \mid J_0 \subseteq J \text{ sottoinsieme finito, e } a_j \in A_j \text{ per ogni } j \in J_0\}$$
   $$\bigcap_{j \in J} A_j$$
5. Ogni sottoinsieme non vuoto A di R definisce un ideale
   $$(A) = \bigcap \{I \mid I \text{ ideale di } R \text{ con } A \subset I\}$$
   ovvero il più piccolo ideale di R che contiene A.

Per $A = \{a_1, \dots, a_r\}$, scriviamo $(A) = (a_1, \dots, a_r)$.
Se R è commutativo, allora

$$(a_1, \dots, a_r) = \{\sum_{i=1}^{n} r_i a_i \mid r_1, \dots, r_n \in R\}$$

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

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

è detto *ideale principale* generato da a

9.2. Esempi

1. Ogni campo K possiede soltanto gli ideali banali 0 e K:
   Se $I \neq 0$, allora contiene un elemento invertibile $a \in I$ e perciò $I = K$
2. Ogni ideale di $\mathbb{Z}$ è principale:
   Se I è un ideale, allora $(I, +) \leq (R, +)$ e pertanto $I = n\mathbb{Z} = (n)$ per un $n \in \mathbb{N}_0$, vedi 1.4
3. Siano $A \subset I$ due insiemi e R un anello, allora

   $$\mathcal{N}(A) := \{f \in R^I \mid f(A) = 0\}$$

   è un ideale nell'anello R^I:
   (i) Se $f, g \in \mathcal{N}(A)$, allora per ogni $x \in A$

   $$(f + g)(x) = f(x) + g(x) = 0_R + 0_R = 0_R$$

   perciò $f + g \in \mathcal{N}(A)$

   (ii) Se $f \in \mathcal{N}(A)$, $g \in R^I$, allora per ogni $x \in A$

   $$(f \cdot g)(x) = f(x)g(x) = 0_R \cdot g(x) = 0_R$$

   perciò $f \cdot g \in \mathcal{N}(A)$ e analogamente per $g \cdot f$.

9.3. Lemma e definizione

Sia $(R,+,\cdot)$ un anello e sia I un ideale di R.
Poiché $(I,+) \lhd (R,+)$, possiamo considerare il gruppo quoziente $(R/I,+)$ dato dai laterali di R modulo I:

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

Si ha $\overline{a} = \overline{b}$ se e solo se $a - b \in I$.
Ponendo $\overline{a} + \overline{b} = \overline{a+b}$ sappiamo che $(R/I,+)$ è un gruppo abeliano.
Definiamo una moltiplicazione su R/I ponendo $\overline{a} \cdot \overline{b} = \overline{ab}$.
Questa operazione è ben definita:
se $\overline{a} = \overline{a'}$ e $\overline{b} = \overline{b'}$, allora

$$\begin{aligned} ab - a'b' &= ab - ab' + ab' - a'b' \\ &= \underset{\substack{\cap \\ R}}{a}\,\underbrace{(b-b')}_{\substack{\cap \\ I}} + \underbrace{(a-a')}_{\substack{\cap \\ I}}\,\underset{\substack{\cap \\ R}}{b'} \in I \end{aligned}$$

perciò $\overline{ab} = \overline{a'b'}$.
Con queste operazioni R/I diventa un anello con

$$0_{R/I} = \overline{0_R} = I \qquad 1_{R/I} = \overline{1_R} = 1_R + I$$

detto **anello quoziente di R modulo I**.

9.4. Esempio $\mathbb{Z}/n\mathbb{Z}$

Per $I = nZ$, consideriamo l'anello $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$

1. $\mathbb{Z}/n\mathbb{Z}^* = \{\overline{a} \mid 0 < a < n, \mathrm{MCD}(a,n) = 1\}$
   Infatti $\overline{a}$ è invertibile se e solo se esiste $\overline{\alpha} \in \mathbb{Z}/n\mathbb{Z}$ tale che $\overline{\alpha a} = \overline{1}$, ovvero $1 - \alpha a = \beta n$ con $\beta \in \mathbb{Z}$, ovvero esistono $\alpha, \beta \in \mathbb{Z}$ tali che

   $$1 = \alpha a + \beta n \text{ (identità di Bézout)}$$

   Ciò equivale a $\mathrm{MCD}(a,n) = 1$ (§10)

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

3. **La funzione di Euler**
   Per ogni $n \in \mathbb{N}$ denotiamo con $\varphi(n)$ il numero degli $0 < a < n$ che sono primi con n, ovvero

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

Otteniamo una funzione $\varphi : \mathbb{N} \to \mathbb{N}$ che si calcola come segue:
Se $n = p_1^{r_1} \cdot \ldots p_m^{r_m}$ è la scomposizione di n in fattori primi, allora

$$\varphi(n) = n(1 - \frac{1}{p_1}) \cdot \ldots \cdot (1 - \frac{1}{p_m})$$

Esempio

$n = 12 = 2^2 \cdot 3$

$$\begin{aligned}\varphi(12) &= |\{1, 5, 7, 11\}| = 4 \\ &= 12(1 - \frac{1}{2})(1 - \frac{1}{3}) \\ &= 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4\end{aligned}$$

Se p è primo $\varphi(p) = p - 1$.

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

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

Dimostrazione.
Per ipotesi $\overline{a} \in \mathbb{Z}/n\mathbb{Z}^*$ che è un gruppo di ordine $\varphi(n)$ rispetto alla moltiplicazione. Per 2.3 si ha $\overline{a}^{\varphi(n)} = \overline{1}$.

□

5. **Piccolo teorema di Fermat**
Se $a \in \mathbb{N}$ e p è un numero primo che non divide a, allora, in $\mathbb{Z}/p\mathbb{Z}$ si ha sempre

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

Dimostrazione.
Caso particolare $n = p$.

□

9.5. Algoritmo RSA

Vedi note

9.6. Definizione

Siano R e S anelli.
Un'applicazione $f : R \to S$ si dice

- **omomorfismo** se
  (i) $f(a+b) = f(a) + f(b)$ per $a, b \in R$
  (ii) $f(a \cdot b) = f(a)f(b)$ per $a, b \in R$
  (iii) $f(1_R) = 1_S$
- **monomorfismo** se è un omomorfismo iniettivo
- **epimorfismo** se è un omomorfismo suriettivo
- **isomorfismo** se è un omomorfismo biiettivo

Due anelli R, S sono *isomorfi* se esiste un isomorfismo $R \to S$.
In tal caso si scrive $R \cong S$.

9.7. Proposizione

Sia $f : R \to S$ un omomorfismo di anelli

1. $\ker f = \{a \in R \mid f(a) = 0_S\}$ è un ideale di R
2. $\operatorname{im} f$ è un sottoanello di S
3. $f(0_R) = 0_S$ e f è un monomorfismo se e solo se $\ker f = \{0_R\}$

Dimostrazione.
Sappiamo che f è anche un omomorfismo di gruppi $f : (R, +) \to (S, +)$, quindi

1. $\ker f \leq (R, +)$
   Inoltre se $r \in R$ e $a \in \ker f$, allora
   $$f(ra) = f(r)f(a) = f(r) \cdot 0_S = 0_S$$
   perciò $ra \in \ker f$, e analogamente per ar.
2. $\operatorname{im} f \leq (S, +)$
   $1_S = f(1_R) \in \operatorname{im} f$
   Se $f(a), f(b) \in \operatorname{im} f$, allora
   $$f(a) \cdot f(b) = f(ab) \in \operatorname{im} f$$
   Perciò $\operatorname{im} f$ è un sottoanello.
3. Come in 3.3

□

9.8. Esempi

1. Se $R \subset S$ è un sottoanello, allora l'immersione $\iota : R \hookrightarrow S$ è un monomorfismo di anelli. Ad esempio, l'immersione $\iota : \mathbb{Z} \hookrightarrow \mathbb{Q}$ è un monomorfismo la cui immagine non è un ideale di $\mathbb{Q}$

2. Sia R un anello. L'applicazione

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

è un epimorfismo con $\ker f = (x)$.
Infatti

$$\begin{aligned}\varphi\left(\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i\right) &= \varphi((a_0 + b_0) + (a_1 + b_1)x + \ldots) \\ &= a_0 + b_0 = \varphi\left(\sum_{i=0}^{n} a_i x^i\right) + \varphi\left(\sum_{i=0}^{m} b_i x^i\right)\end{aligned}$$

$$\begin{aligned}\varphi\left(\left(\sum_{i=0}^{n} a_i x^i\right) \cdot \left(\sum_{i=0}^{m} b_i x^i\right)\right) &= \varphi(a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \ldots + a_n b_m x^{n+m}) \\ &= a_0 b_0 = \varphi\left(\sum_{i=0}^{n} a_i x^i\right) \cdot \varphi\left(\sum_{i=0}^{n} b_i x^i\right) \\ \varphi(1_{R[x]}) &= 1_R\end{aligned}$$

φ è suriettivo: Ogni $a \in R$ è immagine del polinomio costante $f = a$.

$$\begin{aligned}\ker f &= \left\{\sum_{i=0}^{n} a_i x^i \mid a_0 = 0_R\right\} \\ &= \{f \in R[x] \mid f = xg \text{ con } g \in R[x]\} \\ &= (x)\end{aligned}$$

3. Ogni omomorfismo di anelli $\varphi : K \to R$ dove K è un campo è monomorfismo. Infatti $\ker \varphi \subsetneq K$ poiché $\varphi(1_K) = 1_R$ perciò $\ker \varphi = 0$ e φ è un monomorfismo per 9.7

4. Se R è un anello e I un suo ideale, allora

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

è un epimorfismo di anelli con nucleo $\ker \nu = I$, detto *epimorfismo canonico*, si veda 3.3 e si noti che per $a, b \in R$

$$\nu(ab) = \overline{ab} = \overline{a} \cdot \overline{b} = \nu(a) \cdot \nu(b)$$

$$\nu(1_R) = \overline{1_R} = 1_{R/I}$$

Come in 3.4 si ottiene

9.9. Teorema di fattorizzazione di omomorfismi

Siano $f : R \to S$ un omomorfismo di anelli e I un ideale di R tale che $I \subset \ker f$. Allora esiste uno e un solo omomorfismo $\overline{f} : R/I \to S$ tale che il seguente diagramma sia commutativo

$$\begin{tikzcd} R \arrow[r, "\nu"] \arrow[d, "f"'] & R/I \arrow[dl, dashed, "\overline{f}"] \\ S & \end{tikzcd}$$

cioè $\overline{f} \circ \nu = f$.
Si ha $\ker \overline{f} = \ker f / I$ e $\operatorname{im} \overline{f} = \operatorname{im} f$

Dimostrazione.
Si pone

$$\begin{aligned} \overline{f} : R/I &\longrightarrow S \\ \overline{a} &\longmapsto f(a) \end{aligned}$$

come in 3.4.
Verifichiamo che $\overline{f}$ è un omomorfismo di anelli:

$$\overline{f}(\overline{a} \cdot \overline{b}) = \overline{f}(\overline{ab}) = f(ab) = f(a)f(b) = \overline{f}(\overline{a})\overline{f}(\overline{b})$$

$$\overline{f}(1_{R/I}) = \overline{f}(\overline{1_R}) = f(1_R) = 1_S$$

□

9.10. Corollario (Teorema fondamentale dell'omomorfismo)

Sia $f : R \to S$ un omomorfismo di anelli. Allora $R/\ker f \cong \operatorname{im} f$.

Dimostrazione.
Caso $I = \ker f$.

□

9.11. Definizione

Un ideale I di un anello R è detto **massimale** se è un elemento massimale dell'insieme ordinato formato dagli ideali propri di R rispetto all'inclusione "$\subset$".
In altre parole I è massimale se e solo se per ogni ideale A di R con $I \subset A \subset R$ si ha $I = A$ oppure $A = R$

Osservazione

Se R è commutativo allora I è massimale se e solo se R/I è un campo.

Dimostrazione.
La dimostrazione è lasciata per esercizio.

$\square$

9.12. Esempi

1. Gli ideali massimale di $\mathbb{Z}$ sono precisamente gli ideali $p\mathbb{Z}$ con p primo.

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

$$\mathcal{N}(x) := \{f \in K^I \mid f(x) = x\}$$

è un ideale massimale nell'anello K^I.
Infatti l'applicazione

$$R := K^I \to K, f \mapsto f(x)$$

è un epimorfismo di anelli con nucleo $\mathcal{N}(x)$, quindi per il Teorema Fondamentale dell'Omomorfismo $R/\mathcal{N}(x) \cong K$.
Perciò $\mathcal{N}(x)$ è un ideale massimale.

3. Sia K un campo. Allora l'ideale (x) è massimale in $K[x]$.
Infatti per l'epimorfismo

$$\nu : K[x] \to K, \quad \sum_{i=0}^{n} a_i x^i \mapsto a_0$$

ha $\ker \nu = (x)$, perciò per il Teorema Fondamentale dell'Omomorfismo
$K[x]/(x) \cong K$

10. Divisibilità

10.1. Definizione

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

(i) $a = b \cdot q + r$ (*divisione con il resto*)

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

10.2. Esempi

1. $(\mathbb{Z}, |\cdot|)$ è un anello euclideo:

Se $0 < a < b$ scegliamo q tale che $qb \leq a < (q+1)b$ e poniamo $r = a - qb$, analogamente per gli altri casi.

2. Sia K un campo. Allora $(K[x], \deg)$ è un anello euclideo.

Dimostrazione.
Siano $f = \sum_{i=0}^{n} a_i x^i, g = \sum_{i=0}^{m} b_i x^i \in K[x]$, con $\deg f = n, \deg g = m$, entrambi > 0.
Se $m > n$, allora $f = 0 \cdot g + f$.
Assumiamo quindi $n \geq m$ e procediamo per induzione su n:
$\underline{n = 0}$:
$f = a_0$, $g = b_0 \neq 0_K$ e $f = \underbrace{a_0 b_0^{-1}}_{q} g$

$\underline{n > 0}$:

$$f' = f - a_n b_m^{-1} x^{n-m} g = f - (a_n x^n + \dots)$$

ha grado $< n$ e per l'ipotesi induttiva esistono $q, r \in K[x]$ tali che

(i) $f' = gq + r$

(ii) $\deg r < \deg g$ oppure $r = 0$

Ma allora
$$f = f' + a_n b_m^{-1} x^{n-m} g = g(q + a_n b_m^{-1} x^{n-m}) + r$$

□

3. Il sottoanello $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ di $\mathbb{C}$, degli *interi di Gauss* con
$$\begin{aligned} \delta : \mathbb{Z}[i] \smallsetminus \{0\} &\longrightarrow \mathbb{N}_0 \\ a + ib &\longmapsto a^2 + b^2 \end{aligned}$$
è un anello euclideo.

10.3. Proposizione

In un anello euclideo (R, δ) tutti gli ideali sono principali.
Un dominio con questa proprietà è detto **dominio a ideali principali (PID)**.

Dimostrazione.
Sia $I \neq 0$ un ideale e sia $0_R \neq b \in I$ elemento con $\delta(b)$ minimo.
Mostriamo che $I = (b)$.
Chiaramente si ha "$\supset$".
Per "$\subset$" consideriamo $a \in I$ ed eseguiamo la divisione con il resto:
$$a = bq + r \text{ con } r = 0_R \text{ oppure } \delta(r) < \delta(b)$$
Poiché $r = a - bq \in I$, si ha che $r = 0_R$ per la minimalità di b. Perciò $a = bq \in (b)$.

□

10.4. Definizione

Dati $x, y \in R$ in un dominio R si dice che

- x *divide* y, e si scrive $x \mid y$, se esiste un $r \in R$ tale che $y = xr$, ovvero $y \in (x)$
- x, y sono *associati*, e si scrive $x \sim y$, se $x \mid y$ e $y \mid x$, ovvero $(x) = (y)$

Osservazione

$x \sim y$ se e solo se esiste un $r \in R^*$ tale che $y = xr$

Dimostrazione.
"$\Leftarrow$": $y = xr$ e $x = yr^{-1}$, ovvero $x \mid y$ e $y \mid x$, perciò $x \sim y$

"$\Rightarrow$": Esistono $r, s \in R$ tali che $y = xr$ e $x = ys$.
Dunque $y = ysr$ e $y(1 - sr) = 0_R$.
Possiamo assumere $y \neq 0_R$, perciò $1_R - sr = 0_R$ e $s = r^{-1}$.
Quindi $r, s \in R^*$.

□

Esempio

$x, y \in \mathbb{Z}$ sono associati se e solo se $x = y$ oppure $x = -y$.

10.5. Lemma e definizione

Sia (R, δ) un anello euclideo e siano $a_1, \dots, a_n \in R \setminus \{0_R\}$ con $n \geq 2$.
Allora esistono

1. un elemento $d \in R$, detto **massimo comun divisore**, tale che
   (i) d è comun divisore di $a_1, \dots, a_n$:
   $$d \mid a_i \text{ per ogni } 1 \leq i \leq n$$
   (ii) Se t è un comun divisore di $a_1, \dots, a_n$, allora $t \mid d$.
2. un elemento $m \in R$, detto **minimo comune multiplo**, tale che
   (i) m è comune multiplo di $a_1, \dots, a_n$:
   $$a_i \mid m \text{ per ogni } 1 \leq i \leq n$$
   (ii) Se c è un comune multiplo di $a_1, \dots, a_n$, allora $m \mid c$.

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

Dimostrazione.
1. Sappiamo:
   - $x \mid y$ se e solo se $y \in (x)$
   - t comun divisore se e solo se $(a_1, \dots, a_n) \subset (t)$
   - d massimo comun divisore se e solo se $(a_1, \dots, a_n) = (d)$

   Infatti (i) significa che $(a_1, \dots, a_n) \subset (d)$ e (ii) significa
   $$\text{Se } (a_1, \dots, a_n) \subset (t), \text{ allora } d \in (t)$$
   Perciò (ii) significa $(d) \subset (a_1, \dots, a_n)$.
   Dunque d esiste poiché R è un dominio a ideali principali.
   Inoltre se anche d' soddisfa (i) e (ii), allora
   $$(d) = (a_1, \dots, a_n) = (d')$$
   e perciò $d \sim d'$.
2. Analogamente si vede che m è comune multiplo se $(m) \subset (a_1) \cap \dots \cap (a_n)$ ed è minimo comune multiplo se e solo se $(m) = (a_1) \cap \dots \cap (a_n)$.
   Perciò m esiste ed è unico a meno di associazione.

$\square$

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

10.6. Algoritmo euclideo

In un anello euclideo (R, δ) possiamo calcolare MCD e mcm di due elementi $a, b \in R \setminus \{0_R\}$ tramite divisione con il resto successive come segue:
Se $b \mid a$, allora $\mathrm{MCD}(a, b) = b$, $\mathrm{mcm}(a, b) = a$.
Altrimenti poniamo $r_0 = b$ ed eseguiamo

$$\begin{array}{rll} a & = r_0 q_1 + r_1 & \text{con } q_1, r_1 \in R \text{ e } \delta(r_1) < \delta(r_0) \\ r_0 & = r_1 q_2 + r_2 & \text{con } q_2, r_2 \in R \text{ e } \delta(r_2) < \delta(r_1) \\ r_1 & = r_2 q_3 + r_3 & \text{con } q_3, r_3 \in R \text{ e } \delta(r_3) < \delta(r_2) \\ \vdots & & \vdots \\ r_{n-1} & = r_n q_{n+1} + r_{n+1} & \text{con } q_{n+1} \in R \text{ e } r_{n+1} = 0_R \end{array}$$

Allora

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

Inoltre, risalendo dal basso verso l'alto troviamo coefficienti $\alpha, \beta \in R$ tali che

$$r_n = \alpha a + \beta b$$

Dimostrazione.
$(a, b) = (r_0, r_1) = (r_1, r_2) = (r_2, r_3) = \ldots = (r_n, r_{n+1}) = (r_n)$
perciò $r_n = \mathrm{MCD}(a, b)$.
Il secondo enunciato sarà mostrato più avanti.

$\square$

Esempio

Sia $K = \mathbb{Z}/3\mathbb{Z}$ e $R = K[x]$, $f = x^3 + x + 1, g = x^2 + x + 1 \in K[x]$

$$\begin{array}{rll} (x^3 + x + 1) & : (x^2 + x + 1) = & \underbrace{x + 2}_{q_1} \\ -(x^3 + x^2 + x) & & \\ \hline 2x^2 + 1 & & \\ -(2x^2 + 2x + 2) & & f = g q_1 + r_1 \\ \hline \underbrace{x + 2}_{r_1} & & \end{array}$$

$$\begin{array}{rll} (x^2 + x + 1) & : (x + 2) & = \underbrace{x + 2}_{q_2} \\ -(x^2 + 2x) & & \\ \hline 2x + 1 & & g = q_2 r_1 \\ -(2x + 1) & & r_1 = \mathrm{MCD}(f, g) = x + 2 \\ \hline r_2 = 0 & & \end{array}$$

Si ha $r_1 = f - g q_1$, quindi $\alpha = 1$, $\beta = -q_1 = 2x + 1$

10.7. Definizione

In un anello euclideo (R, δ) si dice che $a_1, \ldots, a_n \in R$ sono **coprimi** se ciascun divisore di $a_1, \ldots, a_n$ è invertibile.
Ciò equivale a $\mathrm{MCD}(a_1, \ldots, a_n) = 1_R$.

10.8. Proposizione

Sia (R, δ) un anello euclideo

1. **Identità di Bézout**
   $a, b \in R \setminus \{0_R\}$ sono *coprimi* se e solo se esistono $\alpha, \beta \in R$ tali che
   $$1_R = \alpha a + \beta b$$

2. Siano $b_1, \ldots, b_n \in R \setminus \{0_R\}$ e sia $d = \mathrm{MCD}(b_1, \ldots, b_n)$.
   Se $a_i d = b_i$ per $1 \leq i \leq n$, allora $a_1, \ldots, a_n$ sono coprimi.

3. **Lemma di Euclide**
   Siano $x, a, b \in R$. Se x e a sono coprimi e $x \mid ab$, allora $x \mid b$.

Dimostrazione.

1."⇒": $\mathrm{MCD}(a, b) = 1_R$
e l'algoritmo euclideo produce $\alpha, \beta \in R$ con $1_R = \alpha a + \beta b$.

"⇐": Se t è comun divisore di a e b, allora $t \mid 1_R$, ovvero $t \in R^*$.

2. Sia t un divisore comune di $a_1, \ldots, a_n$. Allora td è un comun divisore di $b_1, \ldots, b_n$ e pertanto $td \mid t$. Perciò esiste un $s \in R$ tale che $std = d$. Perciò $(1_R - st)d = 0_R$, dunque $1_R = st$ e $t \in R^*$.

3. Possiamo assumere $b \neq 0_R$.
   Consideriamo $t = \mathrm{MCD}(xb, ab)$. Poiché b è comun divisore di xb e ab, si ha $b \mid t$, ovvero $bq = t$ per un $q \in R$.
   Allora bq divide xb e ab, perciò q divide x e a.
   Segue che $q \in R^*$ e $b \sim t$ è massimo comun divisore di xb e ab.
   Per ipotesi x è comun divisore di xb e ab e pertanto $x \mid b$.

□

Torniamo alla

Dimostrazione di 10.6.
Vogliamo mostrare che se $d = \mathrm{MCD}(a, b)$, allora $\mathrm{mcm}(a, b) = \frac{ab}{d}$.
Scriviamo $a = a'd$ e $b = b'd$ con $a', b' \in R$. Dunque $m = a'b = ab'$ è comune multiplo di a e b.
Inoltre se c è un comune multiplo di a e b, allora esistono $s, t \in R$ tali che $c = ta = sb = ta'd = sb'd$, perciò $ta' = sb'$.
Si noti che a' e b' sono coprimi. Per il Lemma di Euclide $a' \mid s$, perciò $m = a'b \mid sb = c$.
$\square$

10.9. Definizione

Un elemento non invertibile $p \in R$ si dice **irriducibile** se possiede soltanto divisori banali, cioè se $p = xy$, allora $x \in R^*$ oppure $y \in R^*$.

Osservazione

Sia (R, δ) un anello euclideo e sia $p \in R \setminus \{0_R\}$ non invertibile.
Allora sono equivalenti i seguenti enunciati:

1. p è un elemento irriducibile
2. Se p divide il prodotto xy di due elementi $x, y \in R$, allora divide uno dei due fattori: $p \mid x$ oppure $p \mid y$
3. (p) è massimale

Dimostrazione.

(1) $\Leftrightarrow$ (3): La dimostrazione è lasciata per esercizio

(3) $\Rightarrow$ (2): L'ipotesi 3 equivale a dire che $R/(p)$ è un campo.
Se adesso $p \mid xy$, allora $xy \in (p)$ e $\overline{x} \cdot \overline{y} = \overline{xy} = \overline{0}$ in $R/(p)$.
Per ipotesi si ha $\overline{x} = \overline{0}$ oppure $\overline{y} = \overline{0}$, ovvero $x \in (p)$ oppure $y \in (p)$. Dunque $p \mid x$ oppure $p \mid y$.

(2) $\Rightarrow$ (1): Se $p = xy$, allora per ipotesi $p \mid x$ oppure $p \mid y$, perciò (poiché $x \mid p$ e $y \mid p$) si ha

$$p \sim x \quad \text{oppure} \quad p \sim y$$

Nel primo caso otteniamo $y \in R^*$, nel secondo $x \in R^*$.

$\square$

Osservazione

Gli elementi irriducibili di $\mathbb{Z}$ sono esattamente i numeri primi.
Abbiamo

Teorema Fondamentale dell'Aritmetica

Ogni numero $a \in \mathbb{Z} \setminus \{0, 1, -1\}$ è prodotto di numeri primi e questa scomposizione è unica a meno dell'ordine e segno dei fattori.

10.10. Teorema

In un anello euclideo (R, δ) ogni elemento $a \in R \setminus (\{0_R\} \cup R^*)$ può essere scritto come prodotto di elementi irriducibili, e questa scomposizione è unica a meno dell'ordine dei fattori e di associazione.
Più precisamente

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

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

Dimostrazione.

1. Osserviamo innanzitutto che ogni catena ascendente di ideali di R

   $$I_1 \subset I_2 \subset I_3 \subset \cdots$$

   è stazionaria, cioè esiste $n \in \mathbb{N}$ tale che

   $$I_n = I_{n+1} = I_{n+2} = \cdots$$

   Un anello con tale proprietà si dice *noetheriano.*
   Infatti $I = \sum_{i \in \mathbb{N}} I_i$ è un ideale principale, quindi $I = (a)$ per un $a \in I$ con $a = \sum_{i=1}^{n} a_i$ dove $n \in \mathbb{N}$, $a_i \in I_i$.
   In particolare $a_i \in I_n$ per ogni $1 \leq i \leq n$, perciò $a \in I_n$. Dunque

   $$I = I_n = I_{n+1} = \cdots$$

2. Poiché R è noetheriano, ogni insieme non vuoto $\mathcal{S}$ di ideali contiene un elemento massimale, ovvero esiste un $I \in \mathcal{S}$ che non è contenuto propriamente in un elemento di $\mathcal{S}$.
   Altrimenti potremmo costruire una catena ascendente di ideali di $\mathcal{S}$ che non è stazionaria.

3. Supponiamo adesso che esistano elementi in $R \setminus (\{0_R\} \cup R^*)$ che non soddisfano (i). Sia $\mathcal{S}$ l'insieme degli ideali generati da tali elementi e sia $I = (a)$ un elemento massimale di $\mathcal{S}$. Per ipotesi a non è né nullo, né invertibile, né irriducibile.
   Allora esistono $x, y \in R$ non invertibili tali che $a = xy$.
   Poiché $I \subsetneq (x)$ e $I \subsetneq (y)$, segue che $(x) \notin \mathcal{S}$ e $(y) \notin \mathcal{S}$, perciò x e y sono prodotto di elementi irriducibili. Ma allora anche a è prodotto di irriducibili. $\lightning$

4. Mostriamo (ii) per induzione su n.

   <u>$n = 1$</u>:
   Se $a = p_1 = q_1 \cdot \ldots \cdot q_m$, allora $m = 1$ e $p_1 = q_1$.

   <u>$n > 1$</u>:
   $p_n \mid q_1 \cdot \ldots \cdot q_m$, perciò p_n divide uno dei fattori, e dopo averli eventualmente riordinati, possiamo assumere $p_n \mid q_m$. Dunque $q_m = p_n r$ con $r \in R^*$ e $q_m \sim p_n$. Abbiamo quindi

   $$p_1 \cdot \ldots \cdot p_n = q_1 \cdot \ldots \cdot q_{m-1} \cdot p_n \cdot r$$

   perciò

   $$p_1 \cdot \ldots \cdot p_{n-1} = q_1 \cdot \ldots \cdot (q_{m-1} r)$$

   Per l'ipotesi induttiva segue che, $n - 1 = m - 1$, e dopo aver eventualmente riordinato i fattori,

   $$p_i \sim q_i \text{ per ogni } 1 \leq i < n$$

$\square$

Parte III.

Polinomi

Riassunto

Abbiamo visto che l'anello $K[x]$ su un campo K ha le seguenti proprietà:

1. I polinomi invertibili sono esattamente i polinomi costanti non nulli, ovvero di grado 0.
2. Due polinomi $f, g \in K[x]$ sono associati se e solo se $f = \alpha g$ per un $\alpha \in K \smallsetminus \{0_K\}$.
3. Due polinomi $f, g \in K[x]$ possiedono sempre un MCD e mcm, unici a meno di una costante non nulla.
4. Ogni polinomio $f \in K[x]$ di grado $n > 0$ è prodotto di polinomi irriducibili, e questa scomposizione è unica a meno dell'ordine e di costanti non nulle.

11. Zeri di polinomi

Sia K un campo

11.1. Proposizione

Per un polinomio $f \in K[x]$ sono equivalenti i seguenti enunciati:

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

Dimostrazione.

(1) $\Leftrightarrow$ "(f) è un ideale massimale" $\Leftrightarrow$ (3) (da verificare per esercizio)

(1) $\Leftrightarrow$ (2)

$f \neq 0$ e non invertibile $\Leftrightarrow n > 0$.
Se f è irriducibile e $f = gh$, allora $\deg g = 0$, oppure $\deg h = 0$, ovvero $\deg h = n$ oppure $\deg g = n$.
Viceversa se vale (2) e $f = gh$, uno dei fattori ha grado n e l'altro ha grado 0, perciò è invertibile.

$\square$

11.2. Definizione

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

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

e diciamo che α è uno **zero** (o una *radice*) di f, quando $f(\alpha) = 0_R$.

11.3. Teorema di Ruffini

Per $\alpha \in K$, l'applicazione

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

è un omomorfismo suriettivo con nucleo $\ker \varepsilon_\alpha = (x - \alpha)$.
Dunque α è uno zero di $f \in K[x]$ se e solo se $x - \alpha \mid f$. Inoltre $K[x]/(x - \alpha) \cong K$.

Dimostrazione.

- omomorfismo:

$$\varepsilon_\alpha(f \dot{+} g) = \varepsilon_\alpha(f) \dot{+} \varepsilon_\alpha(g)$$
$$\varepsilon_\alpha(1_{K[x]}) = 1_K$$

- suriettivo:
  Se $a \in K$, allora il polinomio costante $f = a$ soddisfa $\varepsilon_\alpha(f) = a$.

- $\ker \varepsilon_\alpha$:
  Ovviamente $(x - \alpha) \subseteq \ker \varepsilon_\alpha$.
  Viceversa se $f \in \ker \varepsilon_\alpha$, eseguiamo la divisione

$$f = q(x - \alpha) + r \qquad \text{dove } q, r \in K[x] \text{ e } r = 0 \text{ oppure } \deg r < 1$$

  dunque r è costante.
  Allora $r = f - q(x - \alpha)$ soddisfa

$$r(\alpha) = f(\alpha) - q(\alpha)(\alpha - \alpha) = 0$$

  e pertanto $r = 0$. Dunque $f \in (x - \alpha)$.

$K[x]/(x - \alpha) \cong K$ è un'applicazione del Teorema Fondamentale dell'Omomorfismo.

□

11.4. Corollario

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

Dimostrazione.
Per induzione su n.

$\underline{n = 0}$:

f è costante non nullo e quindi non ha zeri.

$\underline{n - 1 \to n}$:

Se $\alpha \in K$ è uno zero di f, allora per 11.3 esiste $g \in K[x]$ tale che $f = (x - \alpha)g$ e $\deg g = n - 1$. Per l'ipotesi induttiva di g ha al più $n - 1$ zeri in K, quindi f ne ha al più n.

□

11.5. Proposizione

1. Ogni polinomio $f = a_0 + a_1 x \in K[x]$ di grado 1 è irriducibile con unico zero $\alpha = -a_1^{-1} a_0$.
2. Se $f \in K[x]$ è irriducibile di grado $n > 1$, allora non possiede zeri.
3. Se $f \in K[x]$ ha grado $n \in \{2, 3\}$, f è irriducibile se e solo se non ammette zeri.

Dimostrazione.

1. $f = a_1(x - \alpha) \sim (x - \alpha)$ è irriducibile poiché lo è $x - \alpha$ per 11.3 e 11.1, e α è il suo unico zero.
2. Se α fosse uno zero di f, avremmo una scomposizione non banale
$$f = \underset{\substack{\uparrow \\ \text{grado } 1<n}}{(x-\alpha)} \; \underset{\substack{\nwarrow \\ \text{grado } n-1}}{g}$$
3. "$\Rightarrow$" : Per (2)
   "$\Leftarrow$" : Sia $f = gh$.

$$\begin{array}{lcc l}
 & \deg g & \deg h & \\
\deg f = 2 & \cancel{1} & \cancel{1} & \text{poiché } f \text{ non ha zeri, si veda (1)} \\
 & 0 & 2 & \\
\deg f = 3 & \cancel{1} & \cancel{2} & \text{si veda sopra} \\
 & 0 & 3 &
\end{array}$$

Quindi g oppure h devono avere grado 0.

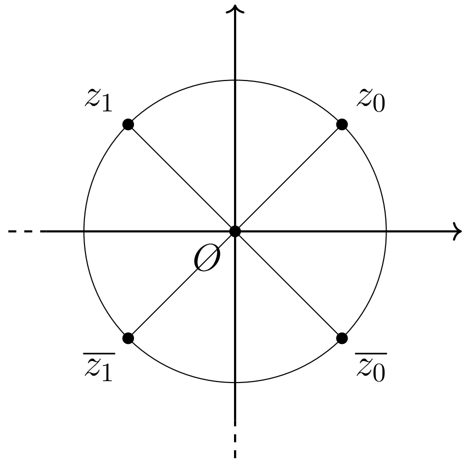
□

11.6. Esempi

1. **Teorema Fondamentale dell'Algebra**
   I polinomi irriducibili in $\mathbb{C}[x]$ sono esattamente i polinomi di grado 1 (per 11.5.(2)).
   Ogni polinomio $f \in \mathbb{C}[x]$ è di forma
$$f = a(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$$
   con $n \in \mathbb{N}_0$, $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$.
2. Sia $f = x^n - a \in \mathbb{C}[x]$. Gli zeri di f sono le radici n-esime di a. Ricordiamo:
   Se $a = r(\cos\alpha + i \sin\alpha)$, allora gli zeri sono
$$z_k = \sqrt[n]{r}\left(\cos\frac{\alpha + 2k\pi}{n} + i \sin\frac{\alpha + 2k\pi}{n}\right), k = 0, 1, \ldots, n-1$$

3. $f = x^4 + 1 \in \mathbb{R}[x] \subset \mathbb{C}[x]$ (caso particolare $n = 4, a = -1 = \cos\pi + i\sin\pi$)
   Gli zeri di f sono

$$z_0 = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$$
$$z_1 = \cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4} = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$$
$$\overline{z_0} = \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$$
$$\overline{z_1} = -\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$$



   Quindi in $\mathbb{C}[x]$ possiamo scrivere

$$f = \underbrace{(x - z_0)(x - \overline{z_0})}_{g}\underbrace{(x - z_1)(x - \overline{z_1})}_{h}$$

$$\begin{aligned} g &= \left(\left(x - \frac{\sqrt{2}}{2}\right) - i\frac{\sqrt{2}}{2}\right)\left(\left(x - \frac{\sqrt{2}}{2}\right) + i\frac{\sqrt{2}}{2}\right) \\ &= \left(x - \frac{\sqrt{2}}{2}\right)^2 - \left(i\frac{\sqrt{2}}{2}\right)^2 \\ &= x^2 - \sqrt{2}x + \frac{1}{2} + \frac{1}{2} = x^2 - \sqrt{2} + 1 \in \mathbb{R}[x] \end{aligned}$$
$$h = x^2 + \sqrt{2}x + 1 \in \mathbb{R}[x]$$

   Quindi f **non** è irriducibile in $\mathbb{R}[x]$ pur non avendo zeri in $\mathbb{R}$.

4. I polinomi irriducibili in $\mathbb{R}$ sono i polinomi di grado 1 e i polinomi $f = a_0 + a_1x + a_2x^2 \in \mathbb{R}[x]$ di grado 2 con discriminante $\Delta = a_1^2 - 4a_0a_2 < 0$.
   Infatti se f non possiede zeri in $\mathbb{R}$ e ha grado > 1, allora

$$f = \underbrace{(x - z)(x - \overline{z})}_{\in\mathbb{R}[x] \text{ come in (3)}}\, g$$

   e se f è irriducibile, allora $\deg g = 0$ e $\deg f = 2$.
   Viceversa, i polinomi descritti sopra sono irriducibili per 11.5. Quindi ogni polinomio in $\mathbb{R}[x]$ è prodotto di polinomi di grado al più 2.

5. $f = x^2 + x + 1$ è irriducibile in $\mathbb{Z}/2\mathbb{Z}[x]$ (perché non ha zeri).
   In $\mathbb{Z}/3\mathbb{Z}[x]$ si ha $f = x^2 - 2x + 1 = (x - 1)^2$ riducibile.
   $g = x^4 + x^2 + 1 = (x^2 + x + 1)^2$ in $\mathbb{Z}/2\mathbb{Z}[x]$ è riducibile , pur non avendo zeri.

12. Criteri di divisibilità

12.1. Osservazione

Per ogni $0 \neq f \in \mathbb{Q}[x]$ esiste un $\alpha \in \mathbb{Q}$ tale che $\alpha f \in \mathbb{Z}[x]$ con coefficienti coprimi.
Un polinomio $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ per il quale $a_0, \ldots, a_n$ sono coprimi si dice **primitivo**.
Per esempio se $f = \frac{2}{3} + \frac{4}{7}x^2$, allora scegliamo $\alpha = \frac{21}{2}$ per ottenere $\alpha f = 7 + 6x^2$.
Ovviamente f è irriducibile in $\mathbb{Q}[x]$ se e solo se lo è αf.
Vedremo in 12.5 che basterà esaminare l'irriducibilità in $\mathbb{Z}[x]$, dunque $f \in \mathbb{Q}[x]$ è irriducibile se e solo se αf è irriducibile in $\mathbb{Z}[x]$.

Esempi

1. Ogni polinomio **monico** (ovvero con coefficiente direttivo 1) è primitivo

2. Ogni polinomio irriducibile in $\mathbb{Z}[x]$ di grado $n > 0$ è primitivo: altrimenti se d è MCD dei coefficienti di f, allora possiamo scrivere $f = df'$ con $\deg f' = n > 0$ e otteniamo una scomposizione di f in fattori non invertibili.

3. $2 \in \mathbb{Z}[x]$ è irriducibile ma non è primitivo.

4. i polinomi irriducibili in $\mathbb{Z}[x]$ sono
   - i polinomi costanti p, dove p è un numero primo
   - i polinomi primitivi di grado $n > 0$ che non sono prodotto di due polinomi di grado strettamente inferiore

12.2. Riduzione modulo p

Sia p un numero primo e

$$\begin{aligned} \rho : \mathbb{Z}[x] &\longrightarrow \mathbb{Z}/p\mathbb{Z}[x] \\ f = \sum_{i=0}^{n} a_i x^i &\longmapsto \rho(f) = \sum_{i=0}^{n} \overline{a_i} x^i \end{aligned}$$

Allora

1. ρ è un epimorfismo con nucleo

$$\begin{aligned} \ker \rho &= \{f = \sum_{i=0}^{n} a_i x^i \mid p \mid a_i \text{ per ogni } 1 \leq i \leq n\} \\ &= \{f = \sum_{i=0}^{n} a_i x^i \mid a_i \in p\mathbb{Z}\} = p\mathbb{Z}[x] \end{aligned}$$

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

Dimostrazione.

2. f come nell'enunciato e sia $\rho(f)$ irriducibile. Mostriamo che f è irriducibile.
   Chiaramente f non è invertibile. Siano $g, h \in \mathbb{Z}[x]$ tali che $f = gh$.
   Allora $\rho(f) = \rho(g)\rho(h) \in \mathbb{Z}/p\mathbb{Z}[x]$ e per ipotesi $\rho(f)$ ha grado n. Poiché $\rho(f)$ è irriducibile, uno dei suoi fattori, poniamo $\rho(h)$, ha grado n.
   Dunque $n = \deg \rho(h) \leq \deg h$, perciò $g = a$ è costante con $f = a \cdot h$.
   Dunque a è comun divisore dei coefficienti di f.
   Concludiamo che $g = a \in \{1, -1\}$ è invertibile.

□

12.3. Criterio di Eisenstein

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

1. p non divide a_n

2. p divide $a_0, \ldots, a_{n-1}$

3. p^2 non divide a_0

Dimostrazione.
Abbiamo che $\rho(f) = \overline{a_n}x^n \neq 0$.
Certamente f non è invertibile. Siano $g, h \in \mathbb{Z}[x]$ tali che $f = gh$.
Scriviamo $g = \sum_{i=0}^{m} b_i x^i$ e $h = \sum_{i=0}^{r} c_i x^i$ e notiamo che p divide b_0 oppure c_0, ma non entrambi, ciò segue dal fatto che $a_0 = b_0 c_0$ e $\overline{0} = \overline{a_0} = \overline{b_0} \cdot \overline{c_0}$, insieme all'ipotesi (3).
Supponiamo $p \mid c_0$, allora $\rho(g) = \underset{\neq 0}{\overline{b_0}} + \overline{b_1}x + \ldots + \overline{b_m}x^m$ divide $\rho(f) = \overline{a_n}x^n$ e perciò $\rho(g) = \overline{b_0}$ dev'essere costante.
La dimostrazione si conclude con 12.2.

$\square$

12.4. Lemma di Gauss

Se $f, g \in \mathbb{Z}[x]$ sono primitivi, allora lo è anche fg.

Dimostrazione.
Supponiamo che esista un numero primo p che divide tutti i coefficienti di fg, ed eseguiamo la riduzione modulo p:

$$\overline{0} = \rho(fg) = \rho(f)\rho(g) \text{ in } \mathbb{Z}/p\mathbb{Z}[x]$$

Quindi uno dei fattori, poniamo $\rho(f)$, è polinomio nullo in $\mathbb{Z}/p\mathbb{Z}[x]$, ma allora $f \in \ker \rho = p\mathbb{Z}[x]$ e p divide tutti i coefficienti di f ↯ (f è primitivo).

$\square$

12.5. Proposizione

Un polinomio primitivo $0 \neq f \in \mathbb{Z}[x]$ è irriducibile in $\mathbb{Z}[x]$ se e solo se lo è in $\mathbb{Q}[x]$.

Dimostrazione.

"$\Rightarrow$": Sia f irriducibile in $\mathbb{Z}[x]$ e siano $g, h \in \mathbb{Q}[x]$ tali che $f = gh$.
Per 12.1 esistono $\alpha, \beta \in \mathbb{Q}$ tali che $\alpha g, \beta h \in \mathbb{Z}[x]$ siano primitivi.
Per il Lemma di Gauss anche $\alpha\beta f = \alpha g \cdot \beta h = f' \in \mathbb{Z}[x]$ è primitivo.
Abbiamo $f = \frac{1}{\alpha\beta} f'$. Scriviamo $\frac{1}{\alpha\beta} = \frac{m}{n}$ con $m, n \in \mathbb{Z}$ coprimi.
Otteniamo $nf = mf'$, perciò se $f' = \sum_{i=0}^{l} a_i x^i$, allora n divide $ma_0, ma_1, \ldots, ma_l$ e per il Lemma di Euclide m divide $a_0, \ldots, a_l$. Poiché f' è primitivo concludiamo $n \in \{-1, 1\}$. Analogamente vediamo che $m \in \{-1, 1\}$, quindi $\frac{1}{\alpha\beta} \in \{-1, 1\}$.
Perciò $f = (\alpha g)(\beta h)$ oppure $f = -(\alpha g)(\beta h)$ in $\mathbb{Z}[x]$. Per ipotesi uno dei fattori, poniamo αg, dev'essere invertibile, ovvero $\alpha g \in \{-1, 1\}$.
Concludiamo che $g \in \mathbb{Q}[x]$ è costante non nullo, perciò è invertibile in $\mathbb{Q}[x]$.

"$\Leftarrow$": Questa implicazione è lasciata per esercizio.

$\square$

12.6. Esempi

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

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

   - non ha zeri
     Possibili divisori di grado 2:

x^2	NO: ha uno zero
x^2+1	NO: ha uno zero
x^2+x	NO: ha uno zero
x^2+x+1	irriducibile

     $$\begin{array}{r l}
     (x^4 + x + 1) & : (x^2 + x + 1) = \quad x^2 + x \\
     -(x^4 + x^3 + x^2) & \\
     \hline
     x^3 + x^2 + x + 1 & \\
     -(x^3 + x^2 + x) & \\
     \hline
     1 &
     \end{array}$$

     Quindi nemmeno $x^2 + x + 1$ divide $\rho(f)$
   - non ha divisori di grado 2

   Concludiamo che $\rho(f)$ è irriducibile in $\mathbb{Z}/2\mathbb{Z}[x]$. Per 12.2 segue che f è irriducibile in $\mathbb{Z}[x]$ (e in $\mathbb{Q}[x]$)

3. $f = x^n - a \in \mathbb{Z}[x]$ con $n \in \mathbb{N}$.
   Se esiste un numero primo p tale che $p \mid a$ ma p^2 non divide a (ad esempio se a è il prodotto di due primi distinti), allora f è irriducibile in $\mathbb{Z}[x]$ (e in $\mathbb{Q}[x]$) per il Criterio di Eisenstein.

12.7. Sostituzione

Sia K un campo e sia $f = \sum_{i=0}^{n} a_i x^i \in k[x]$.
Sostituiamo x con $a + bx$, dove $a, b \in K$ e $b \neq 0$. Otteniamo il polinomio

$$\tilde{f} = \sum_{i=0}^{n} a_i (a + bx)^i \in K[x]$$

Allora f è irriducibile se e solo se lo è $\tilde{f}$.

Dimostrazione.
Si noti che

$$\begin{array}{ccc} K[x] & \longrightarrow & K[x] \\ f & \longmapsto & \tilde{f} \end{array}$$

è un isomorfismo di anelli con inversa data dalla sostituzione di x con $b^{-1}x - b^{-1}a$.

$\square$

12.8. Esempio

Per ogni numero primo p il polinomio $x^{p-1} + x^{p-2} + \ldots + x + 1 \in \mathbb{Z}[x]$ è irriducibile in $\mathbb{Z}[x]$ e $\mathbb{Q}[x]$.

Dimostrazione.
Sostituzione $x \mapsto x + 1$ (da completare per esercizio).

$\square$

Parte IV.

Campi

13. Estensioni algebriche

13.1. Lemma e definizione

Se K, F sono campi e $K \subset F$ è un sottocampo, diciamo che F è un'**estensione** di K. In tal caso F è uno spazio vettoriale su K tramite la moltiplicazione per scalari

$$K \times F \to F, \quad (\alpha, x) \mapsto \alpha x$$

La dimensione di F su K si dice *grado dell'estensione* e si indica con

$$[F : K] = \dim_K F$$

L'estensione $K \subset F$ è **finita** se $[F : K] < \infty$

13.2. Proposizione

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

$$\begin{array}{rcl} \varphi : K & \longrightarrow & F := K[x]/(f) \\ a & \longmapsto & \overline{a} = a + (f) \end{array}$$

è un monomorfismo. Quindi $K \subset F$ è un'estensione di campi.
Si ha $[F : K] = n$ e $\{\overline{1}, \overline{x}, \overline{x}^2, \dots, \overline{x}^{n-1}\}$ è una base di F su K.

Dimostrazione.
F è un campo per 11.1.

$$\varphi(a \dot{+} b) = \overline{a \dot{+} b} = \overline{a} \dot{+} \overline{b} = \varphi(a) \dot{+} \varphi(b)$$

$$\varphi(1_K) = \overline{1_K} = 1_F$$

φ è un omomorfismo iniettivo poiché K è un campo.
Resta da verificare che $\mathcal{B} = \{\overline{1}, \overline{x}, \dots, \overline{x}^{n-1}\}$ è una K-base.

- Si noti che in ${}_K F$ abbiamo per $a \in K$ e $g = \sum_{i=0}^{m} a_i x^i \in K[x]$

$$a \cdot \overline{g} = \overline{a} \cdot \overline{g} = \overline{ag} = \overline{a \sum_{i=0}^{m} a_i x^i} = \overline{\sum_{i=0}^{m} a a_i x^i} = \sum_{i=0}^{m} \overline{a a_i x^i} = \sum_{i=0}^{m} a a_i \overline{x}^i$$

- $\mathcal{B}$ insieme di generatori di ${}_K F$:
  Sia $g = \sum_{i=0}^{m} a_i x^i \in K[x]$ ed eseguiamo la divisione con il resto:

  $$g = qf + r \qquad \text{dove } q, r \in K[x] \text{ e } r = 0 \text{ oppure } \deg r < n$$

  Dunque $r = \sum_{i=0}^{n-1} b_i x^i$ e

  $$\overline{g} = \overline{qf + r} = \overline{r} = \overline{\sum_{i=0}^{n-1} b_i x^i} = \sum_{i=0}^{n-1} b_i \overline{x}^i$$

- $\mathcal{B}$ è linearmente indipendente:
  Siano $a_0, \ldots, a_{n-1} \in K$ tali che $a\overline{1} + a_1\overline{x} + \ldots + a_{n-1}\overline{x}^{n-1} = \overline{0}$.
  Allora il polinomio $g = \sum_{i=0}^{n-1} a_i x^i \in K[x]$ soddisfa

  $$\overline{g} = \overline{\sum_{i=0}^{n-1} a_i x^i} = \sum_{i=0}^{n-1} a_i \overline{x}^i = \overline{0}$$

  Perciò $g \in (f)$, ovvero $f \mid g$.
  Allora esiste un $q \in K[x]$ tale che $g = fq$, e da qui segue che $\deg g = \deg f + \deg q$.
  Ma $\deg g \leq n - 1 < \deg f = n$. Perciò $g = q = 0$ e $a_0 = \ldots = a_{n-1} = 0$.

□

13.3. Esempi

1. $K = \mathbb{R}$, $f = x^2 + 1$
   Allora $F = \mathbb{R}[x]/(x^2 + 1)$ è uno spazio vettoriale su $\mathbb{R}$ con base $\{\overline{1}, \overline{x}\}$. Si noti che in F

   $$\overline{x}^2 + 1 = \overline{f} = \overline{0}$$

   perciò $\overline{x}^2 = -\overline{1}$ e si ha un isomorfismo di campi

   $$\begin{array}{rcl} F & \longrightarrow & \mathbb{C} \\ a\overline{1} + b\overline{x} & \longmapsto & a + ib \end{array}$$

2. $K = \mathbb{Z}/2\mathbb{Z}$, $f = x^2 + x + 1$
   $F = K[x]/(f)$ ha base $\overline{1}, \overline{x}$ su K, quindi $F = \{\overline{0}, \overline{1}, \overline{x}, \overline{x} + \overline{1}\}$ dove $\overline{x} + \overline{1} = \overline{x}^2$, poiché $\overline{x^2 + x + 1} = \overline{x}^2 + \overline{x} + \overline{1} = \overline{0}$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{1}+\overline{x}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{1}+\overline{x}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{1}+\overline{x}$	$\overline{x}$
$\overline{x}$	$\overline{x}$	$\overline{1}+\overline{x}$	$\overline{0}$	$\overline{1}$
$\overline{1}+\overline{x}$	$\overline{1}+\overline{x}$	$\overline{x}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x}^2$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x}^2$
$\overline{x}$	$\overline{0}$	$\overline{x}$	$\overline{x}^2$	$\overline{1}$
$\overline{x}^2$	$\overline{0}$	$\overline{x}^2$	$\overline{1}$	$\overline{x}$

$$\overline{x}\cdot\overline{x}^2 = \overline{x}(\overline{1}+\overline{x}) = \overline{x}+\overline{x}^2 = \overline{1}$$

In $F[X]$ si ha

$$(X-\overline{x})(X-\overline{x}^2) = X^2-(\overline{x}+\overline{x}^2)X+\overline{x}^2 = X^2+X+\overline{1} = f$$

13.4. Teorema (Kronecker)

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

Dimostrazione.
Passando eventualmente ad un suo fattore irriducibile, possiamo assumere che f sia irriducibile.
Consideriamo $F = K[x]/(f)$ che è un'estensione di grado $\deg f$. Poniamo $\alpha = \overline{x}$.
Se $f = \sum_{i=0}^{n} a_i x^i$ otteniamo

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

□

13.5. Definizione

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

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

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

   si dice **aggiunzione** di A a K.

2. Un elemento $\alpha \in F$ si dice **algebrico** se esiste $f \in K[x]$ con $f \neq 0$ e $f(\alpha) = 0$.
   Altrimenti α si dice **trascendente** su K.

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

Osservazioni

1. Ogni estensione finita $K \subset F$ è algebrica:
   Se $[F : K] = n$ e $\alpha \in F$, allora $\{1, \alpha, \ldots, \alpha^n\}$ è un insieme linearmente dipendente. Dunque esistono $a_0, a_1, \ldots, a_n \in K$, non tutti nulli tali che

   $$\sum_{i=0}^{n} a_i \alpha^i = 0$$

   In altre parole , α è uno zero del polinomio non nullo $g = \sum_{i=0}^{n} a_i x^i \in K[x]$.

2. In particolare, $\alpha \in F$ è algebrico su K se e solo se $[K(\alpha) : K] < \infty$.
   Per "$\Rightarrow$" si veda:

13.6. Lemma e definizione

Sia $K \subset F$ un'estensione di campi e sia $\alpha \in F$ un elemento algebrico su K. Allora:

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

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

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

Dimostrazione.

1. Consideriamo l'omomorfismo

   $$\varepsilon = \varepsilon_\alpha : K[x] \longrightarrow F, \quad h \mapsto h(\alpha)$$

   non è iniettivo, per ipotesi su α, quindi esiste un $f \neq 0$ tale che $\ker \varepsilon = (f)$.
   Possiamo assumere che f sia monico (altrimenti consideriamo il polinomio associato $a_n^{-1} f$). Poiché $f \in \ker \varepsilon$, abbiamo $f(\alpha) = 0$.
   Resta da verificare l'irriducibilità.
   Si ha $n = \deg f > 0$. Siano $g, h \in K[x]$ tali che $f = gh$.
   Allora $0 = f(\alpha) = g(\alpha) \cdot h(\alpha)$, perciò uno dei fattori, poniamo $g(\alpha) = 0$.
   Ma allora $g \in \ker \varepsilon = (f)$, perciò $f \mid g$ e $\deg g = n$.
   Unicità di f: se anche f' soddisfa l'enunciato, allora poiché $f(\alpha) = f'(\alpha) = 0$, si ha $f \sim f'$ ed essendo entrambi monici segue $f = f'$.

2. $g(\alpha) = 0 \Leftrightarrow g \in \ker \varepsilon = (f) \Leftrightarrow f \mid g$

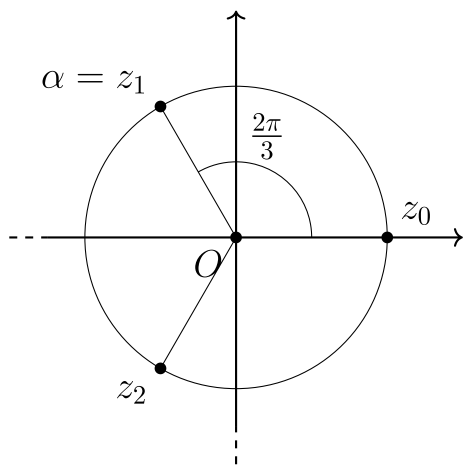
3. Poiché (f) è il nucleo di $\varepsilon : K[x] \to F$, si ha $K[x]/(f) \cong \operatorname{im}\varepsilon$.
   Si noti che $\operatorname{im}\varepsilon$ è un sottocampo di F che contiene $K = \varepsilon(K)$ e $\alpha = \varepsilon(x)$, quindi $K(\alpha) \subseteq \operatorname{im}\varepsilon$.
   D'altra parte $K(\alpha)$ contiene tutti gli elementi di forma $\sum_{i=0}^{m} a_i\alpha^i = \varepsilon(\sum_{i=0}^{m} a_i x^i)$, perciò $K(\alpha) = \operatorname{im}\varepsilon$. Dunque

$$\begin{array}{rcl} K[x]/(f) & \underset{\overline{\varepsilon}}{\cong} & K(\alpha) \\ \overline{x} & \longmapsto & \alpha \\ \underbrace{\{\overline{1}, \overline{x}, \dots, \overline{x}^{n-1}\}}_{\text{base}} & \longleftrightarrow & \underbrace{\{1, \alpha, \dots, \alpha^{n-1}\}}_{\text{base di } K(\alpha)} \end{array}$$

□

13.7. Esempi

1. Il polinomio minimo di i in $\mathbb{R}$ è $x^2 + 1$
2. Il polinomio minimo di $\sqrt{2}$ su $\mathbb{Q}$ è $x^2 - 2$
3. In 13.3(2) il polinomio minimo di $\alpha = \overline{x} \in F$ 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 uno zero di $x^3 - 1 = (x+1)(x^2 + x + 1)$, perciò il polinomio minimo di α è $x^2 + x + 1$.



13.8. Lemma del grado

Sia $K \subset F$ un'estensione finita e sia L un *campo intermedio* (cioè $K \subset L$ e $L \subset F$ sono estensioni di campi). Allora

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

Dimostrazione.
Sia $\{\alpha_1, \ldots, \alpha_n\}$ una base di F su L e sia $\{\beta_1, \ldots, \beta_m\}$ una base di L su K.
Allora $\{\alpha_i \beta_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}$ è una base di F su K.

□

13.9. Corollario

Sia $K \subset F$ un'estensione

1. Se $[F : K]$ è primo, non esistono campi intermedi propri.
2. $[F : K] < \infty \Leftrightarrow$ esistono elementi algebrici $\alpha_1, \ldots, \alpha_n$ su K tali che
$$F = K(\alpha_1, \ldots, \alpha_n)$$
3. Sia $K \subset L \subset F$ un campo intermedio.
Allora $K \subset F$ è algebrico se e solo se lo sono $K \subset L$ e $L \subset F$.
4. Sia $\overline{K}$ l'insieme di tutti gli elementi di F che sono algebrici su K.
Allora $K \subset \overline{K}$ è un'estensione algebrica, detta *chiusura algebrica* di K.

Dimostrazione.

1. Se $K \subset L \subset F$, allora
$$[F : K] = [F : L][L : K]$$
e $[F : L]$ o $[L : K]$ è pari a 1 e $F = L$ oppure $L = K$.
2. "$\Rightarrow$": Se $\{\alpha_1, \ldots, \alpha_n\}$ è una base di F su K, allora ogni elemento di F appartiene a $K(\alpha_1, \ldots, \alpha_n)$, quindi $F = K(\alpha_1, \ldots, \alpha_n)$.
"$\Leftarrow$": Per induzione su n
<u>$n = 1$</u>
Se $F = K(\alpha)$ con α algebrico su K, allora $[F : K] < \infty$ per 13.5.
<u>$n \to n + 1$</u>
Sia $K \subset L \subset F$ con $L = K(\alpha_1, \ldots, \alpha_n)$. Per ipotesi induttiva $[L : K] < \infty$. Inoltre $F = L(\alpha_{n+1})$ e α_{n+1} è algebrico su L, quindi $[F : L] < \infty$, perciò $[F : K] < \infty$ per 13.8

3. "$\Rightarrow$": ✓

   "$\Leftarrow$": Sia $\alpha \in F$ e sia $f = \sum_{i=0}^{n} a_i x^i \in L[x]$ il suo polinomio minimo su L. Ovviamente α è anche algebrico su $L' = K(a_0, \ldots, a_n)$.
   Perciò $L' \subset L'(\alpha)$ è un'estensione finita.
   Inoltre $a_0, \ldots, a_n \in L$ sono algebrici su K, quindi $[L' : K] < \infty$ per (2).
   Per il Lemma del Grado, segue che $[L'(\alpha) : K][L' : K] < \infty$.
   Per 13.5 concludiamo $K \subset L'(\alpha)$ è algebrica e in particolare α è algebrico su K.

4. Dobbiamo mostrare che $\overline{K} \subset F$ è un sottocampo.
   Siano $\alpha, \beta \in \overline{K}$. Per (2) l'estensione $K \subset K(\alpha, \beta)$ è finita e pertanto algebrica.
   Quindi $\alpha + \beta$, $\alpha\beta$ sono algebrici su K, ovvero $\alpha + \beta, \alpha\beta \in \overline{K}$.

□

13.10. Esempio

Un'estensione algebrica di grado infinito: $\mathbb{Q} \subset \overline{\mathbb{Q}}$.
Sia $n \in \mathbb{N}$ e sia p un numero primo, allora $\sqrt[n]{p} \in \overline{\mathbb{Q}}$ con polinomio minimo $x^n - p$ su $\mathbb{Q}$, perciò $\mathbb{Q} \subset \mathbb{Q}(\sqrt[n]{p})$ è un'estensione di grado n (per 12.6 e 13.6).
Per il Lemma del Grado, segue che $\mathbb{Q} \subset \overline{\mathbb{Q}}$ non può essere finita.

14. Campi di riducibilità completa

14.1. Teorema e definizione

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

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

F è detto **campo di riducibilità completa** (**crc**) oppure *campo di spezzamento* di f su K.

Dimostrazione.
Per induzione su n.

$\underline{n = 1}$:
$f = a(x - \alpha) \in K[x]$ e $F = K = K(\alpha)$

$\underline{n \to n + 1}$:
Per il Teorema di Kronecker esiste $K \subset F'$ di grado $[F' : K] \leq n + 1$ dove f possiede uno zero $\alpha = \alpha_{n+1}$. Per il Teorema di Ruffini in $F'[x]$ si ha

$$f = g(x - \alpha_{n+1}) \text{ con } g \in F'[x] \text{ di grado } n.$$

Per l'ipotesi induttiva esiste $F' \subset F$ di grado $[F : F'] \leq n!$ tale che

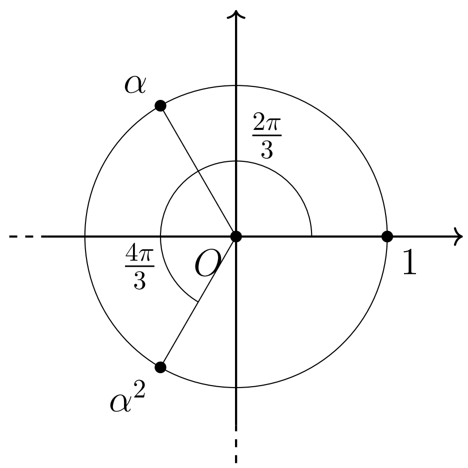
$$q = (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n) \text{ con } a \in K \text{ e } \alpha_1, \ldots, \alpha_n \in F.$$

Quindi $f = a(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_{n+1})$ e $[F : K] \leq n!(n + 1) = (n + 1)!$.
Se poniamo $F = K(\alpha_1, \ldots, \alpha_n)$ vale anche (2).

$\square$

14.2. Esempi

1. Il crc di $f = x^3 - 1$ su $\mathbb{Q}$:
   $f = (x-1)(x^2+x+1)$ ha gli zeri $1, \alpha = -\frac{1}{2} + i\frac{1}{2}\sqrt{3}, \overline{\alpha} = \alpha^2$.

   Perciò $F = \mathbb{Q}(1, \alpha, \alpha^2) = \mathbb{Q}(\alpha)$ e $[F : \mathbb{Q}] = \deg x^2 + x + 1 = 2$.

2. Il crc di $f = x^3 - 2$ su $\mathbb{Q}$:
   f ha zeri $\sqrt[3]{2}, \alpha\sqrt[3]{2}, \alpha^2\sqrt[3]{2}$. Perciò $F = \mathbb{Q}(\sqrt[3]{2}, \alpha\sqrt[3]{2}, \alpha^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \alpha)$.
   Infatti:

   $\subseteqq$: ✓

   $\supseteqq$: $\alpha = \frac{1}{2}(\alpha\sqrt[3]{2}) \cdot (\sqrt[3]{2})^2 \in F$

   Dunque $\mathbb{Q} \subset L = \mathbb{Q}(\sqrt[3]{2}) \subset L(\alpha) = F$ e $[F : \mathbb{Q}] = [F : L] \cdot [L : \mathbb{Q}] = 2 \cdot 3 = 6 = 3!$
   $[L : \mathbb{Q}] = 3$ poiché $x^3 - 2$ è polinomio minimo di $\sqrt[3]{2}$ su $\mathbb{Q}$.
   $[F : L] = 2$ poiché $x^2 + x + 1$ è polinomio minimo di α su $\mathbb{Q}$ e su $L \subset \mathbb{R}$.

14.3. Lemma

Sia $\sigma : K \to K'$ un omomorfismo di campi 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 rende commutativo il diagramma

$$\begin{tikzcd} K \arrow[r, phantom, "\subset"] \arrow[d, "\sigma"'] & F \arrow[d, "\tau"] \\ K' \arrow[r, phantom, "\subset"] & F' \end{tikzcd} \qquad \tau|_K = \sigma$$

Dimostrazione.
Sappiamo che esistono elementi $\alpha_1, \dots, \alpha_n \in F$ algebrici su K tali che $F = K(\alpha_1, \dots, \alpha_n)$.
Caso $n = 1$: $F = K(\alpha)$, $\alpha = \alpha_1$
L'omomorfismo σ induce un omomorfismo di anelli

$$\begin{array}{rcl} \tilde{\sigma} : K[x] & \longrightarrow & K'[x] \\ f = \displaystyle\sum_{i=0}^{n} a_i x^i & \longmapsto & \tilde{\sigma}(f) = \displaystyle\sum_{i=0}^{n} \sigma(a_i) x^i \end{array}$$

Sia f il polinomio minimo di α su K, sia $f' = \tilde{\sigma}(f)$, sia g un fattore irriducibile di f' in $K'[x]$ e sia $F' = K'[x]/(g)$. Allora $K' \subset F'$ è un'estensione finita.
Si noti che $\nu\tilde{\varepsilon}(f) = \nu(f') = 0$ poiché $f' \in (g)$.
Perciò $(f) \subset \ker \nu\tilde{\varepsilon}$ e per il Teorema di Fattorizzazione esiste $\tau : F \to F'$ tale che $\tau \circ \varepsilon_\alpha = \nu \circ \tilde{\sigma}$. Dunque $\tau|_K$ coincide con l'applicazione $K \xrightarrow{\sigma} K' \subset F'$.

$$\begin{tikzcd} & & K[x]/(f) \arrow[d, phantom, "\cong" rotate=-90] \\ K \arrow[r, phantom, "\subset"] \arrow[d, "\sigma"'] & K[x] \arrow[ur] \arrow[r, "\varepsilon_\alpha"] \arrow[d, "\tilde{\sigma}"'] & K(\alpha) = F \arrow[d, dashed, "\tau"] \\ K' \arrow[r, phantom, "\subset"] & K'[x] \arrow[r, "\nu"] & K'[x]/(g) = F' \end{tikzcd} \qquad f \mapsto f'$$

Per $n > 1$ si procede per induzione.

$\square$

14.4. Teorema
(Unicità del campo di riducibilità completa)

Sia $\sigma : K \to K'$ un isomorfismo di campi. 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 il crc di f su K e F' il crc di f' su K'. Allora esiste un isomorfismo $\tau : F \to F'$ che estende σ

$$\begin{tikzcd} K \arrow[d, "\sigma"', "\cong"] & \subset & F \arrow[d, "\cong"', "\tau"] & \text{crc di } f \text{ su } K \\ K' & \subset & F' & \text{crc di } f' \text{ su } K' \end{tikzcd}$$

e induce una biiezione tra gli zeri di f e gli zeri di f'.
In particolare , il crc di f su K è unico a meno di isomorfismo.

Dimostrazione.
Abbiamo

$$\begin{tikzcd} K \arrow[d, "\sigma"'] & \subset & F \arrow[drr, dashed, "\tau"] & & \\ K' & \subset & F' & \subset & L \end{tikzcd}$$

Per il Lemma esistono un'estensione finita $F' \subset L$ e un omomorfismo $\tau : F \to L$ che estende $K \xrightarrow{\sigma} K' \subset F'$. Sappiamo che τ è iniettivo e dobbiamo mostrare che $\operatorname{im}\tau = F'$.
Sappiamo che esistono $\alpha_1, \dots, \alpha_n \in F$ tali che $F = K(\alpha_1, \dots, \alpha_n)$ e
$f = a(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$ con $a \in K$.
Come nel Lemma, consideriamo l'isomorfismo

$$\begin{aligned} \tilde{\sigma} : K[x] &\longrightarrow K'[x] \\ \sum_{i=0}^{n} a_i x^i &\longmapsto \sum_{i=0}^{n} \sigma(a_i) x^i \end{aligned}$$

e l'omomorfismo analogo $\tilde{\tau} : F[x] \to L[x]$. Si noti che

$$\tilde{\tau}|_{K[x]} = \tilde{\sigma} \quad \text{e} \quad \operatorname{im}\tau = \tau(K)(\tau(\alpha_1), \dots, \tau(\alpha_n)) = K'(\tau(\alpha_1), \dots, \tau(\alpha_n))$$

Inoltre

$$\begin{aligned} f' = \tilde{\sigma}(f) = \tilde{\tau}(f) &= \tilde{\tau}(a(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)) \\ &= \tilde{\tau}(a)\tilde{\tau}(x - \alpha_1) \cdot \ldots \cdot \tilde{\tau}(x - \alpha_n) \\ &= \varepsilon(a)(x - \tilde{\tau}(\alpha_1)) \cdot \ldots \cdot (x - \tilde{\tau}(\alpha_n)) \text{ in } L[x] \end{aligned}$$

Dunque $\tau(\alpha_1), \dots, \tau(\alpha_n)$ sono zeri di f' e perciò $K'(\tau(\alpha_1), \dots, \tau(\alpha_n)) = F'$.
Concludiamo che $\operatorname{im}\tau = F'$ e τ induce una biiezione tra $\{\alpha_1, \dots, \alpha_n\}$ e l'insieme degli zeri di f'.

$\square$

15. Campi finiti

15.1. Lemma e definizione

Dato un campo K, consideriamo l'applicazione

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

che è un omomorfismo di anelli.
Se ψ è iniettiva, ovvero se $\ker \psi = 0$, allora si dice che K ha **caratteristica** 0.
Se ψ non è iniettiva, allora $\ker \psi = m\mathbb{Z}$ con m primo: se $m \mid ab$ con $a, b \in \mathbb{Z}$, allora $\psi(a)\psi(b) = \psi(ab) = 0_K$, perciò uno dei fattori, poniamo $\psi(a)$, dev'essere nullo, dunque $a \in \ker \psi = m\mathbb{Z}$ e $m \mid a$.
Dunque se ψ non è iniettivo, $\ker \psi = p\mathbb{Z}$ per un certo p e diciamo che K ha **caratteristica** p.

Osservazioni

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

1. Se $x \in K \smallsetminus \{0_K\}$ e $m \in \mathbb{N}$, allora

$$mx = 0 \text{ se e solo se } p \mid m$$

   Infatti $m \cdot x = \underbrace{x + \ldots + x}_{m \text{ volte}} = x(\underbrace{1_K + \ldots + 1_K}_{m \text{ volte}}) = x\psi(m) = 0$ se e solo se $\psi(m) = 0$, ovvero $m \in \ker \psi = p\mathbb{Z}$.

2. Per $x, y \in K$ si ha $(x + y)^p = x^p + y^p$.
   Infatti

$$(x + y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i}$$

dove
$$\binom{p}{i} = \frac{p!}{i!(p-i)!} \in p\mathbb{Z} \quad \text{per ogni} \quad 1 \leq i \leq p-1$$
e per (1) segue che $(x+y)^p = \binom{p}{0}x^p + \binom{p}{p}y^p = x^p + y^p$

3. L'applicazione $\varphi : K \to K, x \mapsto x^p$ è un omomorfismo, detto *omomorfismo di Frobenius*

15.2. Esempi

1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ hanno caratteristica 0.
2. $\mathbb{Z}/p\mathbb{Z}$ e il campo $\mathbb{Z}/p\mathbb{Z}(x) = \{\frac{f}{g} \mid f, g \in \mathbb{Z}/p\mathbb{Z}[x], g \neq 0\}$ delle *funzioni razionali* su $\mathbb{Z}/p\mathbb{Z}$ (infinito) hanno caratteristica p.
3. Ogni campo finito K ha caratteristica $p \neq 0$, poiché $\psi : \mathbb{Z} \to K$ non può essere iniettiva.

15.3. Lemma e definizione

Dato un campo K consideriamo $\mathcal{P} = \bigcap\{L \subset K \mid L \text{ sottocampo di } K\}$ il suo più piccolo sottocampo, detto **sottocampo fondamentale** di K.
Si ha $\mathcal{P} = \{(n1_K)(m1_K)^{-1} \mid n, m \in \mathbb{Z}, m1_K \neq 0_K\}$.
Inoltre $\operatorname{char} K = 0$ se e solo se $\mathcal{P} \cong \mathbb{Q}$ e $\operatorname{char} K = p$ se e solo se $\mathcal{P} \cong \mathbb{Z}/p\mathbb{Z}$.

Dimostrazione.
Certamente $\mathcal{P} \supset \{(n1_K)(m1_K)^{-1} \mid n, m \in \mathbb{Z}, m1_K \neq 0_K\}$ e $\operatorname{char} K = \operatorname{char} \mathcal{P}$, perciò si ha "$\Leftarrow$".
Sia adesso $\operatorname{char} K = 0$. Allora ψ è iniettiva e

$$\begin{tikzcd} n \arrow[d, mapsto] & \mathbb{Z} \arrow[r, hook] \arrow[d, "\psi"'] & \mathbb{Q} \arrow[dl, dashed, "\tilde{\psi}"] \\ n1_K & K & \end{tikzcd} \qquad \text{dove } \tilde{\psi}(\tfrac{n}{m}) = \psi(n)\psi(m)^{-1}$$

$\tilde{\psi}$ è un omomorfismo che estende ψ.
Poiché $\mathbb{Q}$ è un campo, $\tilde{\psi}$ è iniettiva. Inoltre $\operatorname{im} \tilde{\psi} = \{(n1_K)(m1_K)^{-1} \mid n, m \in \mathbb{Z}, m \neq 0\}$ è un sottocampo di K contenuto in $\mathcal{P}$. Perciò

$$\operatorname{im} \tilde{\psi} = \{(n1_K)(m1_K)^{-1} \mid n, m \in \mathbb{Z}, m \neq 0\} = \mathcal{P}$$

e $\tilde{\psi}$ induce un isomorfismo $\mathbb{Q} \cong \mathcal{P}$.

Se invece char $K = p$, allora $\ker\psi = p\mathbb{Z}$ e

$$\begin{tikzcd} \mathbb{Z} \arrow[r] \arrow[d, "\psi"'] & \mathbb{Z}/p\mathbb{Z} \arrow[dl, dashed, "\overline{\psi}"] \\ K & \end{tikzcd}$$

per il Teorema di Fattorizzazione, $\operatorname{im}\overline{\psi} = \operatorname{im}\psi = \{n1_K \mid n \in \mathbb{Z}\} \subset \mathcal{P}$ e come sopra concludiamo che

$$\operatorname{im}\overline{\psi} = \{(n1_K)m1_k^{-1} \mid n, m \in \mathbb{Z}, m1_K \neq 0_K\} = \mathcal{P}$$

e $\overline{\psi}$ induce un isomorfismo $\mathbb{Z}/p\mathbb{Z} \cong \mathcal{P}$.

□

15.4. Corollario

Sia F un campo finito , allora esistono un numero primo p e un $n \in \mathbb{N}$ tali che $|F| = p^n$ e $x^{p^n} = x$ per ogni $x \in F$.

Dimostrazione.
Sappiamo che char $F \neq 0$ e perciò $\mathcal{P} \cong \mathbb{Z}/p\mathbb{Z}$. Dunque $\mathcal{P} \subset F$ è un'estensione finita, poniamo $n = [F : \mathcal{P}]$, e $F \cong \mathcal{P}^n$ possiede $|\mathcal{P}^n| = p^n$ elementi.
Inoltre se $x \in F \setminus \{0_F\}$, si ha che nel gruppo moltiplicativo $(F \setminus \{0_F\}, \cdot)$ di $p^n - 1$ elementi vale $x^{p^n-1} = 1_F$, perciò $x^{p^n} = x$.

□

15.5. Lemma e definizione

Sia F un campo. L'applicazione

$$\begin{aligned} \mathcal{D} : F[x] &\longrightarrow F[x] \\ f = \sum_{i=0}^{n} a_i x^i &\longmapsto \mathcal{D}f = \sum_{i=1}^{n} i a_i x^{i-1} \end{aligned}$$

detta **derivata formale** è una *derivazione* di $F[x]$, cioè soddisfa, per $f, g \in K[x]$

($\mathcal{D}$1) $\mathcal{D}(f + g) = \mathcal{D}(f) + \mathcal{D}(g)$

($\mathcal{D}$2) $\mathcal{D}(fg) = \mathcal{D}(f)g + f\mathcal{D}(g)$

15.6. Lemma e definizione

Sia F un campo e siano $f \in F[x]$ e $\alpha \in F$ uno zero di f. Diremo che α è uno zero di **molteplicità** n se $(x-\alpha)^n \mid f$ ma $(x-\alpha)^{n+1}$ non divide f.

1. α è zero di f di molteplicità > 1 se e solo se α è zero sia di f sia di $\mathcal{D}f$.

2. Se f e $\mathcal{D}f$ sono coprimi in $F[x]$, allora α è uno zero di molteplicità 1.

15.7. Teorema di classificazione dei campi finiti

1. Per ogni numero primo p e ogni $n \in \mathbb{N}$ esiste un campo di p^n elementi $F = \mathbb{F}_{p^n}$, detto **campo di Galois** di ordine p^n, che si ottiene come campo di riducibilità completa del polinomio $x^{p^n} - x$ su $\mathbb{Z}/p\mathbb{Z}$.

2. Ogni campo finito F è isomorfo ad un campo di Galois $\mathbb{F}_{p^n}$

Dimostrazione.

1. Sia F il crc di $f = x^{p^n} - x$ su $K = \mathbb{Z}/p\mathbb{Z}$ e sia $F' = \{\alpha \in F \mid \alpha^{p^n} = \alpha\}$ l'insieme degli zeri di f in F. Verifichiamo che $K \subset F' \subset F$ è un campo intermedio.
   $K \subset F'$ perché gli elementi di K soddisfano $\alpha^p = \alpha$ per 15.4.
   $F' \subset F$ è un sottocampo:
   Se $\alpha, \beta \in F'$, allora
   $$(\alpha-\beta)^{p^n} = (\alpha + (-\beta))^{p^n} = \alpha^{p^n} + (-\beta)^{p^n} = \alpha - \beta$$
   Infatti $\beta + (-\beta)^{p^n} = \beta^{p^n} + (-\beta)^{p^n} = (\beta-\beta)^{p^n} = 0_K^{p^n} = 0_K$, quindi $(-\beta)^{p^n} = -\beta$.
   E se $\beta \neq 0_K$
   $$(\alpha\beta^{-1})^{p^n} = \alpha^{p^n}(\beta^{p^n})^{-1} = \alpha\beta^{-1}$$
   Perciò $\alpha - \beta$ e $\alpha\beta^{-1} \in F'$. Per la minimalità del crc segue $F' = F$.
   Resta da verificare che $f = x^{p^n} - x$ possiede p^n zeri distinti in F.
   Si ha che $\mathcal{D}f = p^n x^{p^n - 1} - 1 = -1$ non ha zeri in comune con f.
   Per 15.6 segue che $|F| = |F'| = p^n$.

2. Sia F un campo con $|F| = p^n$. Allora sappiamo che ogni $\alpha \in F$ è zero di $f = x^{p^n} - x$ per 15.4, e poiché f ha al più p^n zeri, concludiamo che F è crc di f sul suo sottocampo fondamentale $\mathcal{P} \cong \mathbb{Z}/p\mathbb{Z}$. Abbiamo quindi
   $$\begin{tikzcd} K = \mathbb{Z}/p\mathbb{Z} \arrow[d, "\sigma", "\cong"'] & \subset & \mathbb{F}_{p^n} \arrow[d, dashed, "\tau", "\cong"'] & \text{crc di } f \text{ su } K \\ \mathcal{P} & \subset & F & \text{crc di } f \text{ su } \mathcal{P} \end{tikzcd}$$
   e per l'unicità del crc (14.4) segue $F \cong \mathbb{F}_{p^n}$

$\square$

15.8. Lemma

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

Dimostrazione.
La dimostrazione è lasciata per esercizio.

$\square$

15.9. Teorema dell'elemento primitivo

Se F è un campo finito di ordine p^n, allora esiste un $\alpha \in F$ detto *elemento primitivo*, tale che $F = \{0_F, 1_F, \alpha, \alpha^2, \ldots, \alpha^{p^n-2}\}$.

Dimostrazione.
Per il Lemma $(F \setminus \{0_F\}, \cdot)$ è un gruppo ciclico di ordine $p^n - 1$ e perciò esiste un $\alpha \in F$ tale che $F \setminus \{0_F\} = \langle\alpha\rangle = \{1, \alpha, \alpha^2, \ldots, \alpha^{p^n-2}\}$.

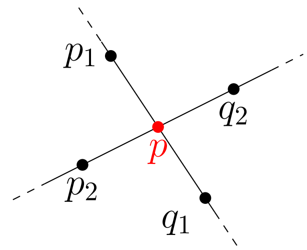
$\square$

16. Costruzioni con riga e compasso

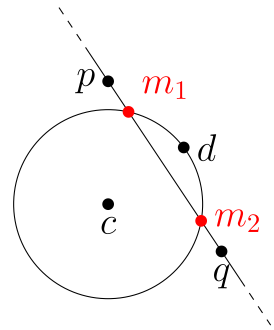
16.1. Definizione

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

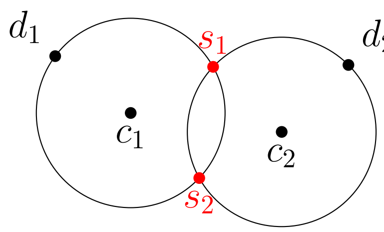
(I) **intersecare due rette**:
Se $\mathcal{R}_1$ e $\mathcal{R}_2$ sono due rette non parallele passanti rispettivamente per i punti p_1 e q_1, p_2 e q_2 di M, allora il punto di intersezione p appartiene ad $\mathrm{E}(M)$



(II) **Intersecare una retta con una circonferenza**:
Se $\mathcal{R}$ è una retta data dai punti p, q di M e $\mathcal{C}$ è la circonferenza di centro $c \in M$ e passante per $d \in M$, allora i punti di intersezione appartengono a $\mathrm{E}(M)$



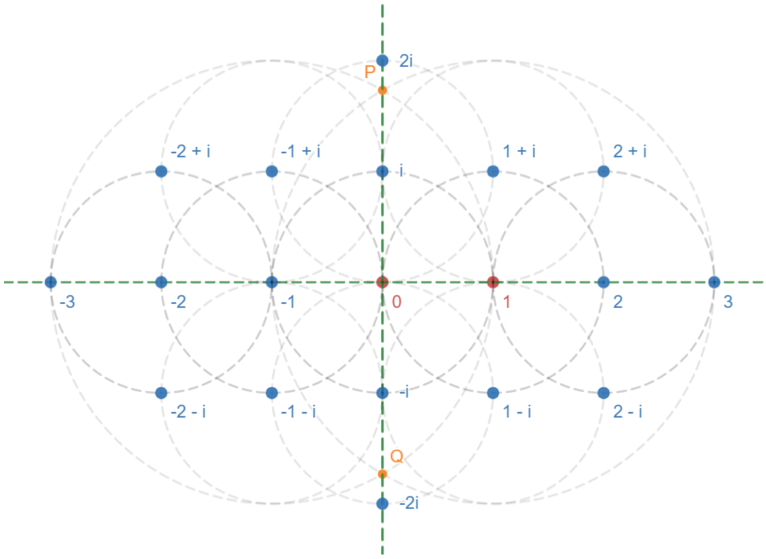
(III) **Intersecare due circonferenze** :
Se $\mathcal{C}_1$, $\mathcal{C}_2$ sono due circonferenze, rispettivamente di centri $c_i \in M$ passanti per $d_i \in M$, allora i punti di intersezione appartengono a $\mathrm{E}(M)$.



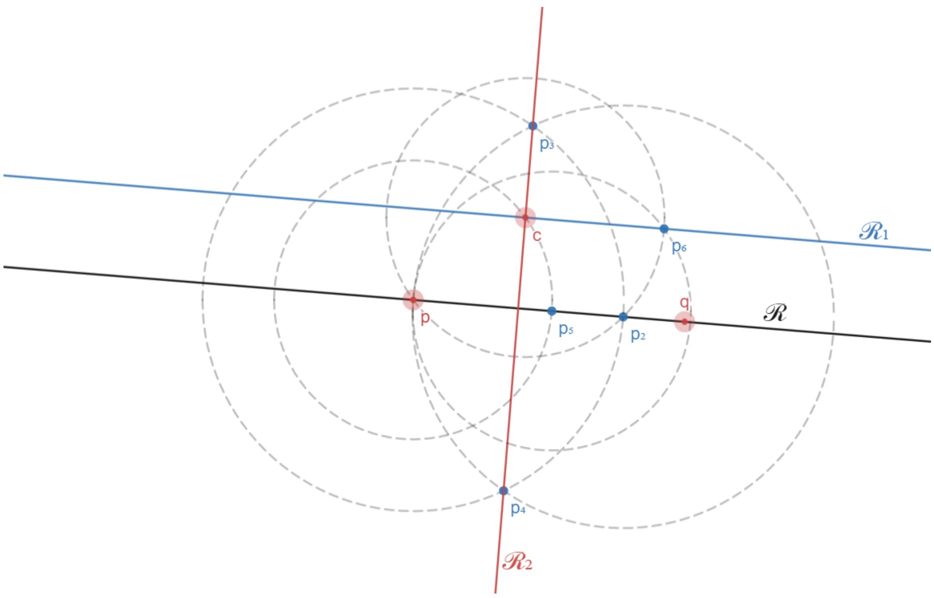
Diremo che $a \in \mathbb{C}$ è *costruibile con riga e compasso* da M se a è ottenuto da M attraverso un numero finito di costruzioni elementari, cioè esistono $a_1, \dots, a_n \in \mathbb{C}$ tali che $a_1 \in \mathrm{E}(M), a_2 \in \mathrm{E}(M \cup \{a_1\}), \dots, a_n \in \mathrm{E}(M \cup \{a_1, \dots, a_{n-1}\})$ e $a_n = a$.
Diciamo che $a \in \mathbb{C}$ è **costruibile** se è costruibile con riga e compasso da $M = \{0, 1\}$.

16.2. Esempi

1. Gli interi di Gauss $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ sono costruibili



2. Sia $M \subset \mathbb{C}$, $p, q, c \in M$ e sia $\mathcal{R}$ la retta passante per p, q. Allora si costruiscono con riga e compasso la retta $\mathcal{R}_1$ parallela a $\mathcal{R}$ passante per c e la retta $\mathcal{R}_2$ normale a $\mathcal{R}$ passante per c.



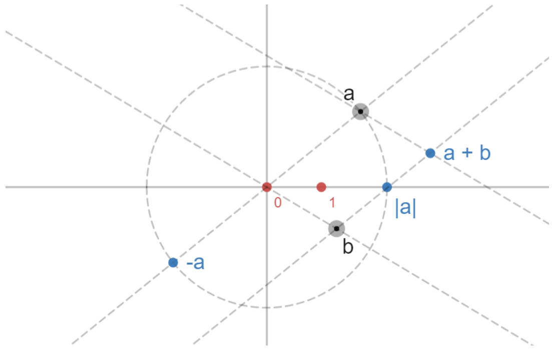
3. Si costruiscono con riga e compasso la bisettrice di angolo, la somma di due angoli e il punto medio di un segmento.

16.3. Lemma

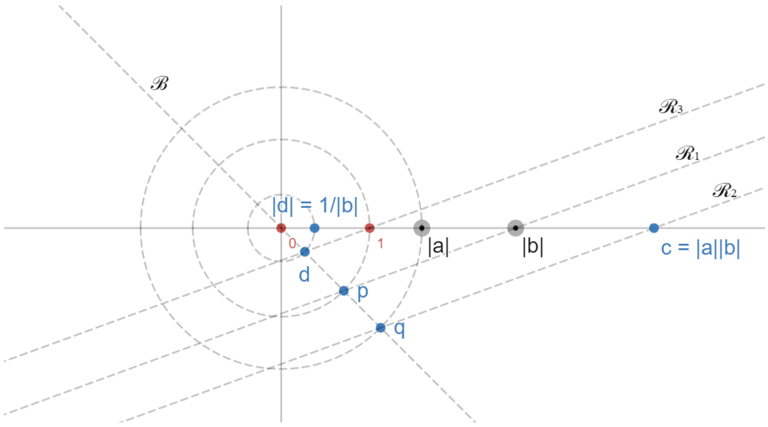
1. I numeri costruibili formano un campo intermedio $\mathbb{Q} \subset \mathbb{K} \subset \mathbb{C}$.
2. Se $c \in \mathbb{C}$ soddisfa $c^2 \in \mathbb{K}$, allora $c \in \mathbb{K}$

Dimostrazione.

1. Siano $a, b \in \mathbb{K}$, allora anche $a + b, -a \in \mathbb{K}$, e $|a| \in \mathbb{K} \cap \mathbb{R}$.



2. $|a| \cdot |b| \in \mathbb{K}$, se $b \neq 0$, anche $\frac{1}{|b|} \in \mathbb{K}$.



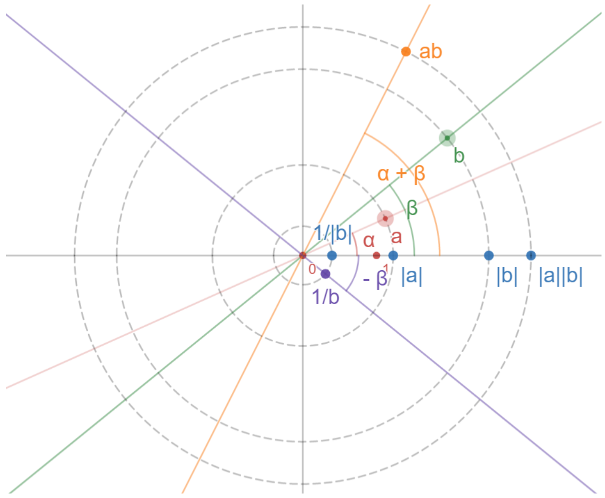
Costruisco:

- la bisettrice $\mathcal{B}$,
- p, q con (II),
- $\mathcal{R}_1$ passante per p e $|b|$,
- $\mathcal{R}_2$ parallela a $\mathcal{R}_1$ passante per q.

  Per il **Teorema di Talete** $\dfrac{|q|}{|p|} = \dfrac{|c|}{|b|}$ e poiché $|p| = 1$, $|q| = |a|$, segue $c = |a| \cdot |b|$.
- $\mathcal{R}_3$ parallela a $\mathcal{R}_2$ e passante per 1,
- d con (I).

  Per il Teorema di Talete $\dfrac{|d|}{|p|} = \dfrac{1}{|b|}$, perciò $|d| = \dfrac{1}{|b|}$.

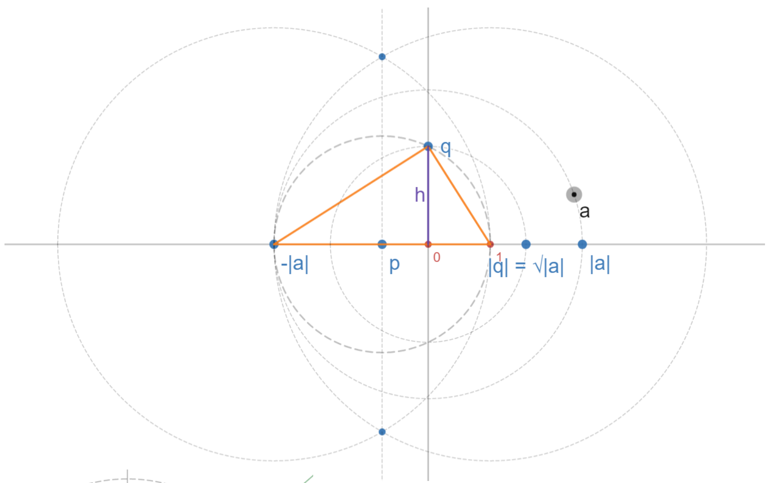
3. $ab \in \mathbb{K}$, $\frac{1}{b} \in K$ se $b \neq 0$

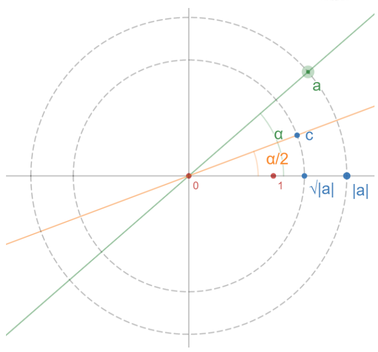


$$a = |a|(\cos\alpha + i\sin\alpha)$$
$$b = |b|(\cos\beta + i\sin\beta)$$
$$ab = |a||b|(\cos(\alpha+\beta) + i\sin(\alpha+\beta))$$
$$\frac{1}{b} = \frac{1}{|b|}(\cos(-\beta) + i\sin(-\beta))$$

4. Costruzione di $\sqrt{a}$ con $a = |a|(\cos\alpha + i\sin\alpha)$:
   Costruiamo $\sqrt{|a|}$:
   Costruiamo:
   - $-|a|$,
   - p punto medio del segmento $-|a|1$,
   - q con (II).

   Il triangolo $-|a|q1$ è rettangolo con $h = |q|$.
   $|a|1 = h^2 = |q|^2$. Quindi $|q| = \sqrt{|a|}$.





$$c = \sqrt{|a|}(\cos\frac{\alpha}{2} + i\sin\frac{\alpha}{2})$$
soddisfa $c^2 = a$

□

16.4. Lemma

Sia $L \subset \mathbb{C}$ un sottocampo tale che $i \in L$ e $\overline{L} = \{\overline{a} \in \mathbb{C} \mid a \in L\} = L$ e sia $M \subset L$.
Per ogni $a \in \mathrm{E}(M)$ esiste un numero complesso $b \in L$ tale che $b^2 \in L$ e $a \in L(b)$.

Dimostrazione.
L'ipotesi su L implica che se $a \in L$, anche $\overline{a}, \Re(a) = \frac{1}{2}(a+\overline{a}), \Im(a) = \frac{1}{2}(a-\overline{a}) \in L$ e $|a|^2 = a\overline{a} \in L$.

Caso (II)

> a è ottenuto intersecando la retta $\mathcal{R} = \{p + t(q-p) \mid t \in \mathbb{R}\}$ con $p, q \in M$ con la circonferenza $\mathcal{C}$ con centro $c \in M$ passante per $d \in M$.
> Sappiamo che $r^2 = |d-c|^2 \in L$. Abbiamo dunque che $|a-c|^2 = r^2$, ovvero
>
> $$(p - c + t(q-p))(\overline{p} - \overline{c} + t(\overline{q} - \overline{p})) = r^2$$
>
> Quindi t è soluzione di un'equazione di secondo grado con coefficienti in L e perciò $t \in L(b)$ dove $b \in \mathbb{C}$ e $b^2 \in L$ (ad esempio $b = \delta$ con $\delta^2 = \Delta$ il discriminante dell'equazione) e $a = p + t(q-p) \in L(b)$.

Analogamente per il caso (III), mentre nel caso (I) si ha che $a \in L$.

□

16.5. Teorema

Sia $a \in \mathbb{K}$ costruibile. Allora esiste una catena finita di campi intermedi

$$\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset \ldots \subset L_m \subset \mathbb{C}$$

Tale che $[L_{i+1} : L_i] = 2$ per ogni $1 \leq i < m$ e $a \in L_m$.
In particolare a è un elemento algebrico su $\mathbb{Q}$ dove $[\mathbb{Q}(a) : \mathbb{Q}]$ è una potenza di 2.

Dimostrazione.
Sia $a \in \mathbb{K} \setminus \{0,1\}$, allora esistono $n \in \mathbb{N}$ e $a_1, \ldots, a_n \in \mathbb{C}$ tali che
$a_1 \in \mathrm{E}(\{0,1\}), a_2 \in \mathrm{E}(\{0,1,a_1\}), \ldots, a = a_n \in \mathrm{E}(\{0,1,a_1,\ldots,a_{n-1}\})$.
Poniamo $L_1 = \mathbb{Q}(i)$, dunque $[L_1 : L_0] = 2$ e L_1 soddisfa le ipotesi del Lemma con $M = \{0,1\}$. Per $a_1 \in \mathrm{E}(M)$ esiste quindi un $b_1 \in \mathbb{C}$ tale che $b_1^2 \in L_1$ e $a_1 \in L_1(b)$.
Poniamo $L_2 = L_1(b_1) \subset L_3 = L_1(b_1, \overline{b_1})$. Si ha $[L_2 : L_1] \leq 2$ e poiché $\overline{b_1}^2 \in \overline{L_1} = L_1$ anche $[L_3 : L_2] \leq 2$.
Poiché L_3 soddisfa le ipotesi del Lemma e $M_3 = \{0,1,a_1\} \subset L_3$, abbiamo che per $a_2 \in \mathrm{E}(M_3)$ esiste $b_2 \in \mathbb{C}$ tale che $b_2^2 \in L_3$ e $a_2 \in L_3(b_2)$.
Continuando così si ottiene una catena con le proprietà desiderate. Dunque abbiamo un campo intermedio $\mathbb{Q} \subset \mathbb{Q}(a) \subset L_m$, perciò $[\mathbb{Q}(a) : \mathbb{Q}] \mid [L_m : \mathbb{Q}] = 2^m$ è una potenza di 2, in particolare a è algebrico su $\mathbb{Q}$.

□

16.6. Corollario

1. La quadratura del cerchio è impossibile:
   Non esiste un quadrato di lato $a \in \mathbb{K}$ la cui area sia pari all'area della circonferenza di raggio 1 e centro 0. Infatti per tale $a \in \mathbb{K}$ si avrebbe $|a|^2 = \pi$ e quindi si avrebbe $\pi \in \mathbb{K}$. Ma per il **Teorema di Lindemann** π è trascendente su $\mathbb{Q}$.

2. La duplicazione del cubo è impossibile:
   Non esiste un cubo di lato $a \in \mathbb{K}$ il cui volume sia il doppio dl volume del cubo di lato 1.
   Infatti per tale $a \in \mathbb{K}$ si avrebbe $a^3 = 2$, ovvero a avrebbe polinomio minimo $x^3 - 2$ su $\mathbb{Q}$ e quindi $[\mathbb{Q}(a) : \mathbb{Q}] = 3$ non sarebbe una potenza di 2. $\lightning$

3. La trisezione dell'angolo è impossibile:
   Prendiamo $\alpha = 60° = \frac{\pi}{3}$. Se $\frac{\alpha}{3} = \frac{\pi}{9}$ fosse costruibile, lo sarebbe anche $\frac{2\pi}{9}$, ovvero $z = \cos\frac{2\pi}{9} + i \sin\frac{2\pi}{9} \in \mathbb{K}$.
   Ma z è una radice nona di 1 e il suo polinomio minimo è $\phi_9 = x^6 + x^3 + 1$.
   Infatti z è zero di $x^9 - 1 = (x^3 - 1)(x^6 + x^3 + 1)$ e perciò è zero di ϕ_9 che è irriducibile (riduzione modulo 2). Quindi $[\mathbb{Q}(z) : \mathbb{Q}] = \deg \phi_9 = 6$ non è una potenza di 2 e $z \notin \mathbb{K}$.

Parte V.

Teoria di Galois

17. Estensioni normali

17.1. Definizione

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

(i) $K \subset F$ è un'estensione algebrica

(ii) Per ogni $\alpha \in F$ il polinomio minimo $f \in K[x]$ di α su K è prodotto di fattori lineari in $F[x]$

$$f = a(x-\alpha_1)\cdot \ldots \cdot (x-\alpha_n) \text{ con } a \in K \text{ e } \alpha_1, \ldots, \alpha_n \in F$$

17.2. Esempi

1. Ogni estensione $K \subset F$ di grado 2 è normale.
   Se $\alpha \in F \setminus K$ il suo polinomio minimo f ha grado 2.
   Infatti $K \subsetneq K(\alpha) \subset F$ mostra che $\deg f = [K(\alpha) : K] = 2$. Quindi in $F[x]$ si ha $f = (x-\alpha)g$ con $\deg g = 1$, perciò $f = a(x-\alpha)(x-\beta)$

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 di grado 2 e pertanto normali, ma $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{p})$ **non** è normale:
   Il polinomio minimo $f = x^4 - p$ di $\sqrt[4]{p}$ è prodotto dei fattori irriducibili in $F[x]$

$$\begin{aligned} f &= (x^2-\sqrt{p})(x^2+\sqrt{p}) \\ &= (x-\sqrt[4]{p})(x-\sqrt[4]{p})(\underset{\substack{\uparrow \\ \text{irriducibile su } F=\mathbb{Q}(\sqrt[4]{p})\subset\mathbb{R} \\ \text{poiché i suoi zeri } i\sqrt[4]{p},\,-i\sqrt[4]{p}\notin F}}{x^2+\sqrt{p}}) \end{aligned}$$

17.3. Teorema

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

Dimostrazione.

"$\Rightarrow$" : Esistono elementi algebrici $\alpha_1, \dots, \alpha_n \in F$ su K tali che $F = K(\alpha_1, \dots, \alpha_n)$. Siano $f_1, \dots, f_n$ i polinomi minimi di $\alpha_1, \dots, \alpha_n$ su K e sia $f = f_1 \cdot \ldots \cdot f_n \in K[x]$. Poiché $K \subset F$ è normale, ogni f_i e quindi anche f è prodotto di fattori lineari in $F[x]$. Dunque $f = a(x - \beta_1) \cdot \ldots \cdot (x - \beta_m)$ con $a \in K, \beta_1, \dots, \beta_m \in F$. Si noti che $\{\alpha_1, \dots, \alpha_n\} \subseteq \{\beta_1, \dots, \beta_m\}$, perciò

$$F = K(\alpha_1, \dots, \alpha_n) \subseteq K(\beta_1, \dots, \beta_m) \subseteq F$$

e F è crc di f su K.

"$\Leftarrow$" : Sia F crc di $f \in K[x]$ su K.
Supponiamo che $K \subset F$ non sia normale. Allora esiste $\alpha \in F$ il cui polinomio minimo $g \in K[x]$ su K non è prodotto di fattori lineari in $F[x]$.
Sia L il crc di g su F. Allora esiste un $\beta \in L \setminus F$ con $g(\beta) = 0$. Si noti che g è anche polinomio minimo di β su K. Dunque abbiamo un isomorfismo

$$\begin{array}{ccccc} \sigma : K(\alpha) & \underset{\overline{\varepsilon_\alpha}}{\cong} & K[x]/(g) & \underset{\overline{\varepsilon_\beta}}{\cong} & K(\beta) \\ \alpha & \longleftarrow & \overline{x} & \longmapsto & \beta \end{array}$$

con $\sigma(\alpha) = \beta$ e $\sigma|_K = \mathrm{id}_K$. Abbiamo quindi

$$\begin{tikzcd} K \arrow[d, "\mathrm{id}_K"'] & \subset & K(\alpha) \arrow[d, "\cong"', "\sigma"] & \subset & F \arrow[d, dashed, "\tau"] & \text{crc di } f \text{ su } K(\alpha) \\ K & \subset & K(\beta) & \subset & F(\beta) & \text{crc di } f \text{ su } K(\beta) \end{tikzcd}$$

Dunque esiste un isomorfismo di campi $\tau : F \to F(\beta)$ che estende σ.
Ma τ è anche un isomorfismo di spazi vettoriali su K: per $k \in K, b \in F$

$$\tau(k \cdot b) = \tau(k) \cdot \tau(b) = k \cdot \tau(b)$$

Dunque $[F(\beta) : K] = [F : K]$ e per il Lemma del Grado applicato a $K \subset F \subset F(\beta)$ otteniamo $[F(\beta) : F] = 1$, perciò $F(\beta) = F$ e $\beta \in F$ $\lightning$

$\square$

17.4. Corollario

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

18. Separabilità

18.1. Teorema

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

1. Esiste un'estensione $K \subset F$ tale che $f = a(x-\alpha_1) \cdot \ldots \cdot (x-\alpha_n)$, dove $a \in K$ e $\alpha_1, \ldots, \alpha_n$ sono elementi distinti di F
2. f e $\mathcal{D}(f)$ sono coprimi in $K[x]$
3. Non esiste un'estensione $K \subset F$ nella quale f abbia uno zero di molteplicità > 1

Se f è irriducibile su K, gli enunciati $(1) - (3)$ sono equivalenti a:

4. $\mathcal{D}(f) \neq 0$

Dimostrazione.

"$(1) \Rightarrow (2)$": Sia $d \in K[x]$ un comun divisore di f e $\mathcal{D}(f)$. Allora in $F[x]$ si ha

$$d = c(x-\alpha_{i_1}) \cdot \ldots \cdot (x-\alpha_{i_r}) \quad \text{con} \quad c \in K, i_1, \ldots, i_r \in \{1, \ldots, n\}$$

per l'unicità della scomposizione in fattori irriducibili.
Poiché f e $\mathcal{D}(f)$ non hanno zeri in comune per 15.6, segue $r = 0$ e $d = c$ è un polinomio costante e pertanto invertibile in $K[x]$.

"$(2) \Rightarrow (3), (4)$": Per l'identità di Bézout, possiamo esprimere

$$1 = \alpha f + \beta \mathcal{D}(f) \quad \text{con} \quad \alpha, \beta \in K[x]$$

Ma allora non può esistere un'estensione $K \subset F$ nella quale f e $\mathcal{D}(f)$ abbiano uno zero comune e per 15.6 segue (3). Inoltre $\mathcal{D}(f) \neq 0$, poiché altrimenti f sarebbe invertibile, ma $\deg f > 0$.

"$(3) \Rightarrow (1)$": Scegliendo per F il crc di f su K.

"$(4) \Rightarrow (2)$": Sia d un divisore comune di f e $\mathcal{D}(f)$ in $K[x]$. Allora esistono $g, h \in K[x]$ tali che $f = dg$ e $\mathcal{D}(f) = dh$. Allora $\deg d \leq \deg \mathcal{D}(f) < \deg f$, perciò per ipotesi su f segue che $\deg g = n$ e $\deg d = 0$, quindi d è invertibile.

$\square$

18.2. Definizione

Sia K un campo e sia $f \in K[x]$ un polinomio di grado $n > 0$. Se f è irriducibile su K, diremo che f è **separabile** su K quando soddisfa gli enunciati del Teorema 18.1. In generale f è separabile su K se lo sono tutti i suoi fattori irriducibili.

18.3. Esempi

1. L'ipotesi "irriducibile" in 18.1 è indispensabile: sia $f = (x-2)^2 \in \mathbb{Q}[x]$. Allora $\mathcal{D}(f) = 2x \neq 0$ ma f ha uno zero di molteplicità 2.

2. Ogni polinomio non costante su un campo K di $\operatorname{char} K = 0$ è separabile. Basta verificarlo per un polinomio $f \in K[x]$ irriducibile: se $f = \sum_{i=0}^{n} a_i x^i$, allora $\mathcal{D}(f) = \sum_{i=1}^{n} i a_i x^{i-1} \neq 0$, poiché $n a_n \neq 0$.

3. Siano $f_1, \ldots, f_n \in K[x]$. Allora $f = f_1 \cdot \ldots \cdot f_n$ è separabile se e solo se lo sono tutti gli f_i. Infatti i fattori irriducibili di f sono esattamente i polinomi irriducibili che dividono uno degli f_i.

4. Un polinomio separabile su K è separabile anche in qualsiasi estensione $K \subset F$. Infatti se $f \in K[x]$ è separabile e $g \in F[x]$ è un suo fattore irriducibile in $F[x]$, allora g divide un fattore irriducibile h di f in $K[x]$ (se $f = f_1 \cdot \ldots \cdot f_r$ è la scomposizione in fattori irriducibili e $g \mid f$ in $F[x]$, allora g deve dividere uno dei fattori $f_1, \ldots, f_r$). Ma allora non può esistere un'estensione $F \subset F'$ nella quale g abbia uno zero di molteplicità > 1 poiché questo sarebbe anche zero del polinomio irriducibile e separabile h.

18.4. Definizione

Un campo K si dice **perfetto** se ogni polinomio non costante in $K[x]$ è separabile se K.

Abbiamo visto che K è perfetto se $\operatorname{char} K = 0$ e vediamo adesso che ogni campo finito è perfetto, grazie a

18.5. Teorema

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

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

è suriettivo (e quindi biiettivo)

Dimostrazione.

"$\Rightarrow$" : Sia $a \in K$. Dobbiamo trovare $\alpha \in K$ tale che $\alpha^p = a$, ovvero uno zero del polinomio $f = x^p - a \in K[x]$. Sia g un fattore irriducibile di f in $K[x]$ e sia F il suo crc e $\alpha \in F$ un suo zero. Allora α è anche zero di f e resta da dimostrare che $\alpha \in K$. In $F[x]$ si ha $f = x^p - \alpha^p = (x-\alpha)^p$, quindi $g = (x-\alpha)^n$ per $n \leq p$. Poiché per ipotesi g è separabile (e irriducibile) su K, abbiamo $n = 1$ e quindi $g = x - \alpha \in K[x]$ e $\alpha \in K$.

"$\Leftarrow$" : Supponiamo che esista un polinomio irriducibile $f = \sum_{i=0}^n a_i x^i \in K[x]$ che non sia separabile. Allora $\mathcal{D}(f) = \sum_{i=1}^n i a_i x^{i-1} = 0$. Perciò $a_i = 0$ per ogni $i \notin p\mathbb{Z}$ e $f = a_0 + a_p x^p + a_{2p} x^{2p} + \dots$. Inoltre per ipotesi ogni a_i, $i \in p\mathbb{Z}$, è di forma $a_i = \alpha_i^p$ per un $\alpha_i \in K$. Dunque

$$\begin{aligned} f &= \alpha_0^p + \alpha_p^p x^p + \alpha_{2p}^p x^{2p} + \dots \\ &= (\alpha_0 + \alpha_p x + \alpha_{2p} x^2 + \dots)^p \end{aligned}$$

$$\lightning$$

$\square$

18.6. Definizione

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

18.7. Esempi

1. Ogni estensione algebrica di un campo perfetto è separabile.

2. Un'estensione algebrica non separabile:
   Sia p primo e sia $K = \mathbb{Z}/p\mathbb{Z}(x) = \{\frac{f}{g} \mid f, g \in \mathbb{Z}/p\mathbb{Z}[x], g \neq 0\}$ il campo delle funzioni razionali su $\mathbb{Z}/p\mathbb{Z}$.
   K è un campo infinito di caratteristica p. Verifichiamo che non è perfetto:
   Consideriamo $f = y^p - x \in K[y]$. È irriducibile, ciò si mostra usando che x è un elemento irriducibile in $\mathbb{Z}/p\mathbb{Z}[x]$ e anche in $\mathbb{Z}/p\mathbb{Z}(x)$; gli argomenti sono analoghi a quelli usati in 12.6 e 12.5. La derivata $\mathcal{D}(f) = py^{p-1} = 0$, perciò f non è separabile su K.
   Il crc di f su K è quindi un'estensione algebrica che non è separabile.

19. Campi intermedi e sottogruppi

19.1. Lemma e definizione

Sia F un campo.

1. Gli automorfismi $\varphi : F \to F$ di F formano un gruppo $(\operatorname{Aut} F, \circ)$ rispetto alla composizione $\circ$.
2. Sia $G \leq \operatorname{Aut} F$. Allora l'insieme
$$\operatorname{Fix}_F(G) = \{a \in F \mid \varphi(a) = a \text{ per ogni } \varphi \in G\}$$
è un sottocampo di F, detto **campo fisso** di G in F.

Dimostrazione.

2. Siano $a, b \in \operatorname{Fix}_F(G)$. Allora per $\varphi \in G$
$$\varphi(a-b) = \varphi(a) - \varphi(b) = a - b$$
$$\text{e se } b \neq 0 \quad \varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = ab^{-1}$$
quindi $a - b, ab^{-1} \in \operatorname{Fix}_F(G)$.

□

19.2. Lemma

Dati due campi K, F consideriamo lo spazio vettoriale K^F su K di tutte le applicazioni $F \overset{\varphi}{\to} K$ con l'addizione di applicazioni e la moltiplicazione per uno scalare
$$k \cdot \varphi : F \to K, x \mapsto k\varphi(x)$$
Gli omomorfismi $F \to K$ formano un insieme linearmente indipendente in K^F.

Dimostrazione.
Supponiamo che esistano n omomorfismi distinti $\varphi_1, \ldots, \varphi_n : F \to K$ che sono linearmente dipendenti su K e scegliamo n minimo. Allora $n \geq 2$ e possiamo supporre $\varphi_1 = \sum_{i=2}^n k_i\varphi_i$ con $k_2, \ldots, k_n \in K$ e $k_2 \neq 0$. Per $a, x \in F$ arbitrari si ha
$$\sum_{i=2}^n k_i\varphi_i(a)\varphi_i(x) = \sum_{i=2}^n k_i\varphi_i(ax) = \varphi_1(ax) = \varphi_1(a)\varphi_1(x) = \varphi_1(a)\sum_{i=2}^n k_i\varphi_i(x)$$

Quindi $\sum_{i=2}^{n} k_i(\varphi_i(a) - \varphi_1(a))\varphi(x) = 0$ e poiché $x \in F$ era arbitrario

$$\sum_{i=2}^{n} \underset{K}{\underset{\cap}{k_i}}\underbrace{(\varphi_i(a) - \varphi_1(a))}_{\substack{\cap \\ K}}\varphi = 0$$

Per la minimalità di n, sappiamo che $\varphi_2, \dots, \varphi_n$ sono linearmente indipendenti, quindi $k_i(\varphi_i(a) - \varphi_1(a)) = 0$ per ogni $1 < i \leq n$. In particolare $\varphi_2(a) = \varphi_1(a)$ con $a \in F$ arbitrario, perciò $\varphi_1 = \varphi_2$ $\lightning$

19.3. Lemma di Dedekind

Siano K, F due campi e siano $\varphi_1, \dots, \varphi_n : F \to K$ omomorfismi distinti. Allora

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

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

Dimostrazione.
Supponiamo che esista una L-base $\{a_1, \dots, a_r\}$ di F con $r < n$. Consideriamo la matrice "orizzontale"

$$A = \begin{pmatrix} \varphi_1(a_1) & \varphi_2(a_1) & \cdots & \varphi_n(a_1) \\ \varphi_1(a_2) & \varphi_2(a_2) & \cdots & \varphi_n(a_2) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_1(a_r) & \varphi_2(a_r) & \cdots & \varphi_n(a_r) \end{pmatrix} \in \mathrm{M}_{r \times n}(K)$$

con l'applicazione lineare $K^n \to K^r, x \mapsto Ax$ che non può essere iniettiva.
Sia dunque $\begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix} \in K^n \setminus \{0\}$ un elemento del nucleo. Abbiamo $A \begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix} = 0$,
dunque per ogni $1 \leq k \leq r$ $\quad \sum_{i=1}^{n} k_i \varphi_i(a_k) = 0.$

Per $a \in F$ arbitrario esistono $l_1, \ldots, l_r \in L$ tali che $a = \sum_{k=1}^{r} l_k a_k$, perciò

$$\begin{aligned}
\sum_{i=1}^{n} k_i \varphi_i(a) &= \sum_{i=1}^{n} k_i \varphi_i \left(\sum_{k=1}^{r} l_k a_k \right) \\
&= \sum_{i,k} k_i \varphi_i(l_k a_k) = \sum_{i,k} k_i \underbrace{\varphi_i(l_k)}_{=\varphi_1(l_k)} \varphi_i(a_k) \\
&= \sum_{k=1}^{r} \varphi_i(l_k) \underbrace{\sum_{i=1}^{n} k_i \varphi_i(a_k)}_{=0} = 0
\end{aligned}$$

Quindi $\sum_{i=1}^{n} k_i \varphi_i = 0$, ma non tutti i k_i sono nulli $\lightning$ (19.2)

19.4. Lemma e definizione

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

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

è detta **traccia** di G in F e soddisfa $\operatorname{im} \tau = \operatorname{Fix}_F(G)$

Dimostrazione.
Sia $G = \{\varphi_1, \ldots, \varphi_n\}$

"$\subseteq$" : Sia $1 \leq i \leq n$

$$\varphi_i(\tau(a)) = \varphi_i \left(\sum_{k=1}^{n} \varphi_k(a) \right) = \sum_{k=1}^{n} \varphi_i \varphi_k(a) \underset{\substack{\uparrow \\ \{\varphi_i\varphi_1, \varphi_i\varphi_2, \ldots, \varphi_i\varphi_n\} = G}}{=} \tau(a)$$

"$\supseteq$" : Per 19.2 si ha che $\tau = \varphi_1 + \ldots + \varphi_n \neq 0$ quindi esiste $a \in F$ con $\tau(a) \neq 0$. Sia $b \in \operatorname{Fix}_F(G)$. Allora anche $c = b\tau(a)^{-1} \in \operatorname{Fix}_F(G)$ e si ha

$$b = c\tau(a) = \sum_{i=1}^{n} c\varphi_i(a) = \sum_{i=1}^{n} \varphi_i(c)\varphi_i(a) = \sum_{i=1}^{n} \varphi_i(ca) = \tau(ca) \in \operatorname{im} \tau$$

$\square$

19.5. Teorema di Artin

Sia F un campo e sia $G \leq \operatorname{Aut} F$ un sottogruppo finito. Allora $[F : \operatorname{Fix}_F(G)] = |G|$

Dimostrazione.
Poniamo $K = \operatorname{Fix}_F(G)$, $n = |G|$ e $G = \{\varphi_1 = \mathrm{id}_G, \varphi_2, \dots, \varphi_n\}$.
Si noti che $\operatorname{Fix}_F(G) = \{a \in F \mid \underbrace{\varphi_1(a)}_{\overset{\|}{a}} = \varphi_2(a) = \ldots = \varphi_n(a)\}$, perciò
$[F : K] \geq n$ per il Lemma di Dedekind.
Supponiamo che esista un insieme K-linearmente indipendente $\{a_1, \dots, a_{n+1}\} \subset F$. La matrice

$$A = \begin{pmatrix} \varphi_1^{-1}(a_1) & \varphi_1^{-1}(a_2) & \cdots & \varphi_1^{-1}(a_{n+1}) \\ \varphi_2^{-1}(a_1) & \varphi_2^{-1}(a_2) & \cdots & \varphi_1^{-1}(a_{n+1}) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_n^{-1}(a_1) & \varphi_n^{-1}(a_2) & \cdots & \varphi_n^{-1}(a_{n+1}) \end{pmatrix} \in \mathrm{M}_{n\times(n+1)}(F)$$

definisce un'applicazione lineare non iniettiva $F^{n+1} \to F^n, x \mapsto Ax$
con $\begin{pmatrix} b_1 \\ \vdots \\ b_{n+1} \end{pmatrix} \in F^{n+1} \setminus \{0\}$ nel nucleo. Dunque per ogni $1 \leq k \leq n$ $\quad \sum_{i=1}^{n+1} \varphi_k^{-1}(a_i) b_i = 0.$
Sia $x \in F$ arbitrario, allora

$$\begin{aligned}
\sum_{i=1}^{n+1} \underbrace{\tau(xb_i)}_{\substack{\cap \\ K \\ \text{per } 19.4}} a_i &= \sum_{i=1}^{n+1} (\varphi_1(xb_i) + \ldots + \varphi_n(xb_i)) a_i \\
&= \sum_{i=1}^{n+1} (\varphi_1(xb_i)\varphi_1\varphi_1^{-1}(a_i) + \ldots + \varphi_n(xb_i)\varphi_n\varphi_n^{-1}(a_i)) \\
&= \sum_{i=1}^{n+1} \sum_{k=1}^{n} \varphi_k(xb_i \cdot \varphi_k^{-1}(a_i)) \\
&= \sum_{k=1}^{n} \varphi_k \left(x \cdot \underbrace{\sum_{i=1}^{n+1} b_i \varphi_k^{-1}(a_i)}_{\substack{\| \\ 0}} \right) = 0
\end{aligned}$$

Per ipotesi segue che $\tau(xb_i) = 0$ per ogni $x \in F$ e $\leq i \leq n+1$.
Scegliendo i con $b_i \neq 0$ otteniamo $\tau(x) = \tau(\underbrace{xb_i^{-1}}_{x' \in F} b_i) = 0$, perciò $\tau = 0$. $\lightning$

19.6. Lemma e definizione

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

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

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

Osservazioni

1. Se $K \subset L \subset F$, allora $\operatorname{Gal}(F/L) \leq \operatorname{Gal}(F/K)$
2. Per ogni estensione finita $K \subset F$ si ha

$$|\operatorname{Gal}(F/K)| \quad \text{divide} \quad [F : K]$$

Dimostrazione di (2).
Siano $G := \operatorname{Gal}(F/K)$, $n := [F : K]$
Supponiamo che $\varphi_1, \ldots, \varphi_{n+1}$ siano automorfismi distinti in G. Allora avremmo

$$K \subset L = \{a \in F \mid \varphi_1(a) = \ldots = \varphi_{n+1}(a)\} \subset F$$

con $[F : L] \geq n + 1$ per 19.3 $\lightning$
Dunque $|G| \leq n$ e per $K \subset \operatorname{Fix}_F(G) \subset F$ vediamo con 19.5 che $|G| = [F : \operatorname{Fix}_F(G)] \mid n$.
$\square$

19.7. Esempi

1. Ogni automorfismo di F fissa gli elementi del sottocampo fondamentale $\mathcal{P}$ (poiché fissa 1_F), perciò $\operatorname{Gal}(F/\mathcal{P}) = \operatorname{Aut} F$
2. Sia $d \in \mathbb{Z} \setminus \{0, 1\}$ prodotto di primi distinti e sia $F = \mathbb{Q}(\sqrt{d})$.
Allora $\operatorname{Gal}(F/\mathbb{Q}) = \operatorname{Aut} F$ è un gruppo di ordine $2 = [F : \mathbb{Q}]$.
Infatti ogni $\varphi \in \operatorname{Aut} F$ fissa gli elementi di $\mathbb{Q}$ e soddisfa $\varphi(\sqrt{d})^2 = \varphi(d) = d$, perciò $\varphi(\sqrt{d}) = \pm\sqrt{d}$, e poiché gli elementi di F sono di forma $x = a + b\sqrt{d}$ con $a, b \in \mathbb{Q}$, si ha $\varphi(x) = a + b\varphi(\sqrt{d})$. Dunque

$$\varphi = \mathrm{id}_F \qquad \text{oppure} \qquad \varphi : F \to F, a + b\sqrt{d} \mapsto a - b\sqrt{d}$$

3. Sia $F = \mathbb{Q}(\sqrt[3]{2})$. Allora $[F : \mathbb{Q}] = 3$ e $\operatorname{Gal}(F/\mathbb{Q}) = \operatorname{Aut} F = \{\mathrm{id}_F\}$.
Infatti per $\alpha = \sqrt[3]{2}$ si ha che ogni elemento di F è di forma $x = a + b\alpha + c\alpha^2$ con $a, b, c \in \mathbb{Q}$ e $\varphi(x) = a + b\varphi(\alpha) + c\varphi(\alpha)^2$, perciò φ è determinato dall'elemento $\varphi(\alpha)$ e $\varphi(\alpha)^3 = \varphi(2) = 2$.

Dunque $\varphi(\alpha) \in F = \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ è una terza radice di 2, quindi $\varphi(\alpha) = \sqrt[3]{2} = \alpha$.
Concludiamo $\varphi = \mathrm{id}_F$.
Abbiamo quindi

$$\mathbb{Q} \subset F \rightsquigarrow G = \mathrm{Gal}(F/\mathbb{Q}) = \{\mathrm{id}_F\} \rightsquigarrow \underset{\underset{\mathbb{Q}}{\not\supseteq}}{\mathrm{Fix}_F(G)} = F$$

19.8. Teorema

Sia F un campo e sia $G \leq \operatorname{Aut} F$ un sottogruppo finito. Allora $\mathrm{Gal}(F/\operatorname{Fix}_F(G)) = G$

Dimostrazione.
Sia $K = \mathrm{Fix}_F(G)$, $n = |G|$ e $G = \{\varphi_1 = \mathrm{id}_F, \dots, \varphi_n\}$. Per 19.5 $[F : K] = n$.

"$\supseteq$" : ✓

"$\subseteq$" : Supponiamo esista un $\varphi \in \mathrm{Gal}(F/K)$ e $\varphi \notin G$. Allora avremmo un campo intermedio

$$K \subset L = \{a \in F \mid \underset{\underset{a}{\parallel}}{\varphi_1(a)} = \ldots = \varphi_n(a) = \varphi(a)\} \subset F$$

e per 19.3 avremmo che $[F : L] \geq n + 1$ $\quad \lightning$

$\square$

Schema da tenere a mente

$$G \leq \operatorname{Aut} F \rightsquigarrow K = \mathrm{Fix}_F(G) \subset F \xrightarrow[19.8]{} \mathrm{Gal}(F/K) = G$$

$$K \subset F \rightsquigarrow G = \mathrm{Gal}(F/K) \leq \operatorname{Aut} F \xrightarrow[19.7.(3)]{\text{se } G \text{ è finito}} K \underset{\underset{\neq}{\text{in generale}}}{\subset} \mathrm{Fix}_F(G) \subset F$$

20. Estensioni di Galois

20.1. Teorema

Per un'estensione di campi $K \subset F$ sono equivalenti i seguenti enunciati:

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

Se $K \subset F$ soddisfa $(1) - (3)$, diciamo che $K \subset F$ è un'**estensione di Galois**

Dimostrazione.

"$(1) \Rightarrow (2), (3)$": Per 19.8 sappiamo che $\operatorname{Gal}(F/K) = G$ e $[F : K] = |G|$ per 19.5

"$(2) \Rightarrow (1)$": Per l'Osservazione in 19.6 $\operatorname{Gal}(F/K)$ è finito

"$(3) \Rightarrow (2)$": Sia $G = \operatorname{Gal}(F/K)$. Sappiamo che $K \subset L := \operatorname{Fix}_F(G) \subset F$ è un campo intermedio con $[F : L] = |G|$ per 19.5.
Segue che $[F : L] = [F : K]$, perciò $[L : K] = 1$ e $K = L$

□

20.2. Esempi

1. $\mathbb{Q} \subset \mathbb{Q}(\sqrt{d})$, dove d è prodotto di primi distinti, 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 $\mathcal{P}$ il suo sottocampo fondamentale, allora $\mathcal{P} \subset F$ è un'estensione di Galois con $\operatorname{Gal}(F/\mathcal{P}) = \operatorname{Aut} F$ generato dall'omomorfismo di Frobenius. Infatti, se $p = \operatorname{char} F$ e $\varphi : F \to F, x \mapsto x^p$, allora
   $G = \langle \varphi \rangle \leq \operatorname{Aut} F \leq \mathrm{S}(F)$ è finito. Verifichiamo che $\mathcal{P} = \operatorname{Fix}_F(G)$:
   Abbiamo $\mathcal{P} \subset \operatorname{Fix}_F(G) \subset \{a \in F \mid a \text{ è zero di } x^p - x\} = \mathcal{P}$
   Perciò $\mathcal{P} \subset F$ è un'estensione di Galois con $\langle \varphi \rangle = \operatorname{Gal}(F/\mathcal{P}) = \operatorname{Aut} F$

20.3. Teorema fondamentale della teoria di Galois

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

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

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

Sono corrispondenze biunivoche mutualmente inverse che invertono l'ordine dato dall'inclusione "$\subseteq$".
Inoltre per ogni campo intermedio $K \subset L \subset F$ si ha

1. $L \subset F$ è un'estensione di Galois
2. Se $H = \mathrm{Gal}(F/L)$, allora $[L : K] = [G : H]$
3. Sono equivalenti i seguenti enunciati:
   a) $K \subset L$ è un'estensione di Galois
   b) $H \lhd G$
   c) $\varphi(L) \subset L$ per ogni $\varphi \in G$

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

Riassumendo:

$$\overbrace{\underbrace{K \quad \subset \quad L}_{\substack{\text{di grado } [G:H] \\ \text{di Galois} \\ \Leftrightarrow H \lhd G \\ \Rightarrow \mathrm{Gal}(L/K) \cong G/H}} \underbrace{\quad \subset \quad F}_{\substack{\text{Galois} \\ \text{di grado } H \\ \text{dove } H = \mathrm{Gal}(F/L)}}}^{\text{Galois di grado } |G|}$$

Dimostrazione.
Siano $n := [F : K] = |G|$, $K = \mathrm{Fix}_F(G)$.
Sappiamo per 19.8 che

$$\mathcal{H} \xrightarrow{\mathrm{Fix}} \mathcal{L} \xrightarrow{\mathrm{Gal}} \mathcal{H}, H \longmapsto \mathrm{Fix}_F(H) \longmapsto \mathrm{Gal}(F/\,\mathrm{Fix}_F(H)) = H$$

coincide con l'identità su $\mathcal{H}$.
Consideriamo un campo intermedio $K \subset L \subset F$ e $H := \mathrm{Gal}(F/L)$.

$$K \subset L \subset L' := \mathrm{Fix}_F(H) \subset F$$

Vogliamo mostrare $L = L'$. Basta verificare $[L' : K] = [L : K]$, ovvero "$\leq$".

(i) $[L' : K] = \dfrac{[F : K]}{[F : L']} = \dfrac{|G|}{|H|} = [G : H] = r$

(ii) Se $g, \tilde{g} \in G$, allora

$$gH = \tilde{g}H \Leftrightarrow g^{-1}\tilde{g} \in H \Leftrightarrow g^{-1}\tilde{g}(a) = a \text{ per ogni } a \in L \Leftrightarrow \tilde{g}(a) = g(a) \text{ per ogni } a \in L$$

(iii) Se $G/H = \{g_1H, \ldots, g_rH\}$ con $g_1 = \mathrm{id}_F$, $g_2, \ldots, g_r \in G$, allora $\varphi_i := g_i\big|_L : L \to F$, per $1 \le i \le r$ sono r omomorfismi distinti per (ii)

(iv) $K = \{a \in L \mid \overset{\overset{a}{\shortparallel}}{\varphi_1}(a) = \ldots = \varphi_r(a)\} \subset L$

"$\subseteq$" : ✓

"$\supseteq$" : Sia $a \in L$ con $\varphi_1(a) = \ldots = \varphi_r(a)$ e sia $g \in G$. Allora $gH = g_iH$ per un $1 \le i \le r$ e per (ii) abbiamo $g(a) = g_i(a) = \varphi_i(a) = \varphi_1(a) = a$. Dunque $a \in \mathrm{Fix}_F(G) = K$

(v) Concludiamo da 19.3 che $[L : K] \ge r \underset{(i)}{=} [L' : K]$

Perciò $L = L' = \mathrm{Fix}_F(H)$ e abbiamo verificato (1) e (2).
Inoltre

$$\mathcal{L} \xrightarrow{\text{Gal}} \mathcal{H} \xrightarrow{\quad\text{Fix}\quad} \mathcal{L}$$

$$L \mapsto H = \mathrm{Gal}(F/L) \mapsto \mathrm{Fix}_F(H) = L$$

è l'identità su $\mathcal{L}$.
Resta da dimostrare (3).

$(b) \Leftrightarrow (c)$: Sia $\varphi \in G$. Abbiamo un campo intermedio $K \subset \underbrace{\varphi(L) \subset F}_{\substack{\text{estensione di Galois}\\ \text{per (1)}}}$ con

$$\begin{aligned}\mathrm{Gal}(F/\varphi(L)) &= \{\psi \in \mathrm{Aut}\,F \mid \psi(\varphi(a)) = \varphi(a) \text{ per ogni } a \in L\}\\ &= \{\psi \in \mathrm{Aut}\,F \mid \varphi^{-1}\psi\varphi(a) = a \text{ per ogni } a \in L\}\\ &= \{\psi \in \mathrm{Aut}\,F \mid \varphi^{-1}\psi\varphi \in \mathrm{Gal}(F/L) = H\} = \varphi H \varphi^{-1}\end{aligned}$$

Quindi

$$(*) \qquad [F : \varphi(L)] = |\,\mathrm{Gal}(F/\varphi(L))| = |H| = [F : L]$$

.

Inoltre $$\begin{aligned} H \lhd G &\Leftrightarrow \varphi H \varphi^{-1} = H \text{ per ogni } \varphi \in G\\ &\Leftrightarrow \mathrm{Gal}(F/\varphi(L)) = H = \mathrm{Gal}(F/L) \text{ per ogni } \varphi \in G\\ &\underset{\substack{\text{Gal}\\ \text{è iniettiva}}}{\Leftrightarrow} \varphi(L) = L \Leftrightarrow \varphi(L) \subseteq L\end{aligned}$$

Infatti se $K \subset \varphi(L) \subset L \subset F$, allora $\varphi(L) = L$ per $(*)$ e il Lemma del Grado.

$(a) \Rightarrow (c)$: Sia $r = [L : K] = \mathrm{Gal}(L/K)$ e siano $\psi_1, \ldots, \psi_r$ gli omomorfismi distinti di $\mathrm{Gal}(L/K)$. Essi inducono r omomorfismi distinti $\varphi_i : L \to L \subset F$. Supponiamo che esista $\varphi \in G$ tale che $\varphi(L) \not\subset L$. Allora $\varphi_1, \ldots, \varphi_r, \varphi|_L$ sono $r+1$ omomorfismi distinti con $K = \{a \in L \mid a = \varphi_1(a) = \ldots = \varphi_r(a) = \varphi|_L\} \subset L$

"$\subseteq$": ✓

"$\supseteq$": Sia $a \in L$ con $\varphi_1(a) = \ldots = \varphi_r(a) = \varphi(a)$. Allora $a \in \mathrm{Fix}_L(\mathrm{Gal}(L/K)) = K$.

Per 19.3 abbiamo $r = [L : K] \geq r + 1$ $\lightning$

$(c) \Rightarrow (a)$: Ogni $\varphi \in G$ induce un automorfismo $\tilde{\varphi} = \varphi|_L \in \mathrm{Aut}\, L$ che appartiene a $\mathrm{Gal}(L/K)$. L'applicazione $\nu : G \to \mathrm{Gal}(L/K), \varphi \mapsto \tilde{\varphi}$ è un omomorfismo di gruppi:

$$\nu(\varphi \circ \psi) = (\varphi\psi)|_L = \varphi|_L \circ \psi|_L = \nu(\varphi) \circ \nu(\psi)$$

con nucleo $\{\varphi \in G \mid \varphi|_L = \mathrm{id}_L\} = \mathrm{Gal}(F/L) = H$.
Perciò $[G : H] = |\,\mathrm{im}\,\nu| \leq |\,\mathrm{Gal}(L/K)|$.
Ma sappiamo che $|\,\mathrm{Gal}(L/K)|$ divide $[L : K] \underset{(2)}{=} [G : H]$.
Perciò $[G : H] = |\,\mathrm{im}\,\nu| = |\,\mathrm{Gal}(L/K)| = [L : K]$.
Dunque $K \subset L$ è un'estensione di Galois e ν è suriettivo, perciò $G/H \cong \mathrm{Gal}(L/K)$.

□

20.4. Calcolo del polinomio minimo

Siano $K \subset F$ un'estensione di Galois e $\alpha \in F$. Sia $G = \mathrm{Gal}(F/K)$ e siano $\alpha_1, \ldots, a_r \in F$ gli elementi distinti dell'insieme $\{\psi(a) \mid \psi \in G\}$.
Allora $f = (x - a_1) \cdot \ldots \cdot (x - a_r)$ è il polinomio minimo di α su K.
In particolare $K \subset F$ è finita, normale e separabile.

Dimostrazione.
Sia $h \in K[x]$ il polinomio minimo di α su K.

$$\text{Mostriamo} \begin{array}{l} \left.\begin{array}{ll} (i) & f \in K[x] \\ (ii) & f(\alpha) = 0 \end{array}\right\} \Rightarrow h \mid f \\ (iii)\ \deg h = \deg f \end{array} \left.\vphantom{\begin{array}{l} a \\ b \\ c \end{array}}\right\} \Rightarrow h = f$$

(i) Sia $\varphi \in G$ e sia $\tilde{\varphi} : F[x] \to F[x], \sum_{i=0}^n b_i x^i \mapsto \sum_{i=0}^n \varphi(b_i) x^i$.
Poiché $\{\varphi(a_1), \ldots, \varphi(a_r)\} = \{\varphi\psi(\alpha) \mid \psi \in G\} = \{a_1, \ldots, a_r\}$ si ha

$$\tilde{\varphi}(f) \underset{\substack{\tilde{\varphi} \\ \text{omomorfismo}}}{=} (x - \varphi(a_1)) \cdot \ldots \cdot (x - \varphi(a_r)) = f$$

e perciò i coefficienti di f appartengono a $\mathrm{Fix}_F(G) = K$, ovvero $f \in K[x]$

(*ii*) $\alpha = \mathrm{id}_F(\alpha) \in \{a_1, \ldots, a_r\}$ è zero di f

(*iii*) Per (*i*) e (*ii*) sappiamo $h \mid f$, perciò $\deg h \leq \deg f$.
Se $h = \sum_{i=0}^{n} c_i x^i$, allora per $a_j = \psi(\alpha)$ abbiamo

$$h(a_j) = \sum_{i=0}^{n} \underset{\substack{\| \\ \psi(c_i) \\ \text{poiché} \\ c_i \in K = \mathrm{Fix}_F(G)}}{c_i} a_j^i = \sum_{i=0}^{n} \psi(c_i)\psi(\alpha)^i = \psi\left(\sum_{i=0}^{n} c_i \alpha^i\right) = \psi(h(\alpha)) = \psi(0) = 0$$

Dunque h possiede almeno r zeri distinti, e $\deg h \geq r = \deg f$.
Concludiamo $\deg h = \deg f$ e $h = f$.

□

20.5. 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 finita, normale, separabile
3. F è il campo di riducibilità completa di un polinomio separabile su K

Dimostrazione.

(1) ⇒ (2): Per 20.4.

(2) ⇒ (3): Sappiamo che F è crc del polinomio $f = f_1 \cdot \ldots \cdot f_n$ dove f_i è il polinomio minimo di α_i e $F = K(\alpha_1, \ldots, \alpha_n)$, vedi 17.3.
Per ipotesi ogni f_i è separabile su K e perciò f è separabile su K.

(3) ⇒ (1): Sia $G = \mathrm{Gal}(F/K)$. Dobbiamo verificare che $K = \mathrm{Fix}_F(G)$.
Sappiamo che F è crc di di un polinomio separabile $f \in K[x]$.
Procediamo per induzione sul numero m di zeri di f in $F \setminus K$

<u>$m = 0$</u>: $F = K$, $\mathrm{Gal}(F/K) = \{\mathrm{id}_F\}$, $\mathrm{Fix}_F(G) = K$

<u>$m > 0$</u>: Sia $\alpha \in F \setminus K$ uno zero di f, e sia $L = K(\alpha)$. Allora

$$\underbrace{K \quad \subset \quad L}_{\substack{\text{di grado} \\ \deg h =: n \\ h \text{ polinomio} \\ \text{minimo di } \alpha \text{ su } K}} \underbrace{\quad \subset \quad F}_{\substack{\text{estensione di Galois} \\ \text{per ipotesi induttiva}}}$$

Sia $H = \mathrm{Gal}(F/L) \leq G$.
Abbiamo $\mathrm{Fix}_F(G) \subseteq \mathrm{Fix}_F(H) = L = K(\alpha)$ dove L ha K-base $\{1, \alpha, \ldots, \alpha^{n-1}\}$.
Sia adesso $a \in \mathrm{Fix}_F(G)$. Allora $a = \sum_{i=0}^{n-1} k_i \alpha^i$ con $k_0, \ldots, k_{n-1} \in K$.
Per ipotesi, l'estensione $K \subset F$ è normale, quindi h è prodotto di n fattori lineari in $F[x]$. Inoltre h è divisore irriducibile del polinomio separabile f.
Dunque h possiede n zeri distinti $\beta_1, \ldots, \beta_n \in F$.
Notiamo che α e β_j hanno lo stesso polinomio minimo h su K.
Per 17.4 esiste $\varphi_j \in \mathrm{Aut}\, F$ tale che $\varphi_j|_K = \mathrm{id}_K$ e $\varphi_j(\alpha) = \beta_j$.
Dunque esistono $\varphi_1, \ldots, \varphi_n \in G$ tali che $\varphi_j(\alpha) = \beta_j$ per $1 \leq j \leq n$.
Allora poiché $a \in \mathrm{Fix}_F(G)$, si ha per ogni $1 \leq j \leq n$

$$a = \varphi_j(a) = \varphi_j\left(\sum_{i=0}^{n-1} k_i \alpha^i\right) = \sum_{i=0}^{n-1} k_i \beta_j^i$$

In altre parole, il polinomio $g = a - \sum_{i=0}^{n-1} k_i x^i \in F[x]$ ha n zeri distinti, ma ha grado $< n$. Perciò $g = 0$ e $a = k_0 \in K$.

□

20.6. Esempio

Siano p, q due primi distinti e sia $\alpha = \sqrt{p} + \sqrt{q}$.
Allora $f = x^4 - 2(p+q)x^2 + (p-q)^2$ è il polinomio minimo di α su $\mathbb{Q}$
e $\mathbb{Q} \subset F := \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ è un'estensione di Galois di grado 4 con $\mathbb{Q}$-base $\{1, \sqrt{p}, \sqrt{q}, \sqrt{pq}\}$

Dimostrazione.
Si verifica che $f(\alpha) = 0$, dunque il polinomio minimo h di α su $\mathbb{Q}$ divide f e $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg h \leq 4$.

$$\overbrace{\underbrace{\mathbb{Q} \quad \subset \quad \mathbb{Q}(\sqrt{p})}_{\text{grado } 2} \quad \subset \quad \mathbb{Q}(\alpha)}^{\text{grado } < 4}$$

Mostriamo che $\mathbb{Q}(\sqrt{p}) \subsetneq \mathbb{Q}(\alpha)$. Infatti:

$$\alpha^2 = p + q + 2\sqrt{pq} = p + q + 2\sqrt{p}(\alpha - \sqrt{p}) = q - p + 2\sqrt{p}\alpha$$

Pertanto $\sqrt{p} = \frac{\alpha^{-1}}{2}(\alpha^2 + p - q) \in \mathbb{Q}(\alpha)$. Analogamente si vede che $\sqrt{q} \in \mathbb{Q}(\alpha)$.
Perciò abbiamo

$$\overbrace{\underbrace{\mathbb{Q} \quad \subset \quad \mathbb{Q}(\sqrt{p})}_{\text{grado } 2} \quad \subset \quad \mathbb{Q}(\sqrt{p}, \sqrt{q}) \quad \subset \quad \mathbb{Q}(\alpha)}^{\text{grado } < 4}$$

Si noti che $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$. Altrimenti

$\sqrt{q} = a + b\sqrt{p}$ con $a, b \in \mathbb{Q}$ e $b \neq 0$ (altrimenti $\sqrt{q} \in \mathbb{Q}$) e $a \neq 0$ (altrimenti $\sqrt{pq} \in Q$)

e $q = a^2 + 2ab\sqrt{p} + b^2 p$ e avremmo $\sqrt{p} \in Q$ $\quad \lightning$

Dunque concludiamo che $\mathbb{Q} \subset \mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\alpha)$ è un'estensione di grado 4.
Ciò mostra che f è il polinomio minimo di α su $\mathbb{Q}$. Inoltre gli elementi di $\operatorname{Aut} F = \operatorname{Gal}(F/\mathbb{Q})$ sono determinati da $\varphi(\sqrt{p})$ e $\varphi(\sqrt{q})$ poiché ogni elemento di F è di forma $a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq}$. Sappiamo che $\varphi(\sqrt{p}) = \pm\sqrt{p}$ e $\varphi(\sqrt{q}) = \pm\sqrt{q}$ poiché $(\varphi(\sqrt{p}))^2 = \varphi(p) = p$ e analogamente per q.
Segue che $|\operatorname{Gal}(F/\mathbb{Q})| = 4 = [F : \mathbb{Q}]$ e $\mathbb{Q} \subset F$ è un'estensione di Galois.

φ	$\sqrt{p}$	$\sqrt{q}$	$\operatorname{Fix}_F(H), H = \langle\varphi\rangle$	$\operatorname{ord}\varphi$
id_F	$\sqrt{p}$	$\sqrt{q}$	F	1
φ_1	$-\sqrt{p}$	$\sqrt{q}$	$\mathbb{Q}(\sqrt{q}) =: L_1$	2
φ_2	$\sqrt{p}$	$-\sqrt{q}$	$\mathbb{Q}(\sqrt{p}) =: L_2$	2
φ_3	$-\sqrt{p}$	$-\sqrt{q}$	$\mathbb{Q}(\sqrt{pq}) =: L_3$	2

$G \cong \mathcal{V}$ abeliano $\Rightarrow H_i \lhd G$ per $i = 1, 2, 3$

$$\begin{tikzcd}[column sep=small]
 & G \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & & & & F \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
H_1 \arrow[dr, dash] & H_2 \arrow[d, dash] & H_3 \arrow[dl, dash] \arrow[r, squiggly, shift left, "\mathrm{Fix}"] & & L_1 \arrow[l, squiggly, shift left, "\mathrm{Gal}"] \arrow[dr, dash] & L_2 \arrow[d, dash] & L_3 \arrow[dl, dash] \\
 & \{\mathrm{id}_F\} & & & & \mathbb{Q} &
\end{tikzcd}$$

$$\mathbb{Q} \underset{\substack{\text{Galois}\\ G/H_i\cong\mathbb{Z}/2\mathbb{Z}}}{\subset} L_i \underset{\substack{\text{Galois}\\ H_i\lhd G}}{\subset} F$$

Calcoliamo il polinomio minimo di α su L_i

$$\{\varphi(\alpha) \mid \varphi \in \operatorname{Gal}(F/L_i) = H_i\}, H_i = \{\mathrm{id}_F, \varphi_i\}$$

$\underline{i = 1}$ $\{\alpha, -\sqrt{p} + \sqrt{q}\}$

$$\begin{aligned} f_1 &= (x - \alpha)(x - (-\sqrt{p} + \sqrt{q})) \\ &= (x - \sqrt{p} - \sqrt{q})(x + \sqrt{p} - \sqrt{q}) \\ &= ((x - \sqrt{q}) - \sqrt{p})((x - \sqrt{q}) + \sqrt{p}) = x^2 - 2\sqrt{q}x + (q - p) \end{aligned}$$

$\underline{i = 2}$ $\{\alpha, \sqrt{p} - \sqrt{q}\}$

$$f_2 = x^2 - 2\sqrt{p}x + (p - q)$$

$\underline{i = 3}$ $\{\alpha, -\alpha\}$

$$f_3 = (x - \alpha)(x + \alpha) = x^2 - \alpha^2 = x^2 - (p + q) - 2\sqrt{pq}$$

$\square$

20.7. Teorema dell'elemento primitivo

Per ogni estensione finita e separabile $K \subset F$ esiste un elemento detto **primitivo** $\alpha \in F$ tale che $F = K(\alpha)$

21. Estensioni per radicali

L'equazione $x^2 + px + q = 0$ possiede le soluzioni $x_{1,2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$.
Formule simili esistono per le equazioni di grado 3 e 4. Per polinomi di grado $n \geq 5$?

Ipotesi generale: $n \in \mathbb{N}$ e K un campo la cui caratteristica non divide n

21.1. Radici n-sime dell'unità

Sia K_n il campo di riducibilità completa del polinomio $f = x^n - 1$ su K. Gli zeri di f, detti **radici n-sime dell'unità**, formano un sottogruppo ciclico $\mathrm{E}_n(K)$ di $(K_n \setminus \{0\}, \cdot)$ di ordine n.

Dimostrazione.
$\mathrm{E}_n(K) \leq (K_n \setminus \{0\}, \cdot)$ è ciclico (Esercizio). Inoltre $\mathcal{D}f = nx^{n-1}$ non ha zeri in comune con con f. Perciò f ha n zeri distinti e $\mathrm{E}_n(K) \cong (\mathbb{Z}/n\mathbb{Z}, +)$.

□

21.2. Radici n-sime di un elemento

Sia $a \in K \setminus \{0\}$ e sia F il campo di riducibilità completa del polinomio $f = x^n - a$ su K. Gli zeri di f sono detti **radici n-sime di** a.

1. F contiene il campo di riducibilità completa K_n di $x^n - 1$ su K.

2. Se $\mathrm{E}_n(K) = \{z_0 = 1, z_1, \ldots, z_{n-1}\}$, e α è uno zero di f, allora $\{\alpha, z_1\alpha, \ldots, z_{n-1}\alpha\}$ sono le radici n-sime di a.

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

4. Se K contiene tutte le radici n-sime dell'unità, allora $F = K(\alpha)$ e $\mathrm{Gal}(F/K)$ è ciclico.

Dimostrazione.

1. Come in 21.1 vediamo che f possiede n zeri distinti $\alpha = \alpha_1, \ldots, \alpha_n$.
   Allora $1 = \alpha^{-1}\alpha_1, \ldots, \alpha^{-1}\alpha_n$ sono le n radici distinte dell'unità.
   Quindi $K_n \subset F$

2. ✓

3. Per (1) e (2) $F = K(z_0, \ldots, z_n, \alpha) = K_n(\alpha)$. Inoltre F è crc del polinomio separabile f, perciò $K \subset F$ è un'estensione di Galois (20.5)

4. Sia $G = \mathrm{Gal}(F/K)$. Per ogni $\sigma \in G$ si ha $(\sigma(\alpha))^n = \sigma(\alpha^n) = \sigma(a) = a$, perciò $\sigma(\alpha)$ è una radice n-sima di a e $\sigma(\alpha)\alpha^{-1} \in \mathrm{E}_n(K)$. Ciò permette di definire un'applicazione
$$\begin{aligned} \psi : G &\longrightarrow \mathrm{E}_n(K) \\ \sigma &\longmapsto \sigma(\alpha)\alpha^{-1} \end{aligned}$$
ψ è un omomorfismo di gruppi: siano $\sigma_1, \sigma_2 \in G$
$$\begin{aligned} \psi(\sigma_1) \cdot \psi(\sigma_2) &= \sigma_1(\alpha)\alpha^{-1}\sigma_2(\alpha)\alpha^{-1} \\ &\underset{(*)}{=} \sigma_1(\alpha)\sigma^{-1}\sigma_1(\sigma_2(\alpha)\alpha^{-1}) \\ &= \sigma_1(\alpha\sigma_2(\alpha)\alpha^{-1})\alpha^{-1} \\ &= \sigma_1(\sigma_2(\alpha))\alpha^{-1} \\ &= (\sigma_1 \circ \sigma_2)(\alpha)\alpha^{-1} = \psi(\sigma_1 \circ \sigma_2) \end{aligned}$$
$$(*) \quad \underset{\mathrm{Gal}(F/K)}{\underset{\cap}{\sigma_1}}\underbrace{(\sigma_2(\alpha)\alpha^{-1})}_{\underset{\mathrm{E}_n(K)\subset K}{\cap}} = \sigma_2(\alpha)\alpha^{-1}$$
ψ è iniettivo: Se $\psi(\sigma) = e_{\mathrm{E}_n(K)} = 1_K$, allora $\sigma(\alpha) = \alpha$. Poiché $\sigma|_K = \mathrm{id}_K$ e $F = K(\alpha)$, segue $\sigma = \mathrm{id}_F$.
Concludiamo che $G \cong \operatorname{im}\psi \leq \mathrm{E}_n(K)$ che è ciclico, quindi G è ciclico.

□

21.3. Radici primitive dell'unità

1. Le radici n-sime dell'unità che generano il gruppo ciclico $E_n(K)$ si dicono **primitive**. Se z è una radice primitiva dell'unità, allora $\mathrm{E}_n(K) = \{z^m \mid m = 0, \ldots, n-1\}$.

2. $K \subset K_n$ è un'estensione di Galois e $\mathrm{Gal}(K_n/K)$ è isomorfo a un sottogruppo di $(\mathbb{Z}/n\mathbb{Z}^*, \cdot)$ ed è abeliano.

Dimostrazione.

1. $$\begin{aligned} \mathrm{E}_n(K) &\cong (\mathbb{Z}/n\mathbb{Z}^*, \cdot) \\ z^m &\longmapsto [m] \end{aligned}$$
e $\mathrm{ord}(z^m) = \mathrm{ord}([m]) = \frac{n}{\mathrm{MCD}(m,n)}$
quindi z^m primitivo $\Leftrightarrow \mathrm{ord}(z^m) = n \Leftrightarrow \mathrm{MCD}(m,n) = 1$

2. $K \subset K_n$ è di Galois poiché K_n è crc del polinomio separabile $x^n - 1$.
Sia $G = \mathrm{Gal}(K_n/K)$. Se $z \in K_n$ e $\sigma \in G$, allora $\sigma(z^d) = \sigma(z)^d = 1 \Leftrightarrow z^d = 1$

Quindi z è una radice primitiva se e solo se lo è $\sigma(z)$.
Possiamo quindi definire un'applicazione a partire da una radice primitiva z

$$\begin{array}{rcl} \psi := \psi_z : G & \longrightarrow & (\mathbb{Z}/n\mathbb{Z}^*, \cdot) \\ \sigma & \longmapsto & [m] \\ & & \text{dove } \sigma(z) = z^m \end{array}$$

(si rammenti che $\sigma(z)$ è primitiva e perciò di forma z^m con $\mathrm{MCD}(m,n) = 1$, e $\mathbb{Z}/n\mathbb{Z} = \{[m] \mid \mathrm{MCD}(m,n) = 1\}$)

ψ è omomorfismo di gruppi:
Se $\sigma_1, \sigma_2 \in G$ soddisfano $\sigma_1(z) = z^{m_1}$ e $\sigma_2(z) = z^{m_2}$, allora
$(\sigma_1 \circ \sigma_2)(z) = \sigma_1(z^{m_2}) = z^{m_1 m_2}$, perciò

$$\psi(\sigma_1 \circ \sigma_2) = [m_1 m_2] = [m_1] \cdot [m_2] = \psi(\sigma_1) \cdot \psi(\sigma_2)$$

ψ iniettiva:
Se $\psi(\sigma) = [1]$, allora $\sigma(z) = z^m$ dove $[m] = [1]$, ovvero $m = qn + 1$ per un $q \in \mathbb{Z}$.
Perciò $\sigma(z) = z^{qn+1} = z^{qn} \cdot z = z$.
Poiché $K_n = K(z)$ e $\sigma|_K = \mathrm{id}_K$, segue $\sigma = \mathrm{id}_K$.
Concludiamo che $G \cong \operatorname{im}\psi \leq \mathbb{Z}/n\mathbb{Z}^*$ che è abeliano, quindi G è abeliano.

□

21.4. Osservazione

L'ipotesi generale all'inizio del capitolo può essere fatta senza perdita di generalità: se K è un campo la cui caratteristica p divide n, possiamo scrivere $n = p^k m$ con $\mathrm{MCD}(p,m) = 1$ e scrivere $x^n - 1 = (x^m - 1)^{p^k}$ dove $x^m - 1$ è separabile su K e si vede che $\mathrm{E}_n(K) = \mathrm{E}_m(K)$ è un gruppo ciclico di ordine m.
D'ora in avanti assumiamo $\operatorname{char} K = 0$, anche se i risultati che seguono valgono per qualsiasi campo K.

21.5. Definizione

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

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

tale 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 $a_i \in L_{i-1}$.

21.6. Osservazioni

1. In 21.5 possiamo sempre assumere che $K \subset F$ sia un'estensione di Galois. Infatti, data un'estensione per radicali $K \subset F$, possiamo sempre trovare $F \subset F'$ tale che $K \subset F \subset F'$ è un'estensione per radicali e $K \subset F'$ è di Galois.
   Si dimostra per induzione su n (vedi filo rosso).

2. Un'estensione per radicali $K = L_0 \subset L_1 \subset \ldots \subset L_n = F$ che sia anche un'estensione di Galois da luogo a una catena di sottogruppi
   $$\{\mathrm{id}_F\} = H_n \leq \ldots \leq H_2 \leq H_1 \leq G = \mathrm{Gal}(F/K)$$
   dove $H_i = \mathrm{Gal}(F/L_i)$

Richiamo

Un gruppo G è risolubile se possiede una catena di sottogruppi
$$\{e\} = H_n \leq \ldots H_2 \leq H_1 \leq H_0 = G$$
tale che

1. $H_i \lhd H_{i-1}$
2. H_{i-1}/H_i è abeliano

per ogni $1 \leq i \leq n$.
Sappiamo:

- Se G è risolubile, allora lo è anche G/N per ogni $N \lhd G$.
- G è risolubile se e solo se esiste $N \lhd G$ tale che N e G/N sono risolubili.

21.7. Lemma

1. Siano $K \subset L \subset F$ tali che $K \subset L$ e $K \subset F$ sono estensioni di Galois.
   Se $\mathrm{Gal}(F/K)$ è risolubile, lo è anche $\mathrm{Gal}(L/K)$.

2. Se $K = L_0 \subset L_1 \subset \ldots \subset L_n = F$ è una catena di campi intermedi tale che $L_{i-1} \subset L_i$ è un'estensione di Galois con $\mathrm{Gal}(L_i/L_{i-1})$ risolubile per ogni $1 \leq i \leq n$ e $K \subset F$ è un'estensione di Galois, allora $G = \mathrm{Gal}(F/K)$ è risolubile.

Dimostrazione.
Si rammenti che se $K \subset F$ e $K \subset L$ sono estensioni di Galois, allora

$$\underbrace{K \subset L}_{G/N} \underbrace{\subset F}_{N \lhd G}$$

$\square$

21.8. Definizione

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

21.9. Teorema di Galois

Per un polinomio $f \in K[x]$ sono equivalenti i seguenti enunciati:

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

Dimostrazione.

(1) $\Rightarrow$ (2):

Per 21.6 possiamo supporre che esista un'estensione di Galois $K \subset F$ tale che

(i) $K \subset F$ è un'estensione per radicali

(ii) f è prodotto di fattori lineari in $F[x]$

Si ha quindi una catena di campi intermedi

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

di forma $L_i = L_{i-1}(\alpha_i)$, dove α_i è radice n_i-sima di un elemento di L_{i-1}.
Per *(ii)* F contiene un crc E di f su K. Poiché K è perfetto, f è separabile su K e quindi $K \subset E$ è un'estensione di Galois. Applicando 21.7(2) a $K \subset E \subset F$, basta mostrare che $\mathrm{Gal}(F/K)$ è risolubile per concludere che $\mathrm{Gal}(f/K) = \mathrm{Gal}(E/K)$ è risolubile. Procediamo per induzione su m.

$\underline{m = 0}$: $K = F$, $\mathrm{Gal}(F/K) = \{\mathrm{id}_F\}$ è risolubile

$\underline{m > 0}$: $K = L_0 \subset L_1 = K(\alpha_1) \subset L_2 \subset \ldots \subset L_m = F$ dove $\alpha := \alpha_1$ è una radice $n := n_1$-esima di un elemento di K. Per ricondurci al caso considerato in 21.2, aggiungiamo a K le radici n-sime dell'unità. Sostituiamo quindi l'estensione $K \subset F$ con $K_n := K(z) \subset F(z) =: F'$ dove z è una radice primitiva n-sima dell'unità. Si noti che $K \subset F'$ è un'estensione di Galois.
Infatti se F è crc del polinomio g su K, allora F' è crc di $g(x^n - 1)$. Abbiamo

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

Per 21.7(2) basta verificare che $G = \mathrm{Gal}(F'/K)$ è risolubile.
Dalla catena di campi intermedi

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

otteniamo

$$K_n = K(z) = L_0(z) \subset L_1(z) \subset L_2(z) \subset \ldots \subset L_m(z) = F'$$

Poniamo $L := L_1(z)$. Per ipotesi induttiva $H := \mathrm{Gal}(F'/L)$ è risolubile. Consideriamo

$$\overbrace{\underbrace{K \quad \subset \quad K_n}_{\substack{21.2 \\ 21.3}\ \substack{\text{di Galois} \\ \mathrm{Gal}(K_n/K) \\ \text{abeliano}}} \quad \subset \quad \underbrace{L = K_n(\alpha)}_{\substack{\text{di Galois} \\ \mathrm{Gal}(L/K_n) \\ \text{ciclico}}} \quad \underbrace{\subset \quad F'}_{H}}^{G}$$

Per 21.7(2) concludiamo che G è risolubile.

(2) $\Rightarrow$ (1): vedi filo rosso.

$\square$

22. Risolubilità del polinomio generale di grado n

Sia $\operatorname{char} K = 0$

22.1. Proposizione

Sia $f \in K[x]$ un polinomio di grado $n > 0$. Allora $\operatorname{Gal}(f/K)$ è isomorfo ad un sottogruppo di S_n.

Dimostrazione.
$\operatorname{Gal}(f/K) = \operatorname{Gal}(E/K)$ dove $E = K(\alpha_1, \ldots, \alpha_n)$ è un crc di f su K e $\alpha_1, \ldots, \alpha_n$ sono gli zeri di f in E.
Se $\sigma \in \operatorname{Gal}(f/K)$ e $f = \sum_{i=0}^{n} a_i x^i$, allora

$$f(\sigma(\alpha_j)) = \sum_{i=0}^{n} \underset{\substack{\Cap \\ K \\ \Rightarrow a_i = \sigma(a_i)}}{a_i} \, \sigma(\alpha_j)^i = \sigma\left(\sum_{i=0}^{n} \alpha_j^i\right) = \sigma(f(\alpha_j)) = 0$$

Dunque σ induce una permutazione degli zeri di f, e possiamo definire

$$\begin{aligned} \Psi : \operatorname{Gal}(f/K) &\longrightarrow S_n \\ \sigma &\longmapsto \sigma\big|_{\{\alpha_1, \ldots, \alpha_n\}} \end{aligned}$$

Ψ omomorfismo:

$$\Psi(\sigma\tau) = \sigma\tau\big|_{\{\alpha_1, \ldots, \alpha_n\}} = \sigma\big|_{\{\alpha_1, \ldots, \alpha_n\}} \circ \tau\big|_{\{\alpha_1, \ldots, \alpha_n\}} = \Psi(\sigma) \circ \Psi(\tau)$$

Ψ iniettivo: Se $\Psi(\sigma) = \sigma\big|_{\{\alpha_1, \ldots, \alpha_n\}} = \operatorname{id}_{\{\alpha_1, \ldots, \alpha_n\}}$ allora poiché $\sigma\big|_K = \operatorname{id}_K$ e
$E = K(\alpha_1, \ldots, \alpha_n)$ si ha $\sigma = \operatorname{id}_E$.

$\square$

22.2. Corollario

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

Dimostrazione.
$\operatorname{Gal}(f/K)$ è isomorfo a un sottogruppo di S_n con $n \leq 4$ ed è quindi risolubile per quanto visto in 4.7, 4.8.

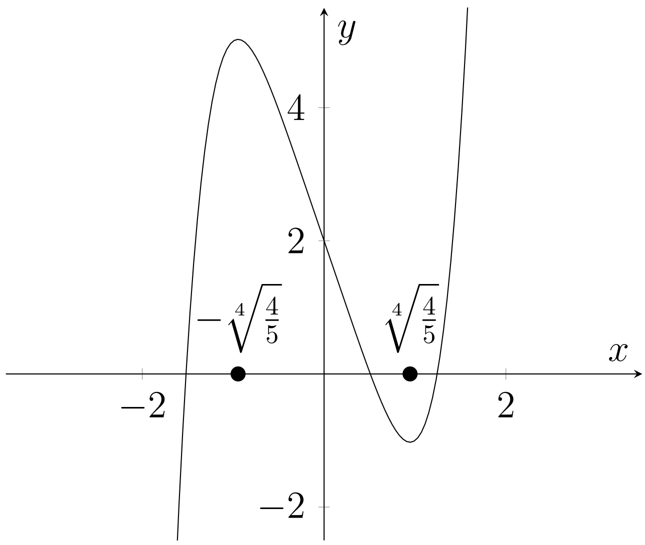
$\square$

22.3. Esempi

1. L'equazione $x^5 = 1$ è risolubile per radicali poiché $\mathrm{Gal}(x^n - 1/K) = \mathrm{Gal}(K_n/K)$ è abeliano (21.3)

2. $f = x^5 - 10x^4 + 27x^3 - 18x^2 + 30x + 50 = (x-5)^2(x^3 + 2x + 2) \in \mathbb{Q}[x]$
   L'equazione $f(x) = 0$ è risolubile per radicali poiché
   $\mathrm{Gal}(f/\mathbb{Q}) = \mathrm{Gal}(x^3 + 2x + 2/\mathbb{Q})$ è risolubile per 22.2

3. Per il polinomio $f = x^5 - 4x + 2 \in \mathbb{Q}[x]$ l'equazione $f(x) = 0$ **non** è risolubile per radicali.



Quindi f ha tre zeri reali e due complessi α, $\overline{\alpha}$.
Dunque se E è il crc di f su $\mathbb{Q}$, abbiamo $\underbrace{\mathbb{Q} \subset \mathbb{Q}(\alpha)}_{\substack{\text{grado 5 con} \\ f \text{ polinomio minimo di } \alpha}} \subset E$. Perciò $5 \mid \underbrace{|\mathrm{Gal}(f/\mathbb{Q})|}_{= [E:\mathbb{Q}]}$.

Per il Teorema di Cauchy $G := \mathrm{Gal}(f/\mathbb{Q})$ contiene un elemento di ordine 5. Inoltre contiene un elemento di ordine 2 dato dalla coniugazione.
Poiché $G \leq S_5$ e contiene un elemento di ordine 5 e un elemento di ordine 2, concludiamo $G = S_5$ (Esercizio). Dunque G non è risolubile (4.7, 4.8).

22.4. Definizione

1. Per $n \in \mathbb{N}$ definiamo ricorsivamente
$$K[x_1, x_2] = K[x_1][x_2]$$
$$K[x_1, \ldots, x_n] = K[x_1, \ldots, x_{n-1}][x_n]$$
l'**anello dei polinomi** $R := K[x_1, \ldots, x_n]$ nelle variabili $x_1, \ldots, x_n$.
I suoi elementi sono di forma
$$\sum_{\substack{(i_1,\ldots,i_n)\in I \\ I\subset\mathbb{N}_0^n \text{ finito}}} a_{(i_1,\ldots,i_n)} x_1^{i_1} \cdot \ldots \cdot x_n^{i_n}$$

2. Il campo delle funzioni razionali $F = K(x_1, \ldots, x_n)$ è dato dagli elementi $\frac{f}{g} = \frac{f(x_1,\ldots,x_n)}{g(x_1,\ldots,x_n)}$, $f, g \in K[x_1, \ldots, x_n]$ e $g \neq 0$

3. Ogni permutazione $\sigma \in S_n$ definisce un automorfismo $\tilde{\sigma} : F \to F$ con
$$\tilde{\sigma}\left(\frac{f}{g}\right) = \tilde{\sigma}\left(\frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)}\right) = \frac{f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})}{g(x_{\sigma(1)}, \ldots, x_{\sigma(n)})}$$

22.5. Esempio

$n = 2$: $R = K[x, y]$, $F = K(x, y)$, $\sigma = \begin{pmatrix}1 & 2\end{pmatrix}$
$$\tilde{\sigma}\left(\frac{x+2y}{x+y}\right) = \frac{y+2x}{y+x} \qquad \tilde{\sigma}\left(\frac{xy}{x+y}\right) = \frac{xy}{x+y}$$

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

22.6. Definizione

I seguenti polinomi di $R = K[x_1, \ldots, x_n]$ sono detti **funzioni simmetriche elementari** nelle variabili $x_1, \ldots, x_n$.
$$\begin{aligned}
s_0 &= 1 \\
s_1 &= x_1 + \ldots + x_n \\
s_2 &= x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n = \sum_{i<j} x_i x_j \\
s_3 &= \sum_{i<j<k} x_i x_j x_k \\
&\vdots \\
s_n &= x_1 \cdot \ldots \cdot x_n
\end{aligned}$$

22.7. Proposizione

Sia $f = (x - x_1) \cdot \ldots \cdot (x - x_n) \in F[x]$

1. Newton
$$f = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \ldots + (-1)^n s_n = \sum_{i=0}^{n} (-1)^i s_i x^{n-i} \in L[x]$$
2. $F = L(s_1, \ldots, s_n)$ e F è il campo di riducibilità completa di f su L
3. $\mathrm{Gal}(f/L) = S_n$

Dimostrazione.

1. Per induzione su n:

$\underline{n = 2}$: $f = (x - x_1)(x - x_2) = x^2 - (\overset{\overset{s_1}{\parallel}}{x_1 + x_2})x + \overset{\overset{s_2}{\parallel}}{x_1 x_2}$

$\underline{n \to n + 1}$:

$$\begin{aligned} f &= (x - x_1) \cdot \ldots \cdot (x - x_n)(x - x_{n+1}) \\ &\underset{\substack{s_i \text{ elementari} \\ \text{in } n \text{ variabili}}}{=} \sum_{i=0}^{n} (-1)^i s_i x^{n-i+1} - \sum_{i=0}^{n} (-1)^i s_i x^{n-i} x_{n+1} \\ &= \underset{i=0}{x^{n+1}} \underbrace{-\underset{i=1}{(x_1 + \ldots + x_n)x^n} - \underset{i=0}{x_{n+1}x^n}}_{\substack{-\tilde{s}_1 x^n \\ \text{elementare in} \\ n+1 \text{ variabili}}} + \underbrace{\underset{i=2}{\sum_{i<j\le n} x_i x_j x^{n-1}} + \underset{i=1}{\sum_{i=1}^{n} x_i x_{n+1} x^{n-1}}}_{\tilde{s}_2 x^{n-1}} - \ldots \end{aligned}$$

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 $\mathrm{Gal}(F/L) = S_n$, quindi $[F : L] = n!$.
D'altra parte possiamo considerare F come crc di f su $K(s_1, \ldots, s_n)$, perciò $[F : K(s_1, \ldots, s_n)] \le n!$ e $K(s_1, \ldots, s_n) = L$ per il Lemma del Grado.
Dunque $\mathrm{Gal}(f/L) = \mathrm{Gal}(F/L) = S_n$.

□

22.8. Teorema di Abel-Ruffini

Per il polinomio generale p di grado $n \geq 5$ l'equazione $p(x) = 0$ non è risolubile per radicali. Più precisamente: se $p = x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \in K[x]$ allora nell'anello $K(a_1, \ldots, a_n)[x]$ si ha

1. $\mathrm{Gal}(p/K(a_1, \ldots, a_n)) = S_n$
2. $p(x) = 0$ non è risolubile per radicali su $K(a_1, \ldots, a_n)$

Dimostrazione.
(2) segue da (1) per il Teorema di Galois.

1. Sia E il crc di p su $K(a_1, \ldots, a_n)$ e siano $\alpha_1, \ldots, \alpha_n \in E$ gli zeri di p.
   Allora in $E[x]$ si ha

   $$p = (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n) = \sum_{k=0}^{n} (-1)^k \tilde{s}_k x^{n-k}$$

   dove $\tilde{s}_1, \ldots, \tilde{s}_n$ sono le funzioni elementari simmetriche nelle variabili $\alpha_1, \ldots, \alpha_n$.
   Confrontando i coefficienti, vediamo che $a_k = (-1)^k \tilde{s}_k$ per $1 \leq k \leq n$.
   Consideriamo l'isomorfismo di anelli

   $$\varphi : R = K[x_1, \ldots, x_n] \longrightarrow K[\alpha_1, \ldots, \alpha_n], x_i \mapsto \alpha_i$$

   si ha $\varphi(s_k) = \tilde{s}_k$, quindi $\varphi((-1)^k s_k) = a_k$ per $1 \leq k \leq n$ con la notazione di 22.7.
   φ induce un isomorfismo

   $$\varphi' : K[s_1, \ldots, s_n] \longrightarrow K[a_1, \ldots, a_n]$$

   e perciò anche un isomorfismo di campi

   $$\psi : L = K(s_1, \ldots, s_n) \longrightarrow K(a_1, \ldots, a_n)$$

   e perciò anche un isomorfismo

   $$\tilde{\psi} : L[x] \longrightarrow K(a_1, \ldots, a_n)[x]$$

   Si noti che nella notazione di 22.7 $\tilde{\psi}(f) = (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n) = p$
   Abbiamo

   $$\begin{array}{ccccl} L & \subset & F & & \text{crc di } f \text{ su } L \ (22.7) \\ \psi \ \wr\!\wr & & \downarrow \cong & & \\ K(a_1, \ldots, a_n) & \subset & E & & \text{crc di } p \text{ su } K(a_1, \ldots, a_n) \end{array}$$

   Per 14.3, 14.4 ψ può essere esteso a un isomorfismo $F \cong E$.
   Dunque $\mathrm{Gal}(E/K(a_1, \ldots, a_n)) = \mathrm{Gal}(F/L) \cong S_n$.

□

22.9. Ancora sul caso $n \leq 4$

Sia $f \in K[x]$ un polinomio non costante di grado $n \leq 4$ e sia E il suo crc su K con $G := \text{Gal}(f/K) = \text{Gal}(E/K)$.
In $E[x]$ abbiamo $f = (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$ e gli elementi di G corrispondono a permutazioni di $\{\alpha_1, \ldots, \alpha_n\}$. Identifichiamo G con un sottogruppo di S_n.
Poniamo $\delta = \prod_{1 \leq i < j \leq n} \alpha_i - \alpha_j \in E$ e consideriamo il discriminante

$$\Delta = \delta^2 = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \in \text{Fix}_F(G) = K$$

Si noti che $\sigma(\delta) = \delta$ se e solo se $\sigma \in A_n$ e perciò $\delta \in K$ se e solo se $G \leq A_n$.

Caso $n = 2$

$f = x^2 + px + q = (x - \alpha_1)(x - \alpha_2)$ con

$$\begin{aligned} -p &= \alpha_1 + \alpha_2 & \qquad \delta &= \alpha_1 - \alpha_2 \\ q &= \alpha_1 \alpha_2 & \qquad \Delta &= (\alpha_1 - \alpha_2) = p^2 - 4q \end{aligned}$$

e abbiamo $\{\alpha_1, \alpha_2\} = \{-\frac{p}{2} + \frac{\delta}{2}, -\frac{p}{2} - \frac{\delta}{2}\}$

Se $\delta \in K$, allora $G = \{\text{id}_E\}$

Se $\delta \notin K$, allora $G = S_2$

Caso $n = 3$

1. Possiamo ridurci al caso $f = x^3 + px + q$.
   Infatti se $f(x) = x^3 + px + q$, allora

   $$f' = f(x - \frac{1}{3}a_1) = \ldots = x^3 + (-a_1 + a_1)x^2 + \ldots$$

   quindi z è zero di $f' = x^3 + px + q$ se e solo se $z - \frac{1}{3}a_1$ è zero di f, perciò f e f' hanno lo stesso discriminante e lo stesso gruppo di Galois.

2. $\Delta = -4p^2 - 27q^2$

3. Se f è prodotto di fattori lineari in $K[x]$ allora $E = K$, $G = \{\text{id}_E\}$

4. Se $f = (x - \alpha_1)g$ dove $\alpha_1 \in K$ e g è irriducibile su K di grado 2, allora g (essendo separabile) ha due zeri distinti e E è crc di g, e $|G| = [E : K] = 2$ e $G \cong S_2$

5. f è irriducibile su K. Allora

$$\underbrace{K \subset K(\alpha_1)}_{\text{grado } 3} \subset E$$

quindi $3 \mid |G| = [E : K]$.

Se $\delta \in K$, allora $G \subseteq A_3$ e $G = A_3$

Se $\delta \notin K$, abbiamo anche $K \subset K(\delta) \subset E$ con $[K(\delta) : K] = 2$ poiché $x^2 - \Delta$ è polinomio minimo di δ su K. Quindi anche $2 \mid [E : K] = |G| \leq 6$. Concludiamo che $|G| = 6$ e $G = S_3$.

(Vedi filo rosso per le formule esplicite ed il caso $n = 4$).