Algebra 2

Alberto Canonaco
alberto.canonaco@unipv.it

Università di Pavia
Corso di Laurea in Matematica

Anno Accademico 2019/2020
Lezione del 29-05-2020

Esercizio sui moduli

A dominio. Un A-modulo M è divisibile se $\forall\, x \in M$ e $\forall\, a \in A \setminus \{0\}$ $\exists\, y \in M$ tale che $x = ay$.

1. Il campo dei quozienti K di A è un A-modulo divisibile.
2. M divisibile $\implies$ $\mathrm{T}(M)$ divisibile.
3. M divisibile, $M' \subseteq M$ sottomodulo $\implies$ M/M' divisibile.
4. $M = \bigoplus_{\lambda\in\Lambda} M_\lambda$ divisibile $\iff$ M_λ divisibile $\forall\, \lambda \in \Lambda$.
5. A a ideali principali ma non campo, M divisibile e finitamente generato $\implies$ $M = \{0\}$.
6. A come nel punto precedente $\implies$ ogni A-modulo finitamente generato è isomorfo a un sottomodulo di un modulo divisibile.

Esercizio sui moduli

A dominio. Un A-modulo M è divisibile se $\forall\, x \in M$ e $\forall\, a \in A \setminus \{0\}$ $\exists\, y \in M$ tale che $x = ay$.

1. Il campo dei quozienti K di A è un A-modulo divisibile.
2. M divisibile $\implies$ $\mathrm{T}(M)$ divisibile.
3. M divisibile, $M' \subseteq M$ sottomodulo $\implies$ M/M' divisibile.
4. $M = \bigoplus_{\lambda\in\Lambda} M_\lambda$ divisibile $\iff$ M_λ divisibile $\forall\, \lambda \in \Lambda$.
5. A a ideali principali ma non campo, M divisibile e finitamente generato $\implies$ $M = \{0\}$.
6. A come nel punto precedente $\implies$ ogni A-modulo finitamente generato è isomorfo a un sottomodulo di un modulo divisibile.

1. $x \in K$, $a \in A \setminus \{0\}$ $\implies$ $\exists\, b, c \in A$ con $c \neq 0$ tali che $x = b/c$ $\implies$ $y := b/(ac) \in K$ tale che $x = ay$.
2. $x \in \mathrm{T}(M) \subseteq M$, $a \in A \setminus \{0\}$ $\implies$ $\exists\, y \in M$ tale che $x = ay$.
   $x \in \mathrm{T}(M)$ $\implies$ $\exists\, b \in A \setminus \{0\}$ tale che $bx = 0$ $\implies$ $(ba)y = b(ay) = bx = 0$ $\implies$ $y \in \mathrm{T}(M)$ (perché $ba \neq 0$) $\implies$ $\mathrm{T}(M)$ divisibile.

Dimostrazione di 3, 4, 5 e 6

3. $\bar{x} \in M/M'$ (con $x \in M$), $a \in A \setminus \{0\} \implies \exists\, y \in M$ tale che $x = ay \implies \bar{x} = a\bar{y} \implies M/M'$ divisibile.
4. $\implies$ $M_\lambda \cong M/\bigoplus_{\lambda' \in \Lambda \setminus \{\lambda\}} M_{\lambda'}$ divisibile $\forall\, \lambda \in \Lambda$ per il punto 3.
   $\impliedby$ $x = (x_\lambda)_{\lambda \in \Lambda} \in M$, $a \in A \setminus \{0\} \implies \forall\, \lambda \in \Lambda\ \exists\, y_\lambda \in M_\lambda$ tale che $x_\lambda = a y_\lambda$ e posso supporre $y_\lambda = 0$ se $x_\lambda = 0 \implies$ $y := (y_\lambda)_{\lambda \in \Lambda} \in M$ tale che $x = ay \implies M$ divisibile.
5. $M = \bigoplus_{i=1}^{r} M_i$ con $M_i \cong A$ o A/P^n (con $P \in \mathrm{Max}(A)$ e $n > 0$) e M_i divisibile (per il punto 4) $\forall\, i = 1, \ldots, r$. Per concludere $r = 0$ basta dimostrare A/P^n (e quindi anche A per il punto 3) non divisibile. $P = (p) \implies \nexists\, y = \bar{b} \in A/P^n$ tale che $py = \overline{pb} = \bar{1}$ (perché $pb \in P$, $1 \notin P$ e $P^n \subseteq P$).
6. $M = \bigoplus_{i=1}^{r} M_i$ come prima $\implies$ basta dimostrare $M_i \cong M_i'$ sottomodulo di N_i divisibile $\forall\, i = 1, \ldots, r$ (perché poi $M \cong \bigoplus_{i=1}^{r} M_i'$ sottomodulo di $\bigoplus_{i=1}^{r} N_i$, divisibile per il punto 4). $A \subseteq K$ sottomodulo con K divisibile per il punto 1. $A/P^n \cong \langle \overline{1/p^n} \rangle_A \subseteq K/A$ (perché $\mathrm{Ann}_A(\overline{1/p^n}) \cong P^n$) con K/A divisibile per il punto 3.

Esercizio sui moduli

Un sottomodulo M' di un A-modulo non nullo M è superfluo se l'unico sottomodulo M'' di M tale che $M' + M'' = M$ è $M'' = M$.

1. $M', M'' \subseteq M$ superflui $\implies$ $M' + M''$ superfluo.
2. M noetheriano $\implies$ $\exists\, M_0 \subseteq M$ superfluo tale che $M' \subseteq M_0$ $\forall\, M' \subseteq M$ superfluo.
3. A dominio a ideali principali, M finitamente generato. Allora ogni sottomodulo $M' \subsetneq M$ è superfluo $\iff$ $M \cong A/P^n$ (con $P \in \mathrm{Max}(A)$ e $n > 0$) o $M \cong A$ e $\#\mathrm{Max}(A) = 1$.
4. $A = \mathbb{Z}$ $\implies$ $\{0\}$ è l'unico sottomodulo superfluo di $\mathbb{Z}^n$.
5. $A = \mathbb{Z}$ $\implies$ $\mathbb{Z} \subset \mathbb{Q}$ superfluo.

Esercizio sui moduli

Un sottomodulo M' di un A-modulo non nullo M è superfluo se l'unico sottomodulo M'' di M tale che $M' + M'' = M$ è $M'' = M$.

1. $M', M'' \subseteq M$ superflui $\implies$ $M' + M''$ superfluo.
2. M noetheriano $\implies$ $\exists\, M_0 \subseteq M$ superfluo tale che $M' \subseteq M_0$ $\forall\, M' \subseteq M$ superfluo.
3. A dominio a ideali principali, M finitamente generato. Allora ogni sottomodulo $M' \subsetneq M$ è superfluo $\iff$ $M \cong A/P^n$ (con $P \in \mathrm{Max}(A)$ e $n > 0$) o $M \cong A$ e $\#\mathrm{Max}(A) = 1$.
4. $A = \mathbb{Z}$ $\implies$ $\{0\}$ è l'unico sottomodulo superfluo di $\mathbb{Z}^n$.
5. $A = \mathbb{Z}$ $\implies$ $\mathbb{Z} \subset \mathbb{Q}$ superfluo.

1. $M''' \subseteq M$ tale che $M = (M' + M'') + M''' = M' + (M'' + M''')$ $\implies$ $M'' + M''' = M$ (perché M' superfluo) $\implies$ $M''' = M$ (perché M'' superfluo) $\implies$ $M' + M''$ superfluo.
2. M noetheriano $\implies$ $\exists\, M_0 \subseteq M$ massimale tra i sottomoduli superflui di M (l'insieme di tali sottomoduli è $\neq \emptyset$ perché contiene $\{0\}$). $M' \subseteq M$ superfluo $\implies$ $M_0 + M'$ superfluo per il punto 1 $\implies$ $M' \subseteq M_0 + M' = M_0$.

Dimostrazione di 3

- In generale $\{0\} \subsetneq M' \subsetneq M$ addendo diretto (quindi M non indecomponibile) $\implies$ M' non superfluo.
- A campo $\implies$ $M \cong A^n$ con $n > 0$.
  Ogni sottomodulo $M' \subsetneq M$ superfluo $\iff$ $n = 1$ $(M' = \{0\})$ perché $M \cong A \oplus A^{n-1}$ non indecomponibile se $n > 1$.
  Inoltre $\mathrm{Max}(A) = \{\{0\}\} \implies A/\{0\}^n \cong A \ \forall\, n > 0$.
- A non campo $\implies$ ogni A-modulo finitamente generato indecomponibile è isomorfo a A o A/P^n (con $P \in \mathrm{Max}(A)$ e $n > 0$), per cui basta dimostrare che i sottomoduli propri di A/P^n sono superflui e che quelli di A lo sono $\iff$ $\#\mathrm{Max}(A) = 1$.
  I sottomoduli propri di A/P^n sono P^i/P^n con $0 < i \leq n$ e sono tutti superflui perché $P^i/P^n + P^j/P^n = P^{\min\{i,j\}}/P^n = A/P^n \iff j = 0$.
  Se $\mathrm{Max}(A) = \{P\}$, $I \subsetneq A$ sottomodulo $\implies$ $I \subseteq P \implies I$ superfluo. Se $\exists\, P, Q \in \mathrm{Max}(A)$ distinti, allora $P, Q \subsetneq A$ non superflui perché $P + Q = A$.

Dimostrazione di 4 e 5

4. $\{0\} \neq H < \mathbb{Z}^n \implies \exists\, 0 \neq a = \sum_{i=1}^{n} a_i e_i \in H$, dove $a_i \in \mathbb{Z}$ e $e_i = (0, \ldots, 1, \ldots, 0) \in \mathbb{Z}^n$ ha 1 in posizione i-esima.
   Posso supporre $a_1 \neq 0 \implies \exists\, p$ primo tale che $p \nmid a_1 \implies$ $H' := \langle pe_1, e_2, \ldots, e_n \rangle < \mathbb{Z}^n$ tale che $H' \neq \mathbb{Z}^n$ (perché $e_1 \notin H'$) e $H + H' = \mathbb{Z}^n$ ($\implies$ H non superfluo).
   Infatti $\mathrm{mcd}(a_1, p) = 1 \implies \exists\, l, m \in \mathbb{Z}$ tali che $la_1 + mp = 1$ $\implies$ $la + mpe_1 = e_1 + b$ con $b \in \langle e_2, \ldots, e_n \rangle \subseteq H' \implies$ $e_1 = la + (mpe_1 - b) \in H + H' \implies H + H' = \mathbb{Z}^n$.
5. $H < \mathbb{Q}$ tale che $\mathbb{Z} + H = \mathbb{Q} \implies H \neq \{0\} \implies \mathbb{Z} \cap H \neq \{0\}$ ($a = l/m \in H$ con $l, m \in \mathbb{Z} \setminus \{0\} \implies 0 \neq l = ma \in \mathbb{Z} \cap H$) $\implies \exists\, n > 0$ tale che $\mathbb{Z} \cap H = n\mathbb{Z}$, e basta dimostrare $n = 1$ (perché poi $\mathbb{Z} \subseteq H \implies \mathbb{Q} = \mathbb{Z} + H = H$).
   Per assurdo $n > 1 \implies \exists\, p$ primo tale che $p \mid n \implies$ $1/p \in \mathbb{Q} = \mathbb{Z} + H \implies \exists\, m \in \mathbb{Z}$ e $a \in H$ tali che $1/p = m + a \implies pa = 1 - pm \in \mathbb{Z} \cap H = n\mathbb{Z} \implies$ $p \mid n \mid (1 - pm) \implies p \mid 1$, assurdo.

Esercizio sui gruppi

p primo, G gruppo di ordine $n := 175p$.

1. $p = 7 \implies G$ abeliano.
2. $p < 7 \implies$ può essere $\{1\} \neq Z(G) \neq G$.
3. G non semplice.

Esercizio sui gruppi

p primo, G gruppo di ordine $n := 175p$.

1. $p = 7 \implies G$ abeliano.
2. $p < 7 \implies$ può essere $\{1\} \neq Z(G) \neq G$.
3. G non semplice.

1. $n = 5^2 7^2 \implies s_5 = 1$ (perché $s_5 \mid 7^2$ e $s_5 \equiv 1 \mod 5$) e $s_7 = 1$ (perché $s_7 \mid 5^2$ e $s_7 \equiv 1 \mod 7$) $\implies G = H_5 \times H_7$ (con H_p p-Sylow per $p = 5, 7$) $\implies G$ abeliano perché $H_p \cong C_{p^2}$ o C_p^2.
2. Basta trovare $G = G_1 \times G_2$ con G_1 non abeliano e G_2 abeliano non banale (perché $Z(G) = Z(G_1) \times Z(G_2)$ con $Z(G_1) \neq G_1$ e $Z(G_2) = G_2 \neq \{1\}$).
   - $p = 2$ Per esempio $D_7 \times C_{25}$.
   - $p = 3$ Per esempio $(C_7 \rtimes_\theta C_3) \times C_{25}$ con $\theta \colon C_3 \to \mathrm{Aut}(C_7) \cong \mathbb{Z}/7\mathbb{Z}^* \cong C_6$ omomorfismo non banale.
   - $p = 5$ Per esempio $(C_{25} \rtimes_\theta C_5) \times C_7$ con $\theta \colon C_5 \to \mathrm{Aut}(C_{25}) \cong \mathbb{Z}/25\mathbb{Z}^*$ omomorfismo non banale (che esiste perché $5 \mid \varphi(25) = 20$).

Dimostrazione di 3

$p = 5 \implies s_5 = 1$ (perché $s_5 \mid 7$ e $s_5 \equiv 1 \mod 5$) $\implies H_5 \triangleleft G$.
$p = 7 \implies G$ abeliano per il punto 1.
Per $p \neq 5, 7$ posso supporre $s_p > 1$, perché se no $H_p \triangleleft G$.
$1 < s_p \mid 5^2 7$, $s_p \equiv 1 \mod p \implies p \mid (s_p - 1)$ con
$s_p = 5, 7, 5^2, 5 \cdot 7, 5^2 7 \implies p = 2, 3, 17, 29$.
$p = 2, 17, 29 \implies s_5 = 1$ (perché $s_5 \mid 7p$ e $s_5 \equiv 1 \mod 5$) $\implies$
$H_5 \triangleleft G$.
$p = 3 \implies$ posso supporre $s_5, s_7 > 1$ (se no $H_5 \triangleleft G$ o $H_7 \triangleleft G$)
$\implies s_5 = 21$ (perché $s_5 \mid 3 \cdot 7$ e $s_5 \equiv 1 \mod 5$) e $s_7 = 15$ (perché
$s_7 \mid 3 \cdot 5^2$ e $s_7 \equiv 1 \mod 7$) $\implies \exists\, H_5, H_5'$ 5-Sylow distinti tali che
$H := H_5 \cap H_5' \neq \{1\}$ (altrimenti G conterrebbe $s_5(5^2 - 1) = 504$
elementi di ordine 5 o 25 e $s_7(7 - 1) = 90$ di ordine 7, assurdo
perché $n = 525 < 504 + 90$).
$C_5 \cong H \triangleleft H_5, H_5'$ (perché H_5 e H_5' abeliani) $\implies$
$H_5, H_5' \subseteq G' := N(H) < G \implies s_5' > 1 \implies s_5' = 21$ (perché
$s_5' \mid [G' : H_5] \mid [G : H_5] = 21$ e $s_5' \equiv 1 \mod 5$) $\implies H \triangleleft G' = G$.

Esercizio sui gruppi

In quali dei seguenti casi esistono almeno m classi di isomorfismo di gruppi di ordine n?

1. $n = 45$ e $m = 3$.
2. $n = 63$ e $m = 4$.
3. $n = 102$ e $m = 4$.
4. $n = 195$ e $m = 3$.

Esercizio sui gruppi

In quali dei seguenti casi esistono almeno m classi di isomorfismo di gruppi di ordine n?

1. $n = 45$ e $m = 3$.
2. $n = 63$ e $m = 4$.
3. $n = 102$ e $m = 4$.
4. $n = 195$ e $m = 3$.

1. Non esistono: G gruppo di ordine $45 = 3^2 5 \implies s_3 = 1$ (perché $s_3 \mid 5$ e $s_3 \equiv 1 \mod 3$) e $s_5 = 1$ (perché $s_5 \mid 9$ e $s_5 \equiv 1 \mod 5$) $\implies G = H_3 \times H_5 \cong C_9 \times C_5$ o $C_3^2 \times C_5$.
2. Esistono: $C_9 \times C_7$, $C_3^2 \times C_7$, $C_7 \rtimes_\theta C_9$ e $C_7 \rtimes_{\theta'} C_3^2$ con $\theta \colon C_9 \to \mathrm{Aut}(C_7)$ e $\theta' \colon C_3^2 \to \mathrm{Aut}(C_7)$ omomorfismi non banali (che esistono perché $\mathrm{Aut}(C_7) \cong C_6$ contiene un sottogruppo di ordine 3). I primi due gruppi sono abeliani e tra loro non isomorfi. Gli ultimi due gruppi sono non abeliani e tra loro non isomorfi perché i loro 3-Sylow (rispettivamente C_9 e C_3^2) non sono isomorfi.

Dimostrazione di 3 e 4

3. Esistono: C_{102}, D_{51}, $D_{17} \times C_3$ e $D_3 \times C_{17}$. Infatti il primo è l'unico abeliano, mentre gli altri tre contengono rispettivamente 51, 17 e 3 elementi di ordine 2.
4. Non esistono: G gruppo di ordine $195 = 3 \cdot 5 \cdot 13 \implies s_{13} = 1$ (perché $s_{13} \mid 15$ e $s_{13} \equiv 1 \mod 13$) e $s_5 = 1$ (perché $s_5 \mid 39$ e $s_5 \equiv 1 \mod 5$) $\implies H_{13}, H_5 \triangleleft G \implies H := H_{13}H_5 \triangleleft G$. $\#H = (\#H_{13})(\#H_5) = 65$ e $13 \not\equiv 1 \mod 5 \implies H \cong C_{65}$. $H \cap H_3 = \{1\} \implies \#(HH_3) = (\#H)(\#H_3) = \#G \implies G = HH_3 \implies G = H \rtimes H_3 \cong C_{65} \rtimes_\theta C_3$ con $\theta\colon C_3 \to \mathrm{Aut}(C_{65}) \cong \mathbb{Z}/65\mathbb{Z}^* \cong \mathbb{Z}/13\mathbb{Z}^* \times \mathbb{Z}/5\mathbb{Z}^* \cong C_{12} \times C_4$ omomorfismo. Poiché 3 è primo e $C_{12} \times C_4$ ha un unico sottogruppo di ordine 3, ci sono al più due classi di isomorfismo di gruppi di ordine 195, corrispondenti a θ banale e a θ non banale (e sono effettivamente due perché nel primo caso $G \cong C_{195}$ e nel secondo G non è abeliano).