0.1 Moduli in domini a ideali principali

Lezione del 26/11/2019 (appunti grezzi, non so più cosa stia succedendo qui ad Algebra)

Definizione

Sia R un PID e sia M un R-modulo finitamente generato di torsione. Sia $\mathfrak{p} \lhd R$ ideale primo di R. Definiamo $M_{\mathfrak{p}} = \{m \in M : x \cdot m = 0 \, \forall x \in \mathfrak{p}\} = \{m \in M : \mathfrak{p} \subseteq \mathrm{Ann}_R(M)\}$. Allora, tale $M_{\mathfrak{p}}$ si dice $\mathfrak{p}$-componente primaria di M (o anche $\mathfrak{p}$-componente di Fitting).

Teorema

Sia R un PID e sia M un R-modulo sinistro finitamente generato di torsione con $\mathrm{Ann}_R(M) = \mathfrak{p}_1^{\alpha_1} ... \mathfrak{p}_r^{\alpha_r}$, dove i $\mathfrak{p}_i \lhd R$ sono ideali primi non nulli. Allora, $M \simeq \oplus_{i=1}^{r} M\mathfrak{p}_i^{\alpha_i}$.

Dimostrazione. La facciamo la prossima volta, le ultime parole famose. ■

Da qui comincia la lezione di oggi, ci sono cose sparse da spostare in torsione etc

Proposizione

Sia R un dominio di integrità e sia M un R-modulo sinistro finitamente generato. Allora, M è di torsione se e solo se $\mathrm{Ann}_R(M) \neq 0$.

Dimostrazione. Siano $m_1, \dots, m_n \in M$ tali che $M = \sum_{i=1}^{n} R \cdot m_1$. Allora, $\mathrm{Ann}_R(M) = \bigcap_{i=1}^{n} \mathrm{Ann}_R(m_i)$. Dunque, se M è di torsione, sappiamo che ogni $\mathrm{Ann}_R(m_i) \neq \{0\}$ da cui $\bigcap_{i=1}^{n} \mathrm{Ann}_R(m_i) \neq \{0\}$.[1] Il viceversa a quanto pare lo abbiamo già fatto. ■

Osserviamo che se R è un anello commutativo e M è un R-modulo sinistro con $\mathrm{Ann}_R(M) \neq \{0\}$, essendo $\mathrm{Ann}_R(M) \lhd R$, M è canonicamente un $\overline{R} = R/\mathrm{Ann}_R(\overline{M})$-modulo. Aggiungere qui il diagramma commutativo negli appunti cartacei. Verifichiamo che vale il Lemma della forbice. Presi $r_1, r_2 \in R$, si ha che $\tau(r_1) = \tau(r_2)$ se e solo se $r_1 - r_2 \in \mathrm{Ann}_R(\overline{M})$, cioè $r_1 = r_2 + a$ con $a \in \mathrm{Ann}_R(\overline{M})$. Per ogni $m \in M$, si ha quindi che $r_1 \cdot m = (r_2 + a) \cdot m = r_2 \cdot m + a \cdot m = r_2 \cdot m$ essendo $a \cdot m = 0$. Dunque, abbiamo dimostrato che $(r_1, m) \sim (r_2, m)$ implica $r_1 \cdot m = r_2 \cdot m$, quindi per il Lemma della forbice esista la mappa $\odot \colon \overline{R} \cdot M \to M$ tale che $(r + \mathrm{Ann}_R M) \odot m = r \cdot m$.

Teorema 3.X.Y: Teorema cinese del resto

Sia R un anello e siano $I_1, \dots, I_n \lhd R$ ideali a due a due coprimi (cioè tali che $I_j + I_k = R$ per ogni $j \neq k$). Sia $\pi \colon R \to \bigoplus_{k=1}^{n} R/I_k$ la mappa definita come $\pi(r) = (r + I_1, \dots, r + I_n)$.

[1] Infatti, presi I, J ideali non banali di un dominio di integrità R, se per assurdo fosse $I \cap J = \{0\}$, essendo $IJ = \{ij : i \in I, j \in J\} \lhd R$ un ideale contenuto in $I \cap J = \{0\}$, avremmo che esistono $i \in I \setminus \{0\}$ e $j \in J \setminus \{0\}$ tali che $ij = 0$, assurdo (perché siamo in un dominio di integrità). Il claim segue per induzione.

Allora, ϕ è un omomorfismo di anelli suriettivo con $\ker(\pi) = \bigcap_{k=1}^{n} I_k$.

Dimostrazione. Che π sia un omomorfismo di anelli è evidente dalla definizione (a casa lo scrivo meglio). Inoltre, $\pi(r) = 0$ se e solo se $r \in \bigcap_{k=1}^{n} I_k$. Sia $J_k = \bigcup_{j \neq k} I_j \lhd R$. Allora, J_k e I_k sono coprimi. Infatti, l'ipotesi che $I_k + I_j = R$ per $j \neq k$ implica che in particolare esistono $a_k \in I_k$ e $b_k \in I_j$ tali che $a_k + b_k = 1_R$. Allora,

$$1_R = (a_1 + b_1) \cdot \ldots \cdot (a_k + b_k) = a_1 a_2 \cdot \ldots \cdot a_n + b_1 a_2 \cdot \ldots \cdot a_n + \ldots + b_1 b_2 \cdot \ldots \cdot b_n$$

dove detti $d_k = b_1 b_2 \cdot \ldots \cdot b_n \in I_1 \ldots I_{k-1} I_{k+1} \ldots I_n \subseteq J_k$ e $e_k =$ tutti gli altri termini $\in I_k$, abbiamo che $d_k + e_k = 1_R$, cioè I_k e J_k sono effettivamente coprimi. Sia $\pi_k \colon R \to R/I_k$ la proiezione canonica, cioè $\pi(r) = r + I_k$. Allora, $\pi_k(d_j) = 0_{R/I_k}$ se $j \neq k$ e $\pi_k(d_j) = 1_{R/I_k} = 1_R + I_k$ per $j = k$. Dunque, $1_R + I_k = \pi_k(1_R) = \pi_k(d_k + e_k) = \pi_k(d_k) + \pi_k(e_k) = \pi_k(d_k)$ perché $\pi_k(e_k) = 0$. Sia ora $y = (r_1 + I_1, \ldots, r_n + I_n) \in \bigoplus_{k=1}^{n} R/I_k$ e sia $z = \sum_{i=1}^{n} r_1 \cdot d_i$. Allora, $\pi_k(z) = \sum_{i=1}^{n} \pi_k(r_i) \cdot \pi_k(d_i) = \pi_k(r_k) \cdot \pi_k(d_k) = r_k + I_k$ essendo $\pi_k(r_k) = r_k + I_k$ e $\pi_k(d_k) = 1_R + I_k$, da cui $\pi(z) = y$ e π risulta quindi essere un omomorfismo suriettivo. ■

Ora parliamo di ideali in domini a ideali principali (PID), dove $\mathfrak{p} \lhd R$ è primo se e solo se è massimale.

Definizione

Sia R un PID. Definiamo spettro di R l'insieme $\operatorname{spec}(R) = \{\mathfrak{p} \lhd R : \mathfrak{p} \neq \{0\} \text{ è primo}\}$.

Proposizione

Sia R un PID e sia $I \lhd R$ un ideale non banale. Allora, esistono $n_{\mathfrak{p}}(I)$, $\mathfrak{p} \in \operatorname{spec}(R)$ e $n_{\mathfrak{p}} \in \mathbb{N}$ tali che $\operatorname{supp}(I) = \{\mathfrak{p} \in \operatorname{spec}(R) : n_{\mathfrak{p}}(I) \neq 0\}$ è un insieme finito, e $I = \prod_{\mathfrak{p} \in \operatorname{spec}(R)} \mathfrak{p}^{n_{\mathfrak{p}}(I)}$, dove si intende che $\mathfrak{p}^0 = R$.

Dimostrazione. Sia $I = R \cdot a$. Se $a \in R^\times$, allora $n_{\mathfrak{p}} = 0$ per ogni $\mathfrak{p} \in \operatorname{spec}(R)$. Poiché $I \neq \{0_R\}$, sappiamo che $a \neq 0_R$. Quindi, possiamo assumere che $a \in R^{\#} = R \setminus (R^\times \cup \{0_R\})$. Allora, esiste $u_a \in R^\times$ e $\varepsilon_p(a) \in \mathbb{N}$ tali che $a = u_a \cdot \prod_{p \in \mathfrak{p}} p^{\varepsilon_p(a)}$ dove $\mathfrak{p} \subseteq \operatorname{prim}_0(R)$ è un sistema di rappresentanti rispetto a $\sim$ e $\{p \in \mathfrak{p} : \varepsilon_p(a) \neq 0\}$ è un insieme finito, cioè $|\operatorname{supp}(I)| < \infty$. Dunque $R \cdot a = \prod_{p \in \mathfrak{p}} (R \cdot p)^{\varepsilon_p(a)}$. Dove finisce la dimostrazione? Boh... ■

Sia $(m_{\mathfrak{p}})$ con $\mathfrak{p} \in \operatorname{spec}(R)$ una successione di interi non negativi tali che $\{\mathfrak{p} \in \operatorname{spec}(R) : m_{\mathfrak{p}} \neq 0\}$ sia un insieme finito e $I = \prod_{\mathfrak{p} \in \operatorname{spec}(R)} \mathfrak{p}^{m_{\mathfrak{p}}}$. Allora, $m_{\mathfrak{p}} = n_{\mathfrak{p}}(I)$ per ogni $\mathfrak{p} \in \operatorname{spec}(R)$ come conseguenza della univocitò della decomposizione in primi. Sia $I = \prod_{\mathfrak{p} \in \operatorname{spec}(R)} \mathfrak{p}^{n_{\mathfrak{p}}(I)} = \prod_{\mathfrak{p} \in \operatorname{supp}(I)} \mathfrak{p}^{n_{\mathfrak{p}}(I)} = \bigcap_{\mathfrak{p} \in \operatorname{supp}(I)} \mathfrak{p}^{n_{\mathfrak{p}}(I)}$. (Ma sti cazzo di $n_{\mathfrak{p}}$ sono così o sono degli $\eta_{\mathfrak{p}}$?)

Sia R un PID e sia M un R-modulo sinistro di torsione. Allora,

$$\mathrm{Ann}_R(M) = \prod_{\mathfrak{p}\in\mathrm{supp}(\mathrm{Ann}_R(M))} \mathfrak{p}^{n_\mathfrak{p}(I)} = \bigcap_{\mathfrak{p}\in\mathrm{supp}(\mathrm{Ann}_R(M))} \mathfrak{p}^{n_\mathfrak{p}(I)}$$

da cui per il Teorema cinese e per il primo teorema d'isomorfismo si ha che $\overline{R} = R/\operatorname{Ann}_R(M) \simeq \bigoplus_{\mathfrak{p}\in\mathrm{supp}(\mathrm{Ann}_R(M))} R/\mathfrak{p}^{n_\mathfrak{p}}$. Sia $d_\mathfrak{p} \in \overline{R}$, $d_\mathfrak{p} \in \bigcap_{\mathfrak{q}\neq\mathfrak{p}} \mathfrak{q}^{n_\mathfrak{q}}$ dove $\mathfrak{q} \in \mathrm{supp}(\mathrm{Ann}_R(M))$. Allora, $d_\mathfrak{p} + \mathfrak{p}^{n_\mathfrak{p}} = 1 + \mathfrak{p}^{n_\mathfrak{p}}$. Detto $\Omega = \{\mathfrak{p}^{n_\mathfrak{p}} : \mathfrak{p} \in \mathrm{supp}(\mathrm{Ann}_R(M))\}$, se $\mathfrak{p},\mathfrak{q} \in \mathrm{spec}(R)$ e $\mathfrak{p} \neq \mathfrak{q}$, significa che $\mathfrak{p}^m + \mathfrak{q}^n = R$ per ogni $m, n \in \mathbb{N}$, cioè Ω sono a due a due coprimi. Infine, si ha quindi che $1_{\overline{R}} = \sum_{\mathfrak{p}\in\mathrm{supp}(\mathrm{Ann}_R(M))} d_\mathfrak{p}$.

Lezione del 27/11/2019 (vedi appunti cartacei)

Lezione del 03/12/2019 (appunti grezzi)

Facciamo un recap. Se R è un PID e M è un R-modulo sinistro finitamente generato di torsione, allora $\mathrm{Ann}_R(M) \neq \{0\}$ ed esistono $\mathfrak{p}_1, \dots, \mathfrak{p}_r \in \mathrm{spec}(R)$ e $\alpha_i \in \mathbb{N}$ tali che $\mathrm{Ann}_R(M) = \prod_{i=1}^r \mathfrak{p}_i^{\alpha_i}$. Sappiamo anche che i $\mathfrak{p}_i^{\alpha_i}$, $\mathfrak{p}_j^{\alpha_j}$ sono a due a due coprimi. Abbiamo visto poi che vale il Teorema cinese del resto, cioè $\overline{R} = R/\operatorname{Ann}_R(M) \simeq \bigoplus_{i=1}^r R/\mathfrak{p}_i^{\alpha_i}$ mediante la mappa π. Inoltre, se prendo $d_1, \dots, d_r \in R$ tali che $\pi(d_i + \mathrm{Ann}_R(M)) = (0, \dots, 1, 0, \dots, 0)$ dove 1 è in posizione i-esima, sappiamo che gli $M_i = d_i \cdot M$ sono R-sottomoduli di M e $M = \bigoplus_{i=1}^r M_i$.

Abbiamo applicato la teoria generale al caso particolare in cui $R = \mathbb{K}[x]$ con $\mathbb{K}$ campo e $(M, \cdot) = (M, *_\alpha)$. In questo caso, $\mathrm{Ann}_{\mathbb{K}[x]}(M) = \mathbb{K}[x] \cdot \min_\alpha(x) \cdot \mathbb{K}[x]$ (forse c'è un $\mathbb{K}[x]$ di troppo), e abbiamo dimostrato che α è un endomorfismo diagonalizzabile se e solo se $\min_\alpha(x) = \prod_{i=1}^k (x - \lambda_i)$ con $\lambda_i \neq \lambda_j$ se $i \neq j$, cioè se e solo se il polinomio minimo splitta completamente in fattori lineari distinti su $\mathbb{K}[x]$.

Proposizione

Si ha che $M_i = M_{\mathfrak{p}_i^{\alpha_i}} = \{m \in M : \mathfrak{p}_i^{\alpha_i} \cdot m = 0\}$.

Dimostrazione. Osserviamo che $d_i \in \mathfrak{p}_j^{\alpha_j}$ per $j \neq i$, quindi $d_i \in \bigcap_{j\neq i} \mathfrak{p}_j^{\alpha_j}$. Sia $m \in d_i \cdot M$. Allora, $m = d_i \cdot m$ perché $(d_i + \mathrm{Ann}_R(M))^2 = d_i + \mathrm{Ann}_R(M)$, cioè esiste $y \in M$ tale che $m = d_i \cdot y = d_i^2 \cdot y = d_i(d_i \cdot y) = d_i \cdot m$. Per ogni $z \in \mathfrak{p}^{\alpha_i}$ tale che $z \cdot d_i \cdot m = 0$ osserviamo che $z \cdot d_i$ (qualcosa, forse è appartiene?) $\mathfrak{p}_i^{\alpha_i} \cap \prod_{j\neq i} \mathfrak{p}_j^{\alpha_j} = \prod_{k=1}^r \mathfrak{p}_k^{\alpha_k} = \mathfrak{p}_1^{\alpha_1} \cap \dots \cap \mathfrak{p}_k^{\alpha_k} = \mathrm{Ann}_R(M)$, e questo prova che $M_i \in M_{\mathfrak{p}_i^{\alpha_i}}$. Sia ora $m \in M_i \in M_{\mathfrak{p}_i^{\alpha_i}}$. Poiché $m = \cdot m$ e $1_{\overline{R}} = \sum_{i=1}^r d_i + \mathrm{Ann}_R(M)$, sappiamo che $m = \sum_{k=1}^r d_k \cdot m = d_i \cdot m$. Per $k \neq i$, l'elemento $d_k \in \bigcap_{j\neq k} \mathfrak{p}_j^{\alpha_j} \subseteq \mathfrak{p}_i^{\alpha_i}$. Dunque $d_k \cdot m = 0$ perché $m \in M_{\mathfrak{p}_i^{\alpha_i}}$, da cui $M_{\mathfrak{p}_i^{\alpha_i}} \subseteq d_i \cdot M = M_i$ come desiderato. ■

Come si applica questa cosa? Sia $R = \mathbb{Z}$ e sia A uno $\mathbb{Z}$-modulo finitamente generato di torsione. Allora, avevamo visto che $|A| < \infty$, cioè A è un gruppo abeliano finito.[2] Per quanto appena provato, possiamo scrivere $A = \bigoplus_{i=1}^{r} A_i$, dove $A_i = A_{p_i^{\alpha_i}\mathbb{Z}} = a \in A : p_i^{\alpha_i} \cdot a = 0 \in \mathrm{Syl}_p(A)$. Sia $|A| = p_1^{n_1} \cdot \ldots \cdot p_r^{n_r} \cdot p_{r+1}^{n_{r+1}} \cdot \ldots \cdot p_{r+k}^{n_{r+k}}$. Allora, $A_i \subseteq A$ è un sottogruppo, anzi è un p_i-sottogruppo, e $|A_i| = p_i^{\beta_i}$. Infatti, se per assurdo fosse $|A_i| = p_i^{\beta_i} \cdot q^{\beta} \cdot r$ con $q \neq p_i$ primo e r intero coprimo a p_i e q, dove ovviamente $\beta \geq 1$, per il Teorema di Sylow esiste $Q \subseteq \mathrm{Syl_q}(A_i) \subseteq A_i$ tale che $|Q| = q^{\beta} \neq 1$, cioè esiste $g \in Q \setminus \{1\}$. Dunque, $g \in \mathrm{Syl}_q(A_i) \subseteq A_i$ da cui, essendo $g^{p_i^{\alpha_i}} = 1$ e $\langle g \rangle \subseteq Q$, per Lagrange $g^{|Q|} = g^{q^{\beta}} = 1$. Dunque, essendo $\gcd(p, q) = 1$, deve essere $g = 1$, il che è assurdo perché questo forza $Q = \{1\}$. Dunque, essendo $A = \bigoplus_{i=1}^{r} A_i$, abbiamo che $|A| = \prod p_i^{\beta_i}$, dove β_i è la massima potenza di p_i che divide $|A|$, da cui $A_i \in \mathrm{Syl}_{p_i}(A)$. (In entrambi gli esempi, ho mostrato che un modulo è somma diretta di sottomoduli che si annullano su ideali particolari che contengolo l'annullatore globale, credo abbia detto così).

Esempio. Se $|G| = 35$, allora $G \simeq \mathbb{Z}/35\mathbb{Z}$. Infatti, per quanto appena detto si ha che $G \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} = \mathbb{Z}/35\mathbb{Z}$, cioè G è ciclico. L'ide è che ho un solo 5-sottogruppo di Sylow e un solo 7-sottogruppo di Sylow, da cui essi sono normali, e si conclude facilmente. □

Vogliamo arrivare al teorema seguente. Per farlo dovremo prima introdurre i moduli liberi.

Teorema 3.X.Y: Teorema fondamentale sui moduli f.g. per PID

Sia M un R-modulo sinistro finitamente generato di torsione. Allora, esistono degli ideali $\mathfrak{a}_1, \ldots, \mathfrak{a}_k \lhd R$ tali che $M \simeq \bigoplus_{i=1}^{k} R/\mathfrak{a}_i$.

Esempio. Se $R = \mathbb{Z}$ e A è uno $\mathbb{Z}$-modulo di torsione con $|A| = 27$, allora $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3 \in \{3\mathbb{Z}, 9\mathbb{Z}, 27\mathbb{Z}\}$ e A è isomorfo a uno tra $\mathbb{Z}/27\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ e $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. □

[2] Ricordiamo che per ogni $g \in G$ gruppo, la mappa $\chi_g : \mathbb{Z} \to G$ definita come $\chi_g(k) = g^k$ è un omomorfismo di gruppi. Definiamo esponente di G l'intero positivo $\exp(G)$ tale che $\exp(G)\mathbb{Z} = \bigcap_{g \in G} \ker(\chi_g)$. In realtà c'è una definizione molto più facile ma a lui piace complicarsi la vita.