Lezione 15

Prerequisiti: Lezione 8. Lezioni 10-14.

La congruenza modulo un polinomio. Gli anelli $K[X]/(f(X))$.

Sia K un campo. In questa lezione presentiamo, per l'anello dei polinomi $K[X]$, nozioni analoghe a quelle introdotte, per l'anello degli interi $\mathbb{Z}$, nella Lezione 8.

Sia $f(X) \in K[X]$ un polinomio non nullo.

Definizione 15.1 Siano $a(X), b(X) \in K[X]$. Diremo che $a(X)$ è *congruo* a $b(X)$ *modulo* $f(X)$ se $f(X)$ divide $a(X) - b(X)$. In tal caso scriveremo $a(X) \equiv b(X) \pmod{f(X)}$.

Nota Ciò definisce una relazione binaria su $K[X]$, detta *congruenza modulo* $f(X)$.

La dimostrazione del prossimo enunciato è analoga a quella data per la Proposizione 8.2.

Proposizione 15.2 La congruenza modulo $f(X)$ è una relazione di equivalenza.

Nota Per ogni $a(X) \in K[X]$, la classe di equivalenza di $a(X)$ rispetto alla congruenza modulo $f(X)$ si chiama *classe di congruenza di* $a(X)$ *modulo* $f(X)$ (o *classe di resto di* $a(X)$ *modulo* $f(X)$), e si indica con $[a(X)]_{f(X)}$ (o, semplicemente, $[a(X)]$). L'insieme quoziente di $K[X]$ rispetto alla congruenza modulo $f(X)$ si denota con il simbolo $K[X]/(f(X))$. Il motivo di questa notazione risulterà chiaro nel corso di Algebra 2, una volta che sarà stata introdotta la nozione di ideale.

Diamo ora l'enunciato analogo alla Proposizione 8.4.

Proposizione 15.3 *(Elementi di* $K[X]/(f(X))$**)** Si ha

$$K[X]/(f(X)) = \{[r(X)] \mid r(X) \in K[X], r(X) = 0 \text{ oppure } r(X) \neq 0 \text{ e } \deg(r) < \deg(f)\}.$$

Inoltre, se $r_1(X), r_2(X) \in K[X]$ sono tali che $r_1(X) \neq r_2(X)$ e, per $i = 1, 2$, $r_i(X) = 0$ oppure $r_i(X) \neq 0$ e $\deg(r_i) < \deg(f)$, allora $[r_1(X)] \neq [r_2(X)]$.

Dimostrazione: Per definizione di insieme quoziente, si ha che $K[X]/(f(X)) = \{[a(X)] \mid a(X) \in K[X]\}$. Chiamiamo S l'insieme che nell'enunciato compare a membro destro. Proviamo che $K[X]/(f(X)) = S$. Naturalmente, $K[X]/(f(X)) \supset S$. Proviamo l'altra inclusione. Sia $a(X) \in K[X]$. Sia $r(X)$ il resto della divisione euclidea di $a(X)$ per $f(X)$.

Allora, detto $q(X)$ il quoziente della stessa divisione euclidea, si ha $a(X)=f(X)q(X)+r(X)$, e quindi $f(X)$ divide $a(X)-r(X)$, cioè $a(X)\equiv r(X)\ (\mathrm{mod}\, f(X))$. Dunque $[a(X)]=[r(X)]\in S$. Ciò prova che ${K[X]}/{(f(X))}\subset S$.

Proviamo ora la seconda parte dell'enunciato. Siano $r_1(X), r_2(X)\in K[X]$ tali che $[r_1(X)]=[r_2(X)]$, e tali che per $i=1,2$, $r_i(X)=0$ oppure $r_i(X)\neq 0$ e $\deg(r_i)<\deg(f)$.

Poiché $r_1(X)=f(X)\cdot 0+r_1(X)$, $r_1(X)$ è il resto della divisione euclidea di $r_1(X)$ per $f(X)$. D'altra parte, per ipotesi, $f(X)$ divide $r_1(X)-r_2(X)$, quindi si ha $r_1(X)=f(X)q(X)+r_2(X)$ per qualche $q(X)\in K[X]$. Segue che anche $r_2(X)$ è il resto della divisione di $r_1(X)$ per $f(X)$. Per l'unicità del resto segue così che $r_1(X)=r_2(X)$. □

Nota Gli elementi $r(X)$ dell'enunciato della Proposizione 15.3 si dicono i *rappresentanti canonici* della congruenza modulo $f(X)$. Essi formano un *sistema completo di rappresentanti* per la congruenza modulo $f(X)$. Analogamente a quanto avviene nel caso dei numeri interi, per la congruenza modulo *n*, tali rappresentanti sono tutti i possibili resti della divisione euclidea di un polinomio di $K[X]$ per $f(X)$.

Esempio 15.4 Sia $K=\mathbb{R}$, $f(X)=X^2+3X+1$. Allora

$$\begin{aligned}{\mathbb{R}[X]}/{(f(X))} &= \{[r(X)]\,|\,r(X)\in\mathbb{R}[X], r(X)=0 \text{ oppure } r(X)\neq 0 \text{ e } \deg(r)\leq 1\}\\ &= \{[aX+b]\,|\,a,b\in\mathbb{R}\}.\end{aligned}$$

L'insieme quoziente trovato nell'Esempio 15.4 è infinito. Otteniamo, invece, un insieme quoziente finito quando il campo *K* è finito.

Esercizio 15.5 Determinare ${\mathbb{Z}_3[X]}/{(X^2+\overline{2})}$.

Svolgimento: In base alla Proposizione 15.3,

$$\begin{aligned}{\mathbb{Z}_3[X]}/{(X^2+\overline{2})} &= \{[r(X)]\,|\,r(X)\in\mathbb{Z}_3[X], r(X)=0 \text{ oppure } r(X)\neq 0 \text{ e } \deg(r)\leq 1\}\\ &= \{[aX+b]\,|\,a,b\in\mathbb{Z}_3\}\\ &= \{[\overline{0}],[\overline{1}],[\overline{2}],[X],[X+\overline{1}],[X+\overline{2}],[\overline{2}X],[\overline{2}X+\overline{1}],[\overline{2}X+\overline{2}]\}.\end{aligned}$$

Osservazione 15.6 L'Esercizio precedente si può generalizzare come segue. Sia *p* un numero primo. Ricordiamo che in tal caso, in virtù della Proposizione 8.9, l'anello $\mathbb{Z}_p$ è un campo. Sia $f(X)\in\mathbb{Z}_p[X]$ non costante, di grado *n*. Allora, in base alla Proposizione 15.3,

$$\mathbb{Z}_p[X]/(f(X)) = \{[r(X)] \mid r(X) \in \mathbb{Z}_p[X], r(X) = 0 \text{ oppure } r(X) \neq 0 \text{ e } \deg(r) < n\}$$
$$= \left\{ \left[\sum_{i=0}^{n-1} a_i X^i \right] \middle| a_i \in \mathbb{Z}_p, \text{ per ogni } i = 0,...,n-1 \right\}.$$

I polinomi $\sum_{i=0}^{n-1} a_i X^i \in \mathbb{Z}_p[X]$ sono tanti quanti le possibili n-uple $(a_0,...,a_{n-1}) \in \mathbb{Z}_p{}^n$, cioè sono p^n. Quindi $\left|\mathbb{Z}_p[X]/(f(X))\right| = p^{\deg(f)}$.

La congruenza modulo $f(X)$ è compatibile con la somma ed il prodotto dell'anello $K[X]$, come lo è la congruenza modulo n rispetto alla somma ed il prodotto di interi, in base a quanto avevamo stabilito nella Proposizione 8.6. Diamo ora il corrispondente enunciato per i polinomi.

Proposizione 15.7 *(Compatibilità della congruenza rispetto alla somma e al prodotto)* Siano $a(X), a'(X), b(X), b'(X) \in K[X]$ tali che $a(X) \equiv a'(X) \pmod{f(X)}$ e $b(X) \equiv b'(X) \pmod{f(X)}$. Allora

(i) $a(X) + b(X) \equiv a'(X) + b'(X) \pmod{f(X)}$;

(ii) $a(X)b(X) \equiv a'(X)b'(X) \pmod{f(X)}$.

Queste proprietà consentono di dotare l'insieme $K[X]/(f(X))$ di una struttura di anello. Definiamo su di esso le seguenti operazioni:

- una somma, ponendo, per ogni $a(X), b(X) \in K[X]$, $[a(X)] + [b(X)] = [a(X) + b(X)]$;
- un prodotto, ponendo, per ogni $a(X), b(X) \in K[X]$, $[a(X)] \cdot [b(X)] = [a(X) \cdot b(X)]$.

Dalla Proposizione 15.7 discende che queste definizioni sono ben poste, ossia la classe di congruenza a secondo membro non dipende dalla scelta dei rappresentanti $a(X)$ e $b(X)$ nelle classi di congruenza a primo membro.

Si verifica facilmente che, rispetto a queste operazioni, $K[X]/(f(X))$ è un anello commutativo unitario. L'elemento zero è $[0]$, l'elemento uno è $[1]$.

Il prossimo enunciato è una conseguenza del Lemma di Bézout in $K[X]$: precisamente, lo si deduce dall'Esercizio 11.17 esattamente come la Proposizione 8.7 si deduce dalla Proposizione 6.22.

Proposizione 15.8 *(Elementi invertibili in $K[X]/(f(X))$)* Sia $a(X) \in K[X]$. Allora $[a(X)] \in K[X]/(f(X))$ è invertibile se e solo se $a(X)$ e $f(X)$ sono coprimi.

Esercizio 15.9 Dire se $[X + \overline{2}]$ è invertibile in $\mathbb{Z}_3[X]/(X^2 + \overline{2})$.

Svolgimento: Poiché il polinomio $f(X)=X^2+\overline{2}$ ha in $\mathbb{Z}_3$ le radici $\overline{1}$ e $\overline{2}$, in base alla Proposizione 12.14, $f(X)$ ha in $\mathbb{Z}_3[X]$ la seguente fattorizzazione

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

Quindi $\mathrm{MCD}(f(X),X+\overline{2})=X+\overline{2}$, e dunque $f(X)$ e $X+\overline{2}$ non sono coprimi. Dunque, in virtù della Proposizione 15.8, $[X+\overline{2}]$ non è invertibile in $\mathbb{Z}_3[X]$.

Esercizio 15.10 Dire se $[X]$ è invertibile in $\mathbb{Z}_3[X]/(X^3+\overline{2})$.

Svolgimento: Poiché $\overline{0}$ non è radice di $f(X)=X^3+\overline{2}$, in base al Teorema di Ruffini (Teorema 12.5), il polinomio X non divide $f(X)$, ossia X non è un fattore irriducibile di $f(X)$. Segue che X e $f(X)$ sono coprimi. Quindi, in base alla Proposizione 15.8, $[X]$ è invertibile in $\mathbb{Z}_3[X]/(X^3+\overline{2})$.

Ne determiniamo l'inverso. Questo è l'elemento $[u(X)]$ di $\mathbb{Z}_3[X]/(X^3+\overline{2})$ tale che $[u(X)][X]=[\overline{1}]$, ossia tale che si abbia $u(X)X+v(X)f(X)=\overline{1}$ per un opportuno $v(X)\in\mathbb{Z}_3[X]$. Questa è un'identità di Bézout (vedi Proposizione 11.4), i cui coefficienti possono essere determinati mediante l'algoritmo delle divisioni successive. In questo caso particolare si può però anche procedere più velocemente: una volta osservato che $\overline{2}^2=\overline{1}$, risulta chiaro che si può prendere $u(X)=X^2, v(X)=\overline{2}$. Infatti:

$$X^2X+\overline{2}(X^3+\overline{2})=\overline{3}X^3+\overline{1}=\overline{1}.$$

Quindi $[X]^{-1}=[X^2]$.

Diamo, infine, l'enunciato analogo alla Proposizione 8.9.

Proposizione 15.11 *(I campi $K[X]/(f(X))$).* Sia $f(X)$ non costante. Sono equivalenti le seguenti condizioni.

(i) $f(X)$ è irriducibile;

(ii) $K[X]/(f(X))$ è un campo;

(iii) $K[X]/(f(X))$ è integro.

Esempio 15.12 Il polinomio $f(X)=X^2+X+\overline{1}\in\mathbb{Z}_2[X]$ è irriducibile, in virtù del secondo corollario al Teorema di Ruffini (Corollario 12.9), in quanto privo di radici in $\mathbb{Z}_2$. Quindi l'anello $\mathbb{Z}_2[X]/(X^2+X+\overline{1})$ è un campo, avente, in base all'Osservazione 15.6, esattamente 4 elementi. Questi sono: $[\overline{0}],[\overline{1}],[X],[X+\overline{1}]$. L'elemento $[\overline{1}]$ è inverso di se stesso, gli elementi $[X],[X+\overline{1}]$ sono uno l'inverso dell'altro. In effetti si ha: $[X][X+\overline{1}]=[X^2+X]=[\overline{1}]$, in quanto $X^2+X-\overline{1}=X^2+X+\overline{1}$, e quindi $X^2+X\equiv\overline{1} \pmod{f(X)}$.