1 ANELLI

Definizione 1.1.

Sia A un insieme su cui sono definite due operazioni $+, \cdot$.
$(A, +, \cdot)$ si dice **Anello** se

$(A, +)$ è un gruppo abeliano

$\cdot$ è associativa

valgono le leggi distributive, cioè se $\forall a, b, c \in A$ si ha $(a + b)c = ac + bc$ e $a(b + c) = ab + ac$.

Definizione 1.2.

Un anello A si dice **Commutativo** se l'operazione $\cdot$ è commutativa.
Si dice **con identità** se $\exists$ l'identità dell'operazione $\cdot$, cioè se $\exists 1 \in A$ tale che $a \cdot 1 = 1 \cdot a = 1 \quad \forall a \in A$.

Nel seguito, senza ulteriormente specificarlo, A indicherà un anello commutativo con identità.

Definizione 1.3.

Sia A un anello. $a \in A$ si dice **invertibile** se $\exists b \in A$ tale che $ab = ba = 1$.
Denotiamo con A^* l'insieme degli elementi invertibili di A .
$a \in A$ si dice **divisore di zero** se $\exists b \in A,\ b \neq 0$ tale che $ab = 0$.
Un anello in cui l'unico divisore di zero è lo 0 si dice **dominio di integrità**.

Esempio 1.4.

1. $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ sono anelli commutativi con identità e hanno come unico divisore dello zero lo 0 .
2. $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ è un anello commutativo con identità.
   Sappiamo già che gli elementi invertibili sono $\mathbb{Z}/m\mathbb{Z}^* = \{[a] \mid (a, m) = 1\}$; è immediato verificare che l'insieme dei divisori di zero è $\{[a] \mid (a, m) \neq 1\}$.
3. $M_{n\times n}(\mathbb{R})$ con le usuali operazioni di somma e prodotto tra le matrici è un anello (non commutativo se $n \geq 2$).

Proposizione 1.5.

Sia A un anello. Allora

1. $\forall a \in A$ si ha $a0 = 0$;
2. $(A^*, \cdot)$ è un gruppo abeliano;
3. posto $D = \{\text{divis. di zero di } A\}$, vale $A^* \cap D = \varnothing$;

4. se A è un dominio di integrità vale la legge d'annullamento del prodotto, cioè

$$ab = 0 \Rightarrow a = 0 \vee b = 0$$

.

DIMOSTRAZIONE.

1. $a0 = a(0+0) = a0 + a0$, la legge di cancellazione ci dà $a0 = 0$.
2. $1 \in A^*$; inoltre se $x, y \in A^* \Rightarrow \exists x_1, y_1 \in A^*$ tali che $xx_1 = 1 yy_1 = 1$ da cui $(xy)(y_1x_1) = x(yy_1)x_1 = 1$.

   Chiaramente se $x \in A^*$ e $x_1 \in A$ è il suo inverso ($xx_1 = 1$) allora x è l'inverso di x_1 , quindi $x_1 \in A^*$.

   Inoltre A^* è abeliano poiché A è un anello commutativo.
3. Per assurdo sia $x \in A^* \cap D$.

   $x \in A^* \Rightarrow \exists y \in A$ tale che $xy = 1$,

   $x \in D \Rightarrow \exists z \in A, z \neq 0$ tale che $xz = 0$.

   Quindi $0 = (xz)y = z(xy) = z1 = z,$ contro l'ipotesi $z \neq 0$.
4. Segue dalla definizione di dominio di integrità.

▲

Definizione 1.6.

Un anello commutativo con identità K si dice **campo** se ogni suo elemento diverso da 0 è invertibile, cioè se $K^* = K \setminus \{0\}$.

Osservazione 1.7.

Dalla Proposizione 1.5 segue che se K è un campo, allora $K \setminus \{0\}$ è un gruppo abeliano rispetto al prodotto. Inoltre ogni campo è un dominio di integrità per cui nei campi vale la legge d'annullamento del prodotto.

Definizione 1.8.

Siano A e B anelli commutativi con identità. Un mappa $\varphi : A \to B$ è un omomorfismo di anelli se $\varphi(1_A) = 1_B$ e $\forall x, y \in A$ vale

$$\varphi(x+y) = \varphi(x) + \varphi(y) \text{ e } \varphi(xy) = \varphi(x)\varphi(y).$$

POLINOMI

Sia A un anello (commutativo con identità) e x una indeterminata.

L'anello dei polinomi con coefficienti in A nella indeterminata x è l'insieme

$$A[x] := \{a_0 + a_1x + \cdots + a_nx^n \mid a_i \in A,\ n \in \mathbb{N}\}.$$

Definizione 1.9.

Siano $f(x) = \sum_{i=0}^{n} a_ix^i$, $g(x) = \sum_{j=0}^{m} b_jx^j \in A[x]$.
Poniamo

$$f(x) + g(x) := \sum_{i=0}^{n}(a_i + b_i)x^i$$

(dove abbiamo supposto $n \geq m$ e abbiamo posto $b_{m+1} = \cdots = b_n = 0$), e

$$f(x) \cdot g(x) := \sum_{h=0}^{n+m}(\sum_{i+j=h} a_ib_j)x^h.$$

Teorema 1.10.

$(A[x], +, \cdot)$ è un anello commutativo con identità.

Dimostrazione.

Si verificano le varie proprietà sfruttando le analoghe per A . ▲

Definizione 1.11.

Sia $f(x) = \sum_{i=0}^{n} a_ix^i \in A[x] \setminus \{0\}$. Definiamo il **grado** di f nel seguente modo:

$$\deg f := \max\{i \in \mathbb{N} \mid a_i \neq 0\}$$

Scegliamo di non definire il grado del polinomio 0 .

Proposizione 1.12.

Sia A un **dominio d'integrità** e siano $f, g \in A[x] \setminus \{0\}$. Allora

1. $\deg(fg) = \deg f + \deg g$;
2. $\deg(f + g) \leq \max\{\deg f, \deg g\}$./

Dimostrazione.

Siano $f = \sum_{i=0}^{n} a_ix^i$ e $g = \sum_{j=0}^{m} b_jx^j$ con $a_n \neq 0$ e $b_m \neq 0$.
Poiché A è un dominio, si ha $a_nb_m \neq 0$, quindi $f(x)g(x) = a_nb_mx^{n+m} +$ termini di grado più basso , cioè $\deg(fg) = n + m = \deg f(x) + \deg g(x)$.

Dalla definizione di $f + g$ segue l'enunciato 2 (il $<$ si ha nel caso in cui il monomio di grado massimo di g sia l'opposto del monomio di grado massimo di f). ▲

Corollario 1.13.

$K[x]^* = K^*$

DIMOSTRAZIONE.

Chiaramente $K^* \subset K[x]^*$.

Viceversa se $f(x) \in K[x]^*$ allora $\exists g(x) \in K[x]$ tale che $f(x)g(x) = 1$, da cui, passando ai gradi

$$0 = \deg(fg) = \deg f + \deg g.$$

Quindi $\deg f = \deg g = 0$, cioè $f \in K^*$. ▲

L'anello $K[x]$ è per molti aspetti somigliante all'anello $\mathbb{Z}$. In questa somiglianza il grado gioca il ruolo che il valore assoluto ha in $\mathbb{Z}$.

Teorema 1.14. (Teorema di divisione euclidea).

Siano $f, g \in K[x]$, con $f \neq 0$. Allora esistono e sono unici $q, r \in K[x]$ tali che $g = qf + r$ con $r = 0$ oppure $\deg r < \deg f$.

DIMOSTRAZIONE.

Esistenza: Se $g = 0$ allora $q = r = 0$. Supponiamo quindi $g \neq 0$ e dimostriamo l'asserto per induzione sul grado di g .

Se $\deg g = 0$ e $\deg f = 0$ allora $g = f\left(\frac{g}{f}\right) + 0$.

Se $\deg g < \deg f$ allora $g = 0f + g$, quindi $r = g$ e $q = 0$.

Sia quindi $m = \deg g \geq \deg f = n$ e $f = \sum_{i=0}^{n} a_i x^i$ e $g = \sum_{j=0}^{m} b_j x^j$.

Pongo

$$g_1(x) = \quad g(x) - \begin{array}{c} \frac{b_m}{a_n} x^{m-n} f(x) \\ \| \\ b_m x^m + \dots \end{array}$$

Allora $\deg g_1 < m$. Quindi per induzione

$$g_1(x) = q(x)f(x) + r(x) \text{ con } r = 0 \text{ opp. } \deg r < \deg f$$

$$\Rightarrow g(x) = g_1(x) + \frac{b_m}{a_n} x^{m-n} f(x) = \left(q + \frac{b_m}{a_n} x^{m-n}\right) f(x) + r(x).$$

Unicità: Sia $g = qf + r = q_1 f + r_1$; allora $(q_1 - q)f = r - r_1$ se i due membri non fossero 0, guardando i gradi si avrebbe un assurdo. ▲

Definizione 1.15.

Siano $f, g \in K[x]$, si dice che f divide g (in simboli $f \mid g$) se $g(x) = f(x)q(x)$.

Teorema 1.16. (Teorema di Ruffini).

Siano $f \in K[x]$ e $a \in K$. Allora

$$f(a) = 0 \Longleftrightarrow x - a \mid f(x)$$

DIMOSTRAZIONE.

Sia $f(x) = (x-a)q(x) + r$, allora, poichè $\deg(r) < \deg(x-a) = 1$, r è una costante. Valutando in a l'espressione di $f(x)$ otteniamo $f(a) = r$, quindi $r = 0 \Leftrightarrow f(a) = 0$. ▲

Corollario 1.17.

Sia $f \in K[x] \setminus \{0\}$, allora f ha al più $\deg f$ radici distinte in K.

DIMOSTRAZIONE.

Per induzione su $n = \deg f$.

Se $n = 0$, il polinomio f è costante e non nullo e quindi non ha radici.

Supponiamo vera la tesi per polinomi di grado $n-1$.

Se f non ha radici vale la tesi. Sia $\alpha \in K$ una radice di $f(x)$, allora $f(x) = (x-\alpha)f_1(x)$ con $\deg f_1(x) = n-1$ e per l'ipotesi induttiva ha al più $n-1$ radici in K. Poiché $\forall \beta \neq \alpha$ tale che $f(\beta) = (\beta - \alpha)f_1(\beta) = 0$ si ha $f_1(\beta) = 0$, si ha la tesi. ▲

Definizione 1.18.

Siano $f, g \in K[x]$ non entrambi nulli. Un polinomio $d(x) \in K[x]$ è un **massimo comune divisore** tra f e g se

1. $d(x) \mid f(x)$ e $d(x) \mid g(x)$,
2. $\forall p(x)$ tale che $p(x) \mid f(x)$ e $p(x) \mid g(x)$, si ha $p(x) \mid d(x)$.

Teorema 1.19. (Esistenza e unicità del MCD **)**

Siano $f, g \in K[x]$ non entrambi nulli, allora esiste un loro massimo comune divisore $d(x)$ e si può trovare con l'algoritmo euclideo.

Inoltre $\exists a(x), b(x) \in K[x]$ tali che

$$d(x) = a(x)f(x) + b(x)g(x).$$

Infine $d_1(x)$ è un massimo comune divisore tra $a(x)$ e $b(x)$ se e solo se $d_1(x) = c \cdot d(x)$ con $c \in K^*$.

DIMOSTRAZIONE.

La dimostrazione segue la stessa linea di quella per gli interi. ▲

Fattorizzazione di polinomi

Definizione 1.20.

Sia $f \in K[x]$ un polinomio non costante. f si dice **irriducibile** se

$$f = gh \Rightarrow g \in K[x]^* = K^* \vee h \in K^*.$$

Definizione 1.21.

$f(x) \in K[x]$ non costante si dice **primo** se $f(x) \mid g(x)h(x)$ implica $f \mid g$ oppure $f \mid h$.

Proposizione 1.22.

Sia $f \in K[x]$. Allora f è irriducibile $\Leftrightarrow$ f è primo.

Dimostrazione.

La dimostrazione è identica a quella fatta per gli interi. ▲

Teorema 1.23.

Ogni polinomio $f \in K[x]$ non costante si fattorizza in modo "unico" come prodotto di polinomi irriducibili.

Dimostrazione.

Anche in questo caso la dimostrazione è analoga a quella fatta per gli interi, e quindi la omettiamo. ▲

Osservazione 1.24.

Nel teorema precedente "unico" vuol dire a meno dell'ordine e di moltiplicazione dei fattori per costanti $\neq 0$. In particolare in $\mathbb{Q}[x]$ si ha ad esempio che

$$(x-1)(x+1) \text{ e } (\frac{1}{2}x - \frac{1}{2})(2x-2)$$

sono considerate fattorizzazioni equivalenti del polinomio $x^2 - 1$.

Corollario 1.25.

$f \in K[x]$, $f \neq 0$ ha al più $\deg f$ radici in K contate con molteplicità.

Teorema fondamentale dell'algebra e sue conseguenze.

Teorema 1.26. (Teorema fondamentale dell'algebra).

Ogni polinomio $p(x) \in \mathbb{C}[x]$ con $\deg p \geq 1$ ha almeno una radice in $\mathbb{C}$.

(Non dimostriamo questo teorema).

Conseguenze:

1. $p(x) \in \mathbb{C}[x]$ è irriducibile $\Leftrightarrow \deg p(x) = 1$.

   ($\Leftarrow$ ovvio;

   $\Rightarrow$ Se $\deg p(x) = n > 1$ allora $\exists \alpha \in \mathbb{C}$ tale che $p(\alpha) = 0$, quindi dal teorema di Ruffini si ha $p(x) = (x - \alpha)p_1(x)$ con $\deg p_1 = n - 1 > 0$, quindi $p_1(x)$ non invertibile. Ne segue che quello esibito è uno spezzamento di $p(x)$ che ne mostra la riducibilità.

2. Ogni polinomio di $\mathbb{C}[x]$ si fattorizza come prodotto di polinomi di primo grado.

3. $\forall p(x) \in \mathbb{C}[x]$ $\deg p(x) = n \Rightarrow p$ ha esattamente n radici in $\mathbb{C}$ (contate con molteplicità).

4. $f(x) \in \mathbb{R}[x]$ è irriducibile $\Leftrightarrow$ $\deg f = 1$ oppure $\deg f = 2$ e $\Delta_f < 2$.

   (Sia $\deg f(x) = n$; poiché $\mathbb{R} \subset \mathbb{C}$, guardiamo al polinomio $f(x)$ come polinomio di $\mathbb{C}[x]$. Per il punto 3 si ha: $f(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$. D'altra parte, poiché $f(x) \in \mathbb{R}[x]$ si ha $f = \overline{f}$, dove $\overline{\ }$ indica il complesso coniugato. Quindi,

   $$f(x) = \overline{f(x)} = c(x - \overline{\alpha_1}) \cdots (x - \overline{\alpha_n}),$$

   da cui, per il Teorema di fattorizzazione unica, si ha $\{\alpha_i\} = \{\overline{\alpha_i}\}$.

   Ne segue che per ogni i , esiste un indice j tale che $\overline{\alpha_i} = \alpha_j$. Vale $\overline{\alpha_i} = \alpha_i \iff \alpha_i \in \mathbb{R}$; quindi se $\alpha_i \notin \mathbb{R}$ oppure $\exists j \neq i$ tale che $\overline{\alpha_i} = \alpha_j$ e in tal caso

   $$(x - \alpha_i)(x - \overline{\alpha_i}) = x^2 - 2\,\mathrm{Re}(\alpha_i)x + |\alpha_i|^2$$

   è un polinomio con coefficienti reali e $\Delta < 0$.

   Questo mostra che che i fattori irriducibili di un qualsiasi polinomio $f \in \mathbb{R}[x]$ si possono ottenere a partire dalla fattorizzazione in $\mathbb{C}[x]$, moltiplicando eventuali fattori corrispondenti a radici non reali con il fattore che ha come radice la complessa coniugata, che deve necessariamente comparire nella fattorizzazione in $\mathbb{C}[x]$ di f poiché f ha coefficienti reali. Otteniamo cosi' che la fattorizzazione di f è fatta con polinomi di primo grado o con polinomi di secondo grado e $\Delta < 0$.

Polinomi con coefficienti in $\mathbb{Q}$.

Sia $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Q}[x]$, a meno di moltiplicare per il mcm dei denominatori degli a_i posso supporre che $f(x) \in \mathbb{Z}[x]$.
Per $f \in \mathbb{Z}[x]$ definiamo il **contenuto** di $c(f)$ del polinomio f come

$$c(f) := \text{MCD}\{a_0, \ldots, a_n\}.$$

Un polinomio $f \in \mathbb{Z}[x]$ si dice **primitivo** se $c(f) = 1$; chiaramente, per ogni $f \in \mathbb{Z}[x]$ il polinomio $c(f)^{-1} f(x)$ ha coefficienti in $\mathbb{Z}$ ed è primitivo.

In sintesi: $\forall f \in \mathbb{Q}[x]\ \exists c \in \mathbb{Q}^*$ tale che $cf(x) \in \mathbb{Z}[x]$ ed è primitivo.
Poiché le costanti non nulle sono invertibili in $\mathbb{Q}$, fattorizzare $f(x) \in \mathbb{Q}[x]$ è equivalente a fattorizzare il polinomio $f_1(x) = cf(x) \in \mathbb{Z}[x]$.

Lemma 1.27. (Lemma di Gauß).

Siano $f, g \in \mathbb{Z}[x]$ polinomi primitivi. Allora il polinomio fg è primitivo. .

Corollario 1.28. Siano $f, g \in \mathbb{Z}[x]$. Allora $c(fg) = c(f)c(g)$.

Corollario 1.29. Siano $f, g \in \mathbb{Z}[x]$; supponiamo $c(f) = 1$ e che $f|g$ in $\mathbb{Q}[x]$. Allora $f|g$ in $\mathbb{Z}[x]$. .

Corollario 1.30. Sia $f \in \mathbb{Z}[x]$ e sia $f(x) = a(x)b(x)$ in $\mathbb{Q}[x]$.
Allora $\exists c \in Q^*$ tale che $a_1(x) = ca(x) \in \mathbb{Z}[x]$, $b_1(x) = c^{-1}b(x) \in \mathbb{Z}[x]$ e quindi

$$f(x) = a_1(x)b_1(x) \text{ in } \mathbb{Z}[x]$$

.

Corollario 1.31. Sia $f \in \mathbb{Z}[x]$ un polinomio primotivo. Allora:
f è irriducibile in $\mathbb{Z}[x] \Leftrightarrow$ è irriducibile in $\mathbb{Q}[x]$.

Metodi per la fattorizzazione in $\mathbb{Q}[x]$

Sia $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$.

1. Ricerca delle radici di f : sia $\frac{b}{d} \in \mathbb{Q}$ con $(b, d) = 1$ tale che $f(\frac{b}{d}) = 0 \Rightarrow b \mid a_0$ e $d \mid a_n$.

Infatti se

$$f\left(\frac{b}{d}\right) = a_n\frac{b^n}{d^n} + \cdots + a_1\frac{b}{d} + a_0,$$

moltiplicando per d^n si ottiene

$$a_n b^n + a_{n-1}b^{n-1}d + \cdots + a_1 b d^{n-1} + a_0 d^n = 0$$

da cui

$$b(a_n b^{n-1} + \cdots + a_1 d^{n-1}) = -a_0 d^n$$

e

$$-a_n b^n = d(a_{n-1}b^{n-1} + \cdots + a_0 d^{n-1}),$$

quindi poiché $(b,d) = 1$ necessariamente $b \mid a_0$ e $d \mid a_n$.

2. Riduzione modulo p .

   Sia p un primo e sia $\pi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}/p\mathbb{Z}[x]$ definita da $\pi(\sum_{i=0}^n a_i x^i) = \sum_{i=0}^n \overline{a_i} x^i$.

   π è un omomorfismo di anelli, quindi in particolare $\pi(a(x)b(x)) = \pi(a(x))\pi(b(x))$.
   Inoltre $\deg \pi(a(x)) \leq \deg a(x)$ e il $<$ vale se e solo se p divide il coefficiente di grado massimo di $a(x)$.

Proposizione 1.32.

Sia p un primo tale che non divide il coefficiente del monomio di grado massimo di $f(x)$. Se $\pi(f(x))$ è irriducibile in $\mathbb{Z}/p\mathbb{Z}[x]$ allora f è irriducibile in $\mathbb{Z}[x]$.

Dimostrazione.

Sia $f(x) = a(x)b(x)$ in $\mathbb{Z}[x]$ con $\deg a(x) \geq 1$ e $\deg b(x) \geq 1$. Allora $\pi(f(x)) = \pi(a(x))\pi(b(x))$.
Passando ai gradi si ha

$$\deg a(x) + \deg b(x) = \deg f(x)$$

$$\deg \pi(a(x)) + \deg \pi(b(x)) = \deg \pi(f(x))$$

Per l'ipotesi su p si ha $\deg f(x) = \deg \pi(f(x))$.

Quindi dalle relazioni $\deg \pi(a(x)) \leq \deg a(x)$ e $\deg \pi(b(x)) \leq \deg b(x)$ e dalle relazioni sopra si ottienre $\deg \pi(a(x)) = \deg a(x) \geq 1$ e $\deg \pi(b(x)) = \deg b(x) \geq 1$, quindi anche $\pi(f(x))$ è riducibile. ▲

Esempio 1.33.

Il polinomio $x^3 + 10x^2 + 7x + 1$ è irriducibile in $\mathbb{Z}[x]$ perché lo è modulo 2 .

3. **Criterio di Eisenstein**

   Sia $f(x) = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x]$ e sia p un primo. Supponiamo che

   (1) $p \nmid a_n$;
   (2) $p \mid a_i \forall i = 0, \ldots, n-1$;
   (3) $p^2 \nmid a_0$.

Allora f è irriducibile in $\mathbb{Z}[x]$ (e quindi in $\mathbb{Q}[x]$).

DIMOSTRAZIONE.

Per assurdo supponiamo che f sia riducibile in $\mathbb{Z}[x]$, cioè $f = g(x)h(x)$, e sia

$$\pi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}/p\mathbb{Z}[x]$$

la riduzione modulo p .

Per il criterio precedente (che si puo' applicare in quanto $p \not| a_n$) otteniamo che $\pi(f) = \pi(g)\pi(h)$ è riducibile in $\mathbb{Z}/p\mathbb{Z}[x]$.

Poniamo $g(x) = b_m x^m + \cdots + b_0$ e $h(x) = c_{n-m}x^{n-m} + \cdots + c_0$; poiché $\pi(f) = \overline{a_n}x^n$, necessariamente $b_{m-1} \equiv \cdots \equiv b_0 \equiv 0 \ (p)$ e $c_{n-m-1} \equiv \cdots \equiv c_0 \equiv 0 \ (p)$. Da questo segue che $a_0 = b_0 c_0 \equiv 0 \ (p^2)$ e questo è assurdo. ▲

Corollario 1.34.

$\forall n$ esistono infiniti polinomi irriducibili di grado n in $\mathbb{Q}[x]$.

DIMOSTRAZIONE.

L'insieme $\mathcal{P}$ dei numeri primi è infinito e $\forall p \in \mathcal{P}$ il polinomio $x^n - p$ è irriducibile per il criterio di Eisenstein. ▲

Quozienti di $K[x]$

Sia K un campo e sia $f(x) \in K[x]$.

Definiamo $(f(x)) := f(x)K[x]$, cioè l'insieme dei polinomi di $K[x]$ che sono multipli di $f(x)$.

Si verifica facilmente che $(f(x))$ è un sottogruppo di $K[x]$ e che $\forall a(x) \in K[x]$ si ha $a(x)(f(x)) \subset (f(x))$.

(un sottogruppo di un anello che sia chiuso rispetto alla moltiplicazione per elementi dell'anello si dice **ideale**).

N.B. $(f(x)) = \{f(x)a(x) |\ a(x) \in K[x]\}$ **NON** è il sottogruppo generato da $f(x)$, infatti

$$< f(x) >= \{nf(x) \mid n \in \mathbb{Z}\}.$$

Poiché $(K[x], +)$ è abeliano, $(f(x)) \lhd K[x]$, quindi possiamo considerare il gruppo quoziente $K[x]/(f(x))$, sappiamo che questo è un gruppo con la somma tra le classi definita da

$$(a(x) + (f[x])) + (b(x) + (f[x])) = a(x) + b(x) + (f[x]).$$

Definiamo anche un prodotto tra classi ponendo

$$(a(x) + (f[x]))(b(x) + (f[x])) := a(x)b(x) + (f[x]).$$

Con verifiche analoghe a quelle fatte per la somma si dimostra che questa definizione è ben posta e che $K[x]/(f(x))$ con queste operazioni è un anello commutativo con identità.

Teorema 1.35.

$K[x]/(f(x))$ con le operazioni definite è un anello commutativo con identità. Un insieme di rappresentanti è dato dai polinomi $r(x) \in K[x]$ con $r(x) = 0$ oppure $\deg r(x) < \deg f(x)$.

In particolare $K[x]/(f(x))$ è un $K-$ spazio vettoriale tale che

$$\dim_K K[x]/(f(x)) = \deg f(x).$$

DIMOSTRAZIONE.

La verifica che il prodotto tra le classi è associativo e che vale la proprietà distributiva discende dalle analoghe proprietà per $K[x]$ ed è lasciato per esercizio.

Sia $a(x) + (f(x))$ una classe di $K[x]/(f(x))$ e sia

$a(x) = q(x)f(x) + r(x)$ con $r(x) = 0$ oppure $\deg r(x) < \deg f(x)$. Allora

$a(x) + (f(x)) = r(x) + (f(x))$, cioè una qualsiasi classe è rappresentata dal suo resto nella divisione euclidea per $f(x)$.

D'altra parte se $r_1(x), r_2(x) \in K[x]$ sono nulli o di grado minore di $f(x)$ si ha che

$$r_1(x) + (f(x)) = r_2(x) + (f(x)) \iff r_1(x) - r_2(x) \in (f(x))$$

e per questioni di grado questo è possibile se e sole se $r_1(x) = r_2(x)$.

Sia $n = \deg f(x)$ e poniamo $\overline{x} = x + (f(x))$.

Allora $\{1, \overline{x}, \overline{x^2}, \ldots, \overline{x^{n-1}}\}$ sono una $K-$ base di $K[x]/(f(x))$:

generano perché come loro combinazione otteniamo le classi di tutti i polinomi di grado $< n$ e quindi rappresentanti di tutte le classi;

sono linearmente indipendenti perché

$$a_0 + a_1\overline{x} + \cdots + a_{n-1}\overline{x^{n-1}} = \overline{0}$$

$$\iff a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in (f(x))$$

e questo è possibile $\Leftrightarrow a_i = 0 \; \forall i = 0, \ldots, n-1$. ▲

Proposizione 1.36.

Sia $\overline{a(x)} = a(x) + (f(x)) \in K[x]/(f(x))$. Si ha che

1. $\overline{a(x)}$ è invertibile $\iff (a(x), f(x)) = 1$
2. $\overline{a(x)}$ è un divisore di zero $\iff (a(x), f(x)) \neq 1$.

DIMOSTRAZIONE.

1. $(a(x), f(x)) = 1 \iff \exists h(x), k(x) \in K[x]$ tali che $a(x)h(x) + k(x)f(x) = 1 \iff \overline{a(x)h(x)} = \overline{a(x)h(x)} = \overline{1} \iff \overline{a(x)}$ è invertibile.
2. Analogamente $\overline{a(x)}$ è un divisore di zero $\iff \exists \overline{b(x)} \neq \overline{0}$ tale che $\overline{a(x)b(x)} = \overline{0} \iff a(x)b(x) + (f(x)) = (f(x)) \iff f(x) \mid a(x)b(x)$.

   Ora se $(a(x), f(x)) = d(x) \neq 1$ questo è sempre vero, basta prendere $b(x) = \frac{f(x)}{d(x)}$.

   Se invece $(a(x), f(x)) = 1$, allora $\overline{a(x)}$ è invertibile e quindi non può essere un divisore di zero.

▲

Corollario 1.37.

L'anello $K[x]/(f(x))$ è un campo se e solo se il polinomio $f(x)$ è irriducibile.

Dimostrazione.

$K[x]/(f(x))$ è un campo se e solo se tutti i suoi elementi non nulli sono invertibili e, per la Proposizione 1.36, questo si ha se e solo se tutti i polinomi non nulli di grado minore di $\deg f(x)$ sono coprimi con $f(x)$. Questo significa esattamente che $f(x)$ è irriducibile. ▲

Osservazione 1.38.

Si noti la completa analogia tra l'anello $K[x]/(f(x))$ e l'anello $\mathbb{Z}/n\mathbb{Z}$.