Anelli

Def. Un anello con unità R è un insieme munito di due op. $+$ e $\cdot$ t.c.:

- $(R,+)$ è un gruppo abeliano;
- $\forall a,b,c \in R, \ (ab)c = a(bc)$
- $[\exists 1 \in R \mid \forall a \in R, \ a \cdot 1 = a = 1 \cdot a]$ (UNITÀ)
- $\forall a,b,c \in R$:
  - $(a+b)\cdot c = ac + bc$
  - $a(b+c) = ab + ac$

Un anello in cui la moltiplicazione è commutativa si dice anello commutativo.

Def. Sia R un anello commutativo, si dice che $a \in R$ è un DIVISORE di 0 se $\exists\, b \in R,\ b \neq 0 \mid ab = 0$.

Un anello commutativo R in cui $0 \neq 1$ e in cui l'unico divisore di 0 è 0, si chiama DOMINIO o DOMINIO DI INTEGRITÀ.

Si usa dire con $0 \neq 1$ per escludere l'anello banale $\{0\}$.

Def. Un elemento u di un anello R si dice INVERTIBILE se $\exists\, v \in R \mid uv = vu = 1$. Si denota con R^* l'insieme degli invertibili di R.

Oss. $(R^*, \cdot)$ è un gruppo.

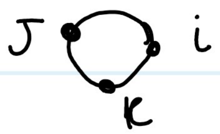
Def. Due elementi a, b di un anello commutativo R si dicono ASSOCIATI se $\exists\, \gamma \in R^* \mid a = b\gamma$.

Def. Un anello R in cui $0 \neq 1$ e in cui ogni elemento $\neq 0$ ammette un inverso si chiama CORPO (o DIVISION RING)

Def. Un corpo commutativo si dice CAMPO.

es. $\mathbb{H}$ è un corpo. $i^2 = j^2 = k^2 = -1$

$ij = k,\ jk = i,\ ki = j$



Esso ammette tutti gli elementi invertibili.

$$(a+bi+cj+dk)\,\frac{a-bi-cj-dk}{\sqrt{a^2+b^2+c^2+d^2}} = 1.$$

Estraendo $Q_8=\{\pm 1, \pm i, \pm j, \pm k\}$, esso è un gruppo con la moltiplicazione. Tutti i suoi sottogruppi sono normali, nonostante Q_8 non sia abeliano.

Lemma Sia A un anello, allora $\forall a,b\in A$:

(i) $a\cdot 0 = 0\cdot a = 0$

(ii) $-a$ è unico $\wedge$ $-(-a)=a$

(iii) $a(-b) = (-a)b = -(ab)$, in particolare

$(-1)a = a(-1) = -a$

(iv) $(-a)(-b) = ab$, in particolare $(-1)(-1)=1$

(i) $a\cdot(0+0) = a\cdot 0 + a\cdot 0 = a\cdot 0 \Rightarrow a\cdot 0 = 0$

$(0+0)\cdot a = 0\cdot a + 0\cdot a = 0\cdot a \Rightarrow 0\cdot a = 0$ ☒

(ii) vista con i gruppi

(iii) $a\cdot b + a\cdot(-b) = a\cdot(b-b) = a\cdot 0 = 0 \Rightarrow$

$\Rightarrow$ l'opposto è unico, quindi: $a\cdot(-b) = -ab$ ☒

(iv) $(-a)(-b) = -a(-b) = -(-ab) = ab.$ ☒

Approfondiamo il concetto di dominio:

- $\mathbb{Z}/10\mathbb{Z}$ NON è un dominio
- $\mathbb{R}[x]$ è un dominio
- ogni campo è un dominio

Prop. Se D è un dominio, vale la legge di cancellazione, ossia se $a \in D$ e $a \neq 0$, allora
$ab = ac \Rightarrow b = c$.

$$ab - ac = 0 \iff a(b-c) = 0 \overset{\substack{D \text{ dominio} \\ a \neq 0 \Rightarrow b-c=0}}{\iff} b - c = 0 \iff$$
$$\iff b = c. \qquad \boxtimes$$

es. $\mathbb{Z}$ è un dominio, $\mathbb{Z}[x]$ idem.

Def. Un sottoanello T di un anello R è un sottoinsieme t.c.:

- $(T, +) < (R, +)$
- $\forall\, a, b \in T,\ a \cdot b \in T$
- $1_R \in T$

Def. Dati R ed S anelli una funzione $\phi : R \to S$ si dice OMOMORFISMO se:

- $\phi(a+b) = \phi(a) + \phi(b)$
- $\phi(ab) = \phi(a)\,\phi(b)$
- $\phi(1_R) = 1_S$

Oss. è ammesso $\{0\}$ come codominio poiché 0 è anche l'1.

Def. Data $\phi : R \to S$ omomorfismo chiamiamo $\operatorname{Ker}\phi$, nucleo di ϕ, l'insieme $\{r \in R \mid \phi(r) = 0_S\}$.

Oss. $\operatorname{Ker}\phi$ non è un sottoanello ($1 \notin \operatorname{Ker}\phi$), a meno che $S = \{0\}$.

Oss. noto che, data $f : R \to S$ omomorfismo, $\operatorname{Ker} f$ ha la seguente proprietà:

- $n \in \operatorname{Ker} f,\ r \in R \Rightarrow nr, rn \in \operatorname{Ker} f$

  $(f(nr) = f(n)f(r) = 0\,f(r) = 0)$

Def. Un IDEALE I di un anello R è un suo sottogruppo additivo t.c. $\forall r \in R$, $h \in I$, $rh \in I$ e $hr \in I$. Se $I \neq R$, si dice che è un IDEALE PROPRIO.

OSS. $\ker f$ è un IDEALE

es. $I + J$ e $I \cap J$ sono ideali.

Def. $IJ = \{ a_1 b_1 + a_2 b_2 + \dots + a_n b_n \mid a_i \in I, b_j \in J \}$

OSS. IJ è un ideale di R.

Def. $(a) = \{ a \cdot r \mid r \in R \}$. $(a,b) = (a) + (b)$ (vd. span).

es. $A = \mathbb{R}[x]$, dato $a = x^2 + x + 1$

$(x^2+x+1) = \{ (x^2+x+1) f(x) \mid f(x) \in \mathbb{R}[x] \}$

OSS. In $\mathbb{Z}$, per esempio, (a) (sottogruppo generato) e (a) (ideale generato) coincidono.

OSS. $\mathbb{Z} \times \mathbb{Z}$ non è un dominio, benché $\mathbb{Z}$ lo sia, infatti: $(1,0)(0,1) = (0,0)$.

L'anello $\mathbb{K}[x]$

Sia $\mathbb{K}$ un campo, un polinomio di $\mathbb{K}[x]$ è del tipo
$$f(x) = a_m x^m + \ldots + a_1 x + a_0$$

Si definisce il grado come:

- $\deg f(x) = m$, se $m > 0 \vee a_0 \neq 0_{\mathbb{K}}$
- $\deg 0$ invece è talvolta non definito (porlo 0 rende problematiche le proprietà del grado).

Divisione euclidea tra polinomi

Sia $f(x) \in \mathbb{K}[x]$ e $g(x) \in \mathbb{K}[x] \setminus \{0\}$, allora $\exists\ q(x), r(x) \mid f(x) = q(x)\,g(x) + r(x)$ con $r(x) = 0$ $\vee$ $\deg(r(x)) < \deg(g(x))$.

es.

$$
\begin{array}{cccc|l}
x^3 & & 6x & 7 & x^2+3x+2 \\
x^3 & 3x^2 & 2x & & \hline x-3 \\
\hline
 & -3x^2 & 4x & 7 & \\
 & -3x^2 & -9x & -6 & \\
\hline
 & 0 & 13x & 13 &
\end{array}
$$

$$\Longleftrightarrow \quad x^3+6x+7 = (x^2+3x+2)\overbrace{(x-3)}^{q(x)} + \underbrace{13(x+1)}_{r(x)}$$

MCD in $\mathbb{K}[x]$

Def. Dati $f(x), g(x) \in \mathbb{K}[x] \mid (f(x), g(x)) \neq (0,0)$, $MCD(f(x), g(x))$ soddisfa le seguenti proprietà:

- $c(x) \mid f(x) \wedge c(x) \mid g(x) \Rightarrow \deg c(x) \leq \deg MCD(f(x), g(x))$, $c(x) \in \mathbb{K}[x]$
- $MCD(f(x), g(x)) \mid f(x) \wedge MCD(f(x), g(x)) \mid g(x)$

Algoritmo di Euclide

$$f(x) = g(x)\, q(x) + r(x), \quad \deg r(x) < \deg q(x)$$

- $a(x) \mid f(x) \wedge a(x) \mid g(x) \Longrightarrow$
  $\Longrightarrow a(x) \mid r(x)$
- $a(x) \mid g(x) \wedge a(x) \mid r(x) \Longrightarrow$
  $\Longrightarrow a(x) \mid f(x)$

Quindi: $\mathrm{Div}(f(x), g(x)) = \mathrm{Div}(g(x), r(x))$.
E' pertanto possibile applicare l'algoritmo di Euclide per trovare un MCD (che <u>non</u> è generalmente unico!).

L'algoritmo termina perché i gradi dei resti decrescono strettamente e sono maggiori di 0 (eccetto per 0).

Identità di Bézout

$\forall f(x), g(x) \in \mathbb{K}[x] \mid (f(x), g(x)) \neq (0,0) \;\exists$
$\lambda(x), \mu(x) \in \mathbb{K}[x] \mid \lambda(x) f(x) + \mu(x) g(x) =$
$= m(x)$, dove $m(x)$ e' un MCD di $f(x)$ e di $g(x)$.

Si nota subito che ogni MCD divide ogni altro MCD:

quindi ogni MCD differisce per una costante moltiplicativa.

Prop. $a(x) \mid b(x)c(x)$ con $MCD(a(x), b(x)) = 1$, allora $a(x) \mid c(x)$.

$$\lambda(x)\, a(x) + \mu(x) b(x) = 1 \implies$$

$$\to \underbrace{\lambda(x) a(x) c(x)}_{a(x) \mid a(x)} + \mu(x) \underbrace{b(x) c(x)}_{a(x) \mid b(x) c(x)} = c(x)$$

$$a(x) \mid a(x) \quad \wedge \quad a(x) \mid b(x)c(x) \implies a(x) \mid c(x) \quad \boxtimes$$

Anelli quozienti

Dati A anello e I ideali, si considera A/I (classi laterali su I):

$$A/I = \{a + I \mid a \in A\}$$

A/I è gruppo perché I è normale, in quanto abeliano.

Si definisce anche il prodotto:

$$(b_1 + I)(b_2 + I) = b_1 b_2 + I$$

Si verifica quando è ben definito:

- $b_1' + I = b_1 + I \Rightarrow b_1' = b_1 + \gamma_1,\ \gamma_1 \in I$
- $b_2' + I = b_2 + I \Rightarrow b_2' = b_2 + \gamma_2,\ \gamma_2 \in I$
- $b_1 b_2 + I \overset{?}{=} (b_1 + \gamma_1)(b_2 + \gamma_2) + I$
  - $(b_1 + \gamma_1)(b_2 + \gamma_2) = b_1 b_2 + \underbrace{\gamma_2 b_1 + \gamma_1 b_2 + \gamma_1 \gamma_2}_{\in I}$
  - Quindi sono le stesse classi laterali $\Rightarrow$ È BEN DEFINITO

Pertanto A/I è un anello con unità.

es. $A = \mathbb{K}[x]$ e sia $f(x) \in \mathbb{K}[x]$, posso dunque costruire l'anello quotiente $\mathbb{K}[x]/(f(x))$.

OSS. $f(x) + (g(x)) = r(x) + (g(x))$, dove $r(x)$ è il resto della divisione di $f(x)$ per $g(x)$.

es. $\mathbb{Z}_2[x]/(x^2 + x + 1)$ ha 4 elementi:

- $0, 1$
- $x, x+1$

es. $(x+I)(x+1+I) = x^2+x+I =$ $\quad I = (x^2+x+1)$

$= 1+I$ (infatti $x^2+x = (x^2+x+1)+1$ in $\mathbb{Z}_2$).

In particolare $\mathbb{Z}_2[x]/(x^2+x+1)$ è un campo perché x^2+x+1 è IRRIDUCIBILE.