Alcuni richiami sui polinomi

Le prime definizioni che riportiamo sono le ben note definizioni delle strutture algebriche fondamentali che sono necessarie per precisare correttamente la definizione di polinomio e le relative questioni di divisibilità.

1. Un insieme non vuoto A è un *anello associativo* se in A sono definite due operazioni, denotate con + e $\cdot$ rispettivamente, tali che per a, b, c in A:
i. $a+b$ sta in A
ii. $a+b = b+a$
iii. $(a+b)+c = a+(b+c)$
iv Esiste in A un elemento 0 tale che $a+0 = a$, per ogni a in A.
v. Per ogni a esiste un elemento $-a$ in A tale che $a+(-a) = 0$.
vi. $a \cdot b$ sta in A.
vii. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
viii. $a \cdot (b+c) = a \cdot b + a \cdot c$ e $(b+c) \cdot a = b \cdot a + c \cdot a$
Come è ben noto gli assiomi da i a v dicono che A con l'operazione + è un gruppo abeliano.
2. Un anello A si dice *anello con unità (o unitario)* se esiste in A un elemento 1 tale che $a \cdot 1 = 1 \cdot a = a$, per ogni a di A.
3. Un *anello A* si dice *commutativo* se $a \cdot b = b \cdot a$, per ogni a e b in A.
4. Un anello commutativo si dice *dominio di integrità* se è privo di *divisori dello zero* (cioè non esistono a e b non nulli tali che $a \cdot b = 0$).
5. Un anello si dice *anello di divisione o corpo* se i suoi elementi non zero formano un gruppo rispetto alla moltiplicazione.
6. Un *campo* è un corpo commutativo.
7. Un dominio di integrità A si dice *anello euclideo* se per ogni elemento a di A non nullo é definito un intero non negativo $d(a)$ tale che

- $\forall a, b \in A$, entrambi diversi da 0, $d(a) \leq d(a \cdot b)$
- $\forall a, b \in A (a, b \neq 0), \exists q, r \in A : a = bq + r$, dove $r=0$ oppure $d(r)<d(b)$

Sono ben noti gli esempi di gruppo, anello, campo.

Può essere invece utile proporre qualche esempio di anello euclideo:

- L'insieme degli interi relativi con le ordinarie operazioni di addizione e di moltiplicazione è un anello euclideo ponendo $d(a)=|a|$
- Gli interi di Gauss, cioè i numeri complessi della forma $a+ib$ con a,b numeri interi, con le ordinarie operazioni di addizione e moltiplicazione in $\mathbb{C}$ sono un anello euclideo, ponendo $d(a+ib)= a^2+b^2$.

Vedremo nel seguito che anche i polinomi in una indeterminata a coefficienti in un campo sono un anello euclideo.
L'interesse degli anelli euclidei per il problema di cui ci stiamo occupando sta nel fatto che in un anello euclideo si definisce la divisibilità, si dimostra l'esistenza di un massimo comun divisore, si dà la definizione di elemento primo o irriducibile e si dimostra il teorema di "fattorizzazione unica".
Questi concetti sono ben noti nell'insieme dei numeri interi e possono così essere "trasferiti" ai polinomi. Questa analogia, al di là del livello di formalizzazione e di astrazione a cui si vuole arrivare, è certamente importante dal punto di vista didattico in quanto può fare da guida nella trattazione della fattorizzazione di polinomi in una variabile.

8. In un anello euclideo A un elemento non invertibile p si dice *primo (o irriducibile)* se quando $p = a \cdot b$, con $a,b \in A$, allora a o b è invertibile. (Ricordiamo che in un anello commutativo A, con unità 1, un elemento a si dice invertibile se esiste un elemento b in A tale che $ab=1$).

9. Un dominio d'integrità A con unità si dice *dominio a fattorizzazione unica* se:

i. Ogni elemento diverso da zero di A o è invertibile o si può scrivere come prodotto di un numero finito di elementi irriducibili di A.

ii. La decomposizione di cui in (i) è unica, a meno dell'ordine e di associati degli elementi irriducibili.

Ricordiamo che un elemento a si dice associato di b se $a=b \cdot u$ dove u è invertibile (ad esempio in $\mathbb{Z}$ due elementi tra loro opposti sono associati in quanto ottenibili uno dall'altro moltiplicando per –1 che è invertibile).

Un anello euclideo è un dominio a fattorizzazione unica. Il viceversa è però falso. Si può ad esempio dimostrare che l'insieme dei polinomi in due variabili a coefficienti in un campo, di cui sarà data una definizione più precisa in seguito, è un dominio a fattorizzazione unica ma non un anello euclideo.

10. Se $a \neq 0$ e b sono elementi di un anello commutativo A si dice che a divide b se esiste $c \in A$ tale che $b=a \cdot c$.

11. Sia A un anello commutativo con unità. Se $a, b \in A$, allora $d \in A$ si dice *massimo comun divisore* di a e b se

i. d divide a e d divide b

ii. se c divide a e c divide b allora c divide d.

Si dimostra che in un dominio a fattorizzazione unica due elementi qualunque ammettono un massimo comun divisore.

12. Definiamo **polinomio** in una indeterminata x a coefficienti in un campo K una espressione della forma $a_0 + a_1 x + ... a_i x^i ..... + a_n x^n$, dove i, $0 \leq i \leq n$, è un intero non negativo e $a_0, a_1, ..., a_n$ sono elementi di K e sono detti coefficienti (x è un simbolo formale).

Con le usuali ben note operazioni di addizione e moltiplicazione l'insieme dei polinomi in x a coefficienti in K risulta un anello commutativo con unità che si indica con $K[x]$

Posto $p(x) = a_0 + a_1 x + ... + a_n x^n$ con $a_n \neq 0$, allora l'intero n si chiama grado di $p(x)$ e si indica con deg $p(x)$ o più brevemente deg p.

a_n è invece il coefficiente direttivo del polinomio $p(x)$.

Si dimostra che:

- $K[x]$ è un dominio di integrità,
- $\deg f(x) \leq \deg(f(x)g(x))$, $\forall f(x), g(x)$ diversi dal polinomio nullo,
- vale inoltre il cosiddetto **teorema di divisione per polinomi:**

Sia K un campo. Siano $f(x), g(x)$ polinomi in $K[x]$, con $f(x) \neq 0$.
Allora esistono polinomi $q(x), r(x)$, con $\deg r(x) \leq \deg f(x)$ tali che
$g(x) = f(x)q(x)+r(x)$.
Se anche $g(x) = f(x)q_1(x)+r_1(x)$ con $\deg r_1(x) < \deg f(x)$,
allora $q(x) = q_1(x)$, $r(x) = r_1(x)$.

Ne segue che $K[x]$ è un anello euclideo ponendo $d(p(x))=\deg p(x)$.

Dunque

i) due polinomi $f(x)$ e $g(x)$ di $K[x]$ ammettono un massimo comun divisore esprimibile nella forma $d(x)=a(x)f(x)+b(x)g(x)$.

ii) Ogni polinomio di $K[x]$ si può scrivere in modo unico come prodotto di polinomi irriducibili in $K[x]$ (a meno dell'ordine e di associati degli elementi irriducibili, cioè di elementi del campo).

Può essere conveniente riformulare la definizione di elemento primo, già vista per un qualunque anello euclideo, nel caso particolare dei polinomi.

In particolare è utile osservare che:
Un **polinomio** *p(x)* di *K[x]* si dice **irriducibile o primo** su *K* se una fattorizzazione *p(x) = a(x)b(x),* con *a(x), b(x)∈ K[x]* implica che uno dei due polinomi *a(x)* o *b(x)* ha grado 0 (è cioè una costante).
Esempio: in $\mathbb{Q}[x]$ i polinomi *2x+4* , *x+2*, *-x-2*, *4x+8* sono tutti irriducibili. Essi sono anche fra loro "associati" in quanto ottenibili uno dall'altro moltiplicando per un elemento invertibile cioè un polinomio di grado zero (elemento non nullo del campo).
Un polinomio di grado n, a coefficienti in un campo *K*, si dice allora **riducibile** se può essere espresso come prodotto di due polinomi a coefficienti in *K* di grado maggiore di 0 e minore di n.
In *K[x]* è inoltre possibile:
- dimostrare il **teorema del resto (o della radice o di Ruffini)**: *Se p(x) é un polinomio in K[x] (K é un campo) e a∈K é una sua radice (cioè p(a)=0) allora* $p(x) = (x-a)q(x)$ *e viceversa.*
- ricavare costruttivamente il massimo comun divisore con l'algoritmo di Euclide.

Spesso nella pratica didattica si considerano polinomi a coefficienti interi cioè elementi di $\mathbb{Z}[x]$.
Va osservato che $\mathbb{Z}[x]$ é solamente un "dominio a fattorizzazione unica" ma non é euclideo (non sempre esiste un polinomio quoziente a coefficienti interi).
Per quanto riguarda i polinomi in più variabili si è già detto che *K[x,y],* inteso come *(K[x])[y]* , cioè come insieme dei polinomi in *y* a coefficienti in *K[x],* è un dominio a fattorizzazione unica ma non è un anello euclideo.

Esaminiamo ora il problema della fattorizzazione in $\mathbb{C}[x]$, $\mathbb{R}[x]$,$\mathbb{Q}[x]$, $\mathbb{Z}[x]$.

Fattorizzazione in $\mathbb{C}[x]$.
Il teorema fondamentale dell'algebra, come è noto, afferma che un polinomio in $\mathbb{C}[x]$ di grado $n \geq 1$ ha una radice in $\mathbb{C}$. Ne segue immediatamente che in $\mathbb{C}[x]$ ogni polinomio di grado n si scompone nel prodotto di n fattori lineari.

Fattorizzazione in $\mathbb{R}[x]$.
Se guardiamo un polinomio di $\mathbb{R}[x]$ come polinomio in $\mathbb{C}[x]$ esso si scompone in fattori lineari:
$(x-\beta_1)\ldots.(x-\beta_n)(x-\alpha_1)(x-\alpha_1^*)\ldots..(x-\alpha_m)(x-\alpha_m^*)$ dove $\beta_1,...,\beta_n$ sono radici reali mentre le α_i , α_i^* sono coppie di soluzioni complesse coniugate. Si dimostra infatti facilmente che se α é una soluzione complessa di un polinomio a coefficienti in $\mathbb{R}$, anche α^*, sua coniugata, é una soluzione. Essendo $(x-\alpha_i)(x-\alpha_i^*) = x^2 - 2\mathrm{Re}(\alpha_i)x + \alpha_i\alpha_i^*$ un polinomio irriducibile in $\mathbb{R}[x]$ si deduce che in $\mathbb{R}[x]$ gli unici polinomi irriducibili sono quelli di primo grado e quelli di 2° grado della forma $ax^2 + bx + c$ che hanno radici complesse coniugate, cioè, come è noto, quelli in cui $b^2 - 4ac < 0$.
Da queste considerazioni segue anche che un polinomio di grado dispari ha sempre almeno un fattore lineare in $\mathbb{R}[x]$, un polinomio di grado pari può avere al più un numero pari di fattori lineari. Naturalmente questo risultato ci consente di dire se un polinomio in $\mathbb{R}[x]$ è o no riducibile ma non ci dà informazioni su come fattorizzare un polinomio riducibile: è noto che non sempre questo può essere fatto in modo semplice.

Fattorizzazione in $\mathbb{Q}[x]$.
In $\mathbb{Q}[x]$ a differenza di quanto accade in $\mathbb{R}[x]$ e in $\mathbb{C}[x]$ non possiamo descrivere esplicitamente l'insieme dei polinomi irriducibili ma possiamo solo fornire alcuni criteri che implicano l'irriducibilità.
Il problema della fattorizzazione in $\mathbb{Q}[x]$ è strettamente connesso allo stesso problema in $\mathbb{Z}[x]$. Infatti ogni polinomio di $\mathbb{Q}[x]$ è associato di un polinomio in $\mathbb{Z}[x]$, ottenuto moltiplicando ciascun coefficiente per il m.c.m. fra i denominatori dei suoi coefficienti. Si dimostra inoltre una proposizione (lemma di Gauss) che asserisce che un polinomio a coefficienti interi è irriducibile in $\mathbb{Q}[x]$ se e solo se lo è in $\mathbb{Z}[x]$. Dunque un polinomio di $\mathbb{Q}[x]$ è irriducibile se e solo se lo è in $\mathbb{Z}[x]$ il polinomio a coefficienti interi ad esso associato.
Esaminiamo allora il problema della fattorizzazione in $\mathbb{Z}[x]$.

Fattorizzazione in $\mathbb{Z}[x]$.

Un primo passo nello studio della irriducibilità di un polinomio in $\mathbb{Z}[x]$ è la ***ricerca di eventuali fattori lineari.***

Si dimostra facilmente che se $a_n x^n + \ldots + a_1 x + a_0$ è un polinomio a coefficienti interi e a/b (a , b primi fra loro) ne è una radice, allora a divide il termine noto e b divide il coefficiente del termine di grado più alto.

La ricerca delle radici ci consente di dire se il polinomio ha o meno fattori lineari. Questo risolve il problema dell'irriducibilità per polinomi di grado 2 o 3 che, se sono riducibili, hanno almeno un fattore lineare.

Più complicato è stabilire se un polinomio che non ha fattori lineari è o no irriducibile.

Un criterio per dimostrare che alcuni polinomi sono irriducibili è il ***Criterio di Eisenstein***: se $a(x) = a_0 + a_1 x + \ldots + a_n x^n$ è un polinomio in $\mathbb{Z}[x]$ ed esiste un numero primo p tale che p divide tutti gli a_i tranne il coefficiente di grado massimo e p^2 non divide il termine noto, allora $a(x)$ é irriducibile in $\mathbb{Z}[x]$.

Esempi: 1) $x^5 + 3x^2 - 3x + 6$ risulta irriducibile prendendo p=3.

2) $x^4+5x+15$ risulta irriducibile prendendo p=5.

3) $x^n - p$ con p primo è irriducibile (questo dice tra l'altro che esistono polinomi irriducibili di qualsiasi grado).

Il Criterio di Eisenstein è molto utile ma è evidente che non sempre è possibile applicarlo.

E' chiaro che nei casi in cui tale criterio non si applica il polinomio può essere irriducibile (come ad esempio $x^2-3x+13$) o riducibile (ad esempio $x^5+5x^3+2x^2+10$ che si fattorizza nel prodotto $(x^3+2)(x^2+5)$, come si vede facilmente applicando opportunamente la proprietà distributiva (secondo la terminologia usualmente utilizzata a scuola, effettuando un raccoglimento parziale)).

Nei casi in cui il criterio considerato non si applica e non vi sono fattori lineari si può anche cercare di fattorizzare il polinomio dato scrivendolo come prodotto di due polinomi di grado inferiore con coefficienti incogniti, svolgendo tale prodotto ed imponendo l'uguaglianza fra i coefficienti così ottenuti e quelli del polinomio dato. Si perviene così ad un sistema di cui si cercano le eventuali soluzioni intere. Tale metodo è però effettivamente praticabile soltanto per polinomi di grado non molto alto (ad esempio 4 o 5), in quanto altrimenti comporta calcoli troppo complessi.

Un'altra possibilità è utilizzare il seguente risultato:

Se un polinomio $p(x)$ é irriducibile in $Z_m[x]$ per un m primo con a_n allora $p(x)$ é irriducibile in $Z[x]$.

Infatti se $a(x)b(x)$ é una fattorizzazione in $Z[x]$ di $p(x)$, ad essa, passando a $Z_m[x]$, corrisponde una effettiva fattorizzazione $\underline{a(x)}\cdot\underline{b(x)}$ se m é primo con a_n.

Ad esempio il polinomio $2x^3 + 7x^2 - 3x + 2$ è irriducibile in $Z[x]$, in quanto passando a $Z_3[x]$ diventa $\underline{2}x^3+x^2+\underline{2}$ che é irriducibile perché $\underline{0},\underline{1},\underline{2}$ non sono soluzioni.

Analogamente il polinomio x^5+x^3+2x+5 è irriducibile in $Z[x]$ in quanto passando a $Z_2[x]$ si ottiene $x^5+x^3+\underline{1}$ che non ha radici in $Z_2[x]$ e non si scompone nel prodotto di due fattori di 3° e 2° grado rispettivamente come si può facilmente verificare. Notiamo a questo proposito che è evidente che in $Z_m[x]$ la ricerca delle possibili fattorizzazioni anche "per tentativi" risulta più semplice.

E' altrettanto evidente, ma importante sottolineare, che la riducibilità di un polinomio in $Z_m[x]$ non implica la riducibilità in $Z[x]$. (Ad esempio x^2+1 è riducibile in $Z_2[x]$, dove $x^2+\underline{1}=(x+\underline{1})(x+\underline{1})$, mentre è irriducibile in $Z[x]$.)