Corso di Algebra C. Anno accademico 2005-2006

Note integrative

- **La definizione formale di anello e di campo.**

Definizione Un anello (non banale, con identità) R è un insieme che possiede due elementi speciali diversi fra loro (0 e 1) e dove sono definite due operazioni, che chiamiamo addizione ($+$) e moltiplicazione ($\cdot$), che soddisfano le seguenti proprietà:
- $\forall\ a, b, c \in R$ vale $(a+b)+c = a+(b+c)$ (proprietà associativa dell'addizione).
- $\forall\ a, b \in R$ vale $a+b = b+a$ (proprietà commutativa dell'addizione).
- $\forall\ a \in R$ vale $a+0 = a$ (0 è l'elemento identico per l'addizione).
- $\forall\ a \in R$ esiste un elemento "$-a$" in R tale che $a+(-a) = 0$ (esistenza dell'opposto per l'addizione).
- $\forall\ a, b, c \in R$ vale $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (proprietà associativa della moltiplicazione).
- $\forall\ a \in R$ vale $a \cdot 1 = a$ (1 è l'elemento identico per la moltiplicazione).
- $\forall\ a, b, c \in R$ vale $(a+b) \cdot c = a \cdot c + b \cdot c$ e anche $a \cdot (b+c) = a \cdot b + a \cdot c$ (proprietà distributive).

Osservazione importante: la definizione data sopra, per "colpa" della richiesta $0 \neq 1$, non include l' anello "banale" $A = \{0\}$, in cui tutte le operazioni sono banali e dunque lo 0 funziona da elemento identico sia per la somma che per la moltiplicazione. Noi vogliamo considerare A come un anello con identità e dunque lo aggiungiamo a quelli (non banali) che risultano dalla definizione.

Definizione Un anello (con identità) R che soddisfa anche la seguente proprietà si dice "commutativo":
- $\forall\ a, b \in R$ vale $a \cdot b = b \cdot a$ (proprietà commutativa della moltiplicazione).

Definizione Un anello (con identità) R che soddisfa anche la seguente proprietà si dice "privo di divisori di 0":
- $\forall\ a, b \in R$ vale che $a \cdot b = 0$ implica $a = 0$ o $b = 0$.

Definizione Un elemento u di un anello con identità R si dice una "unità" o "invertibile" se esiste un $v \in R$ tale che $u \cdot v = v \cdot u = 1$ (cioè se esiste un inverso sinistro e destro di u rispetto alla moltiplicazione).

Definizione Un anello non banale, con identità, commutativo, che soddisfa anche la seguente proprietà è detto "campo":
- ogni $a \in R - \{0\}$ è invertibile (esistenza dell'inverso rispetto alla moltiplicazione per tutti gli elementi diversi da 0).

Osservazione. Come si può facilmente dimostrare (esercizio!), un campo è anche automaticamente "privo di divisori dello 0".

- **Il piccolo teorema di Fermat.**

Oltre agli anelli ($\mathbb{Z}$) e campi ($\mathbb{Q}, \mathbb{R}$) noti fin dalle scuole superiori, nel corso di LMM abbiamo introdotto gli anelli $\mathbb{Z}_m$ (dove m è un intero positivo) i cui elementi sono le classi di resto in $\mathbb{Z}$ rispetto alla divisione euclidea per m. Nella prima lezione di questo corso di algebra abbiamo anche ridimostrato che, se $m = p$ è un numero primo, allora $\mathbb{Z}_p$ è un campo e che, se invece m non è primo, $\mathbb{Z}_m$ non è un campo.

A riguardo dei campi $\mathbb{Z}_p$, ricordiamo l'enunciato del piccolo teorema di Fermat: per vedere due dimostrazioni ed alcuni esempi potete consultare le note integrative del corso di LMM alla pagina

$http://www.dm.unipi.it/\ gaiffi/lmm\_\_2005/Newappunti\_\_integrazioni.pdf$

Teorema Se p è un numero primo e a è un numero intero positivo che non è un multiplo di p, allora vale

$$a^{p-1} \equiv 1 \quad (p)$$

Il piccolo teorema di Fermat si può anche esprimere con il linguaggio degli anelli $\mathbb{Z}_p$. Ecco come:
Teorema Se p è un numero primo e $[a] \neq [0]$ in $\mathbb{Z}_p$ allora in $\mathbb{Z}_p$ vale

$$[a]^{p-1} = [1]$$

Questo è (ovviamente) un enunciato equivalente:
Teorema Se p è un numero primo allora per ogni $[a]$ in $\mathbb{Z}_p$ vale

$$[a]^p = [a]$$

Quando è chiaro che stiamo lavorando in $\mathbb{Z}_p$ si possono, per brevità, omettere le parentesi quadre:
Teorema Se p è un numero primo allora per ogni a in $\mathbb{Z}_p$ vale

$$a^p = a$$

- **I polinomi**.

I polinomi sono somme formali, a cui possono essere associate delle funzioni.

Definizione Un polinomio nella variabile x a coefficienti nel campo K è una espressione del tipo $p(x) = \sum_{i=1}^{n} a_i x^i$, con $\{a_0, ..., a_n\} \subset K$. Se inoltre per qualche $m \leq n$ si ha che $a_m \neq 0$ e $\forall k > m \;\; a_k = 0$ diciamo che p è di grado m, e scriviamo $deg(p) = m$. L'insieme dei polinomi nella variabile x a coefficienti nel campo K si indica con $K[x]$.

Osservazione. Si noti che non abbiamo assegnato un grado al polinomio nullo, ossia a $p(x) = 0$. Abbiamo assegnato un grado a tutti i polinomi non nulli.

Definizione Diciamo che due polinomi sono uguali se sono uguali tutti i loro coefficienti (principio di identità fra polinomi).

Un polinomio p determina una funzione da K a K, associando al numero c il valore $p(c) = \sum_{i=1}^{n} a_i c^i$.

Osservazione. ATTENZIONE ! In classe abbiamo visto che se le funzioni associate a due polinomi p, q sono uguali, non è detto che i due polinomi siano uguali. Per esempio abbiamo considerato in $\mathbb{Z}_2[x]$ i due polinomi $f(x) = x + 1$ e $g(x) = x^{134} + 1$ che sono DIVERSI ma che danno luogo alla stessa funzione. Questo può accadere dato che il campo su cui stiamo lavorando ha solo un numero finito di elementi, mentre invece, come vedremo, non capita con i campi infiniti.

Definizione Dati due polinomi $p(x) = \sum_{i=1}^{n} a_i x^i, q(x) = \sum_{j=1}^{m} b_i x^i$ si definiscono la loro somma ed il loro prodotto come

$$(p+q)(x) = \sum_{i=0}^{max(m,n)} (a_i + b_i)x^i, \quad pq(x) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j x^{i+j}$$

Teorema $(K[x], +, \cdot, 0, 1)$ è un anello.
Dimostrazione : esercizio (lunghe e facili verifiche). □

Teorema Dati due polinomi non nulli $p, q \in K[x]$, si ha che

$$deg(pq) = deg(p) + deg(q)$$

Dimostrazione Siano $h = deg(p)$, $k = deg(q)$. Si ha allora che $p = \sum_{i=0}^{h} a_i x^i$ e $q = \sum_{j=0}^{k} b_j x^j$, con $a_h \neq 0$ e $b_k \neq 0$. Per la definizione di prodotto, vale $pq = \sum_{i=0}^{h}\sum_{k=0}^{k} a_i b_j x^{i+j}$. Il massimo esponente per x in questa somma è $h + k$, e il suo coefficiente e' $a_h b_k$, che è diverso da zero in quanto sia che a_h che b_k sono diversi da zero. Quindi per definizione di grado, il grado di pq è esattamente $h+k$. □

Teorema Dati due polinomi $p(x) = \sum_{i=1}^{n} a_i x^i, q(x) = \sum_{j=1}^{m} b_i x^i$ e $c \in \mathbb{R}$, si ha che

$$(p+q)(c) = p(c) + q(c), \quad pq(c) = p(c)q(c)$$

Dimostrazione : esercizio. □

Esercizio: Dato il polinomio $p(x) = x^2 - 2$, si determinino i $c \in \mathbb{R}$ per cui $p(c) \geq 0$.

Definizione Diciamo che $\lambda \in K$ è una *radice* del polinomio $p(x)$ se $p(\lambda) = 0$.

Esempio Sia $p(x) = x^2 + 1 \in \mathbb{R}[x]$. Il polinomio p non ha radici in $\mathbb{R}$: se $\lambda \in \mathbb{R}$, si ha che $p(\lambda) = 1 + \lambda^2 \geq 1 > 0$. Costruiremo in seguito un campo (il campo $\mathbb{C}$ dei numeri complessi) che include $\mathbb{R}$, dove questo polinomio ha due radici.

Così come per i numeri interi, in $K[x]$ esiste una nozione di divisione con resto fra i polinomi, nella quale gioca un ruolo cruciale il concetto di grado di un polinomio.

Definizione Siano $p(x), s(x) \in K[x]$, con K un campo e $s(x) \neq 0$. Diciamo che $q(x), r(x) \in K[x]$ sono *quoziente* e *resto* della divisione di p per s se $p(x) = q(x)s(x) + r(x)$ e $r(x) = 0$ oppure $deg(r(x)) < deg(s(x))$

Ma si trovano sempre il quoziente e il resto descritti sopra, ossia si può sempre fare la divisione euclidea fra polinomi ? Ci risponde il seguente teorema:

Teorema Dati $p(x), s(x) \in K[x]$, con K un campo e $s(x) \neq 0$, esistono e sono unici $q(x), r(x) \in K[x]$ *quoziente* e *resto* della divisione di p per s
Dimostrazione Per quanto riguarda l'unicità, supponiamo che esistano q_1, q_1, r_1, r_2 tali che

$$p(x) = q_1(x)s(x) + r_1(x), \quad p(x) = q_2(x)s(x) + r_2(x)$$

con $deg(r_1) < deg(p)$, $deg(r_2) < deg(p)$. Facendo la differenza fra le due equazioni precedenti otteniamo

$$(q_1(x) - q_2(x))s(x) = -(r_1(x) - r_2(x))$$

Se $q_1 \neq q_2$, allora $q_1 - q_2 \neq 0$ e quindi il polinomio a sinistra ha grado pari a $deg(s) + deg(q_1 - q_2) \geq deg(s)$. A destra però abbiamo due polinomi di grado strettamente più piccolo del grado di s, e quindi la loro differenza ha grado strettamente più piccolo di quello di s, assurdo. Si deve quindi avere $q_1 = q_2$, e quindi anche $r_1 = r_2$. La dimostrazione dell'esistenza è per induzione su $deg(p)$.
Se $deg(p) < deg(s)$, possiamo prendere $q = 0$ e $r = p$. Supponiamo di conoscere l'esistenza di q, r quando $deg(p) \leq n$, e sia $deg(p) = n + 1$. Se $a \in K$ è il coefficiente di grado massimo di p e b è il coefficiente di grado massimo di s, il polinomio $p_1 = p - (\frac{a}{b}x^{deg(p)-deg(s)})s$ ha grado strettamente più basso del grado di p, e quindi esistono per ipotesi induttiva q_1, r_1 tali che

$$p_1(x) = q_1(x)s(x) + r_1(x)$$

con $deg(r_1) < deg(s)$. Si ha quindi che

$$p(x) = p_1(x) + (\frac{a}{b}x^{deg(p)-deg(s)})s = q_1(x)s(x) + r_1(x) + (\frac{a}{b}x^{deg(p)-deg(s)})s(x) =$$

$$\left(q_1(x) + \frac{a}{b}x^{deg(p)-deg(s)}\right)s(x) + r_1(x)$$

□

La dimostrazione del teorema fornisce anche un algoritmo per calcolare quoziente e resto in una divisione fra polinomi; si tratta in sostanza della "divisione fra polinomi"

che avete imparato alle scuole superiori.

Esempio In $\mathbb{Q}[x]$, dividere il polinomio $p(x) = 2x^4 + x^3 + -x^2 + 1$ per $s(x) = 3x^2 + 1$.

Definiamo q e r per approssimazioni successive, seguendo il metodo di dimostrazione del teorema.

$$p_1 = p - (\frac{a}{b}x^{deg(p)-deg(s)})s = 2x^4 + x^3 + -x^2 + 1 - \frac{2}{3}x^2(3x^2 + 1) = x^3 - \frac{5}{3}x^2 + 1$$

Ripetiamo il procedimento con p_1 al posto di p

$$p_2 = p_1 - \frac{1}{3}x(3x^2 + 1) = -\frac{5}{3}x^2 - \frac{1}{3}x + 1$$

Ripetiamo una terza volta il procedimento con p_2 al posto di p

$$p_3 = p_2 + \frac{5}{9}(3x^2 + 1) = -\frac{1}{3}x + \frac{14}{9}$$

Possiamo ora usare questo p_3 come r, e abbiamo

$$p = p_1 + \left(\frac{2}{3}x^2\right)s = p_2 + \left(\frac{1}{3}x + \frac{2}{3}x^2\right)s = p_3 + \left(-\frac{5}{9} + \frac{1}{3}x + \frac{2}{3}x^2\right)s$$

Riassumendo, abbiamo calcolato

$$p = \left(-\frac{5}{9} + \frac{1}{3}x + \frac{2}{3}x^2\right)(3x^2 + 1) + \left(-\frac{1}{3}x + \frac{14}{9}\right)$$

□

Definizione Diciamo che il polinomio s *divide* il polinomio p se esiste un polinomio q tale che $p(x) = q(x)s(x)$. In modo equivalente, s divide p se il resto della divisione di p per s è uguale a zero. In questo caso scriviamo $s|p$.

Teorema Il polinomio $p(x) \in K[x]$ ha la radice $\lambda \in K$ se e solo se il polinomio $x - \lambda$ divide p.
Dimostrazione Supponiamo che il polinomio $x - \lambda$ divida p. Per definizione, esiste q tale che $p(x) = q(x)(x - \lambda)$. Sostituendo λ in questa espressione otteniamo che $p(\lambda) = 0$.
Viceversa, supponiamo che λ sia una radice di p, e siano q, r il quoziente e il resto della divisione di p per $s = x - \lambda$. Per dimostrare che $x - \lambda$ divide p basta dimostrare che $r = 0$. Si ha

$$p(x) = q(x)(x - \lambda) + r(x)$$

con $r(x) = 0$ oppure $deg(r) < 1$. Deve allora essere $r(x) = 0$ oppure $deg(r) = 0$, cioè $r(x) = k \neq 0 \in K$. Supponiamo per assurdo che valga $r(x) = k \neq 0 \in K$; sostituendo λ nell'espressione si ha

$$p(\lambda) = 0 + k$$

e quindi deve essere $k = 0$ dato che $p(\lambda) = 0$ per ipotesi. Questo è assurdo, dunque deve valere $r(x) = 0$. □

Corollario Dato un campo K, ogni polinomio $p(x) \in K[x]$ di grado $n \in \mathbb{N}$ ha al più n radici distinte in K.
Dimostrazione Per induzione su $deg(p)$. Se $deg(p) = 0$ l'enunciato è vero perché p è una costante e non ha radici. Se $deg(p) = 1$ allora p è della forma $p(x) = ax + b$ con $a \neq 0$ e ha esattamente una radice in K, cioè $\frac{-b}{a}$.

Ora dedichiamoci al passo induttivo: se $deg(p) = n+1 > 1$, possono darsi due casi: o p non ha radici, e allora verifica l'enunciato, oppure p ha radici, e allora sia α una radice di p. Per il teorema precedente, $p(x) = p_1(x)(x - \alpha)$. Per ipotesi induttiva, $p_1(x)$, che ha grado n, ha al più n radici distinte in K, chiamiamole $\alpha_1, \ldots, \alpha_r$ con $r \leq n$. Possiamo concludere che non ci sono radici di $p(x)$ diverse da $\alpha, \alpha_1, \ldots, \alpha_r$ (perché? Se non vi è chiaro guardate la nota alla fine) e dunque ce ne sono al più $r+1$ distinte (potrebbero essere anche r se α fosse uguale a una delle α_i). Comunque $r + 1 \leq n + 1$ come volevamo. □

Nota: infatti se per assurdo β fosse una radice diversa da $\alpha, \alpha_1, \ldots, \alpha_r$, allora si potrebbe scrivere

$$p(\beta) = p_1(\beta)(\beta - \alpha)$$

ossia

$$0 = p_1(\beta)(\beta - \alpha)$$

Poiché $\beta - \alpha \neq 0$, deve valere $p_1(\beta) = 0$ e dunque β sarebbe una radice di p_1 ma questo è assurdo perché β è diversa da $\alpha_1, \ldots, \alpha_r$.

Grazie a questo corollario possiamo dimostrare che:

Teorema Se K è un campo infinito, allora due polinomi $f(x), g(x)$ che sono uguali come funzioni da K in K sono anche uguali come polinomi.
Dimostrazione Consideriamo il polinomio $h(x) = f(x) - g(x)$. Visto che come funzione è la funzione nulla, ogni elemento di K è una radice per h. Dunque h ha infinite radici in K. Visto il corollario appena dimostrato, h non può essere un polinomio di grado n per nessun $n \in \mathbb{N}$. Dunque resta solo la possibilità che h sia il polinomio 0, ossia che $f(x) = g(x)$ come POLINOMI. □

- **Massimo comun divisore e Lemma di Bezout per polinomi a coefficienti in un campo.**

Definizione Dati due polinomi $p_1(x), p_2(x)$ in $K[x]$, non entrambi nulli, un *massimo comun divisore* di p_1, p_2 è un polinomio $d(x)$ che divide sia p_1 che p_2, e tale che ogni altro polinomio che divide sia p_1 che p_2 ha grado minore o uguale a quello di d.

Osservazione. Abbiamo scritto "un" massimo comun divisore e non "il" massimo comun divisore perché' secondo la nostra definizione il MCD fra due polinomi non è unico. Infatti se $d(x)$ è un massimo comune divisore, anche $kd(x)$ le proprietà richieste, dove $k \in K - \{0\}$, dunque anche $kd(x)$è un massimo comune divisore. Fra poco

dimostreremo appunto che tutti i massimi comuni divisori di due polinomi differiscono fra loro solo per la moltiplicazione per una costante.

Operativamente, un $MCD(p_1(x), p_2(x))$ si può calcolare usando l'algoritmo di Euclide, che funziona in maniera del tutto simile al caso dei numeri interi (esercitatevi !).

Teorema (il "Lemma di Bezout per polinomi"). Dati due polinomi non entrambi nulli f, g in $K[x]$, un massimo comun divisore d di f e g si può scrivere nella forma $d = af + bg$ per opportuni polinomi a, b di $\mathbb{K}[x]$.

Dimostrazione Consideriamo l'insieme $Z = \{z = xf + yg : \ (x, y \in \mathbb{K}[x]) \wedge (z \neq 0)\}$ e scegliamo un elemento $d = af + yg \in Z$ tale che $\forall z \in Z$ vale $deg(d) \leq deg(z)$. Adesso dividiamo f per d ottenendo $f = qd + r$ con $r = 0$ oppure $deg(r) < deg(d)$ e osserviamo come r sia un polinomio della forma $xf + yg$:

$$r = f - qd = f - q(af + yg) = f - qaf - qyg = (1 - qa)f + (-qy)g$$

Se r fosse diverso da zero apparterrebbe a Z, ma avendo supposto d come elemento di grado minimo di Z e sapendo che $deg(r) < deg(d)$ dobbiamo scartare questa ipotesi, per cui r è il polinomio zero. Dunque:

$$f(x) = c(x)d(x)$$

cioè $d \mid f$. Ripetendo lo stesso ragionamento per g troviamo che $d \mid g$.

Resta da mostrare che se un polinomio c è tale che $c \mid f$ e $c \mid g$ allora $deg\ c \leq deg\ d$. Mostreremo addirittura che $c \mid d$. Per ipotesi abbiamo che $f = ck$ e $g = cl$ per opportuni polinomi k e l; inoltre, considerando quanto visto al punto precedente, possiamo scrivere:

$$d = af + bg = a(ck) + b(cl) = c(ak + bl)$$

dunque $c \mid d$. □

Corollario Dati due polinomi non entrambi nulli $f(x), g(x)$ in $K[x]$, se $d_1(x)$ e $d_2(x)$ sono due massimi comuni divisori di $f(x)$ e $g(x)$, allora $d_1(x)$ e $d_2(x)$ differiscono fra loro solo per la moltiplicazione per una costante $k \in K$, $k \neq 0$:

$$d_1(x) = k\ d_2(x)$$

Dimostrazione Per prima cosa osserviamo che d_1 e d_2 devono avere lo stesso grado (infatti, essendo entrambi massimi comuni divisori, deve valere $deg\ d_1 \leq deg\ d_2$ e $deg\ d_2 \leq deg\ d_1$). Inoltre, nel corso della dimostrazione precedente abbiamo provato che se un polinomio c è tale che $c \mid f$ e $c \mid g$ e d è un massimo comune divisore, allora $c \mid d$. Dunque, visto che d_1 e d_2 sono entrambi massimi comuni divisori, deve valere $d_1 \mid d_2$ e $d_2 \mid d_1$. In particolare sia $m(x)$ tale che $d_2(x)m(x) = d_1(x)$: per considerazioni sul grado si conclude che $m(x)$ deve essere una costante non zero, cioè $m(x) = k \neq 0$. □

- **Polinomi irriducibili e il teorema di fattorizzazione unica per polinomi.**

Cominciamo ricordando la definizione di polinomio irriducibile. Notiamo che la definizione si riferisce non solo a $K[x]$, con K campo, ma anche ad anelli di polinomi i cui coefficienti stanno in un anello (per esempio $\mathbb{Z}[x]$).

Definizione Dato un anello A, un polinomio $p(x) \in A[x]$ si dice irriducibile se ha grado ≥ 1 e, ogni volta che vale

$$p(x) = a(x)b(x)$$

con $a(x)$ e $b(x)$ in $A[x]$, allora o $a(x)$ o $b(x)$ è una costante. Un polinomio non irriducibile si dice riducibile.

In altre parole, la definzione dice che un polinomio $p(x) \in A[x]$ è irriducibile se e solo se ha grado ≥ 1 e non ha fattorizzazioni non banali, ossia ogni sua fattorizzazione

$$p(x) = a(x)b(x)$$

è una "falsa" fattorizzazione, perché guardandola bene si scopre che uno dei due fattori $a(x)$ o $b(x)$ è di grado 0, una costante.

In classe abbiamo dimostrato il seguente teorema:

Teorema (*"primalità di un polinomio irriducibile"*). Se $p(x)$ è un polinomio irriducibile in $K[x]$ dove K è un campo, e $p(x) \mid f(x)g(x)$ (dove $f(x), g(x) \in K[X]$) allora o vale $p(x) \mid f(x)$ o vale $p(x) \mid g(x)$.

Questo teorema ci fa capire che i polinomi irriducibili in $K[x]$ svolgono lo stesso ruolo che i numeri primi svolgono in $\mathbb{Z}$ (infatti una proprietà caratterizzante di un numero primo era proprio questa: se $p \mid ab$ allora o $p \mid a$ o $p \mid b$).

Vale anche l'analogo del teorema di fattorizzazione unica (la dimostrazione è un esercizio caldamente consigliato; è una applicazione del teorema di primalità, e si procede in maniera del tutto simile alla dimostrazione della fattorizzazione unica in $\mathbb{Z}$; la trovate comunque sul Childs). Ricordiamo che due polinomi $f(x), g(x)$ in $K[x]$ si dicono "associati" se differiscono moltiplicativamente per una costante non nulla, ossia se $f(x) = k \cdot g(x)$ con $k \neq 0$.

Teorema Ogni polinomio di grado ≥ 1 in $K[x]$ (dove K è un campo) è irriducibile o si fattorizza come prodotto di polinomi irriducibili. Inoltre, se

$$f = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$$

sono due fattorizzazioni del polinomio f come prodotto di irriducibili, allora vale che $s = t$ e che i polinomi p_i e i polinomi q_j sono a due a due associati.

Notiamo che nel teorema precedente, quando si scrive

$$f = p_1 p_2 \cdots p_s$$

si intende che i p_i sono scritti anche con ripetizioni. Un altro modo di scrivere la fattorizzazione di un polinomio è quello di evidenziare gli irriducibili distinti (e non

associati) scrivendo ciascuno con l'esponente con cui compare. Per esempio si scriverà

$$h = q_1^{r_1} q_2^{r_2} \cdots q_t^{r_t}$$

dove i q_j sono polinomi irriducibili distinti e non associati fra loro e gli r_i sono numeri naturali positivi.

In questo modo è facile individuare, proprio come avveniva in $\mathbb{Z}$, un MCD di due polinomi. Se infatti prendiamo una fattorizzazione di un altro polinomio:

$$g = p_1^{s_1} p_2^{s_2} \cdots p_j^{r_j}$$

allora un MCD (h, g) si otterrà facendo il prodotto degli irriducibili che compaiono sia fra i p_m che fra i q_n, ciascuno preso col minimo esponente fra i due esponenti che troviamo nelle due fattorizzazzioni.

Per esempio, in $\mathbb{Q}[x]$, se

$$h(x) = (x-1)^2(x^2-5)^3(x^4-7x+7)$$

$$g(x) = (x-1)^7(x^2-5)(x^5+11x^2+11)^2$$

allora un MCD (h, g) è

$$(x-1)^2(x^2-5)$$

Gli altri MCD (h, g), come sappiamo, sono tutti i polinomi associati a $(x-1)^2(x^2-5)$.

Domanda. Perché i polinomi che compaiono in queste fattorizzazioni sono irriducibili in $\mathbb{Q}[x]$? Per alcuni è facile provarlo, per altri ci vogliono tanti calcoli. Come affrontereste il problema ? Vedremo più avanti in questo corso il criterio di irriducibilità di Eisenstein che ci darà un aiuto.

Osservazione. Il teorema di fattorizzazione unica vale in $K[x]$ quando K è un CAMPO. Per la dimostrazione usiamo infatti il teorema di primalità che a sua volta si dimostra tramite il teorema di Bezout che vale in $K[x]$ con K campo.

In realtà si può dimostrare che un teorema di fattorizzazione unica vale anche in $\mathbb{Z}[x]$. Ma in generale se A è un anello qualunque, bisogna stare attenti; guardate cosa può succedere in $\mathbb{Z}_{30}[x]$:

$$x^2 - 1 = (x-1)(x-29) = (x-19)(x-11)$$

Fate i conti e verificate che è vero. Queste sono due distinte fattorizzazioni in irriducibili (giacché si tratta di polinomi di grado 1) !

- **Polinomi irriducibili e radici.**

Questa osservazione merita un paragrafetto a parte. Se $p(x) \in K[x]$ è un polinomio irriducibile di grado > 1, allora $p(x)$ non può avere radici in K. Infatti se ne avesse una, diciamo α, allora come sappiamo si potrebbe scrivere:

$$p(x) = (x-\alpha)q(x)$$

Questa sarebbe una fattorizzazione non banale (uno dei fattori ha grado 1 e l'altro ha grado $(deg\ p - 1) \geq 1$..), ma ciò è assurdo visto che p è irriducibile.

Il viceversa in generale non è vero: un polinomio in K[x] che non ha radici potrebbe non essere irriducibile. Prendiamo per esempio $x^4 + 2x^2 + 1$ in $\mathbb{R}[x]$. Questo polinomio non ha radici (si nota che come funzione assume solo valori positivi) ma non è irriducibile, infatti vale:

$$x^4 + 2x^2 + 1 = (x^2 + 1)(x^2 + 1)$$

Dunque, se abbiamo un polinomio $f(x) \in K[x]$ di grado > 1 e dobbiamo decidere se è irriducibile o no, una strada che è possibile tentare è quella di controllare se $f(x)$ ha radici: se troviamo una radice in K possiamo concludere che il polinomio non è irriducibile. Se invece scopriamo che non ha radici in K non siamo arrivati a nulla, perché NON POSSIAMO, IN GENERALE, concludere che $f(x)$ è irriducibile.

Vale però la pena fare una considerazione a parte se il polinomio $f(x)$ ha grado 2 o 3. In tal caso infatti $f(x)$ è irriducibile se e solo se non ha radici in K. Perché ?

Sappiamo che se ha una radice non è irriducibile. Viceversa, se non è irriducibile allora si spezza come

$$f(x) = a(x)b(x)$$

dove o $a(x)$ o $b(x)$ ha grado 1. Dunque per esempio a meno di costanti si potrà scrivere $a(x) = x - \beta$. Allora $f(x)$ ha una radice in K (proprio β).

- **I numeri complessi.**

Definizione $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$, e inoltre si hanno due operazioni di somma e di prodotto, $\cdot, +$ definite come:
$(a + bi) + (c + di) = a + c + (b + d)i$,
$(a + bi)(c + di) = ac - bd + (ad + bc)i$.

Teorema Con gli elementi $1 = 1 + 0i$ e $0 = 0 + 0i$ si ha che $(\mathbb{C}, +, \cdot, 0, 1)$ è un campo
Dimostrazione La dimostrazione è lasciata come esercizio (l'esistenza dell'inverso moltiplicativo la abbiamo verificata in classe, e la trovate anche nell'esempio alla fine). □
I numeri complessi si possono rappresentare come punti del piano $\mathbb{R}^2$, mandando il numero $a + bi$ nel punto (a, b).
Definizione Dato $a + bi \in \mathbb{C}$, definiamo la sua *norma* come $|a + bi| = \sqrt{a^2 + b^2}$, e il suo *coniugato* come $\overline{a + bi} = a - bi$.
Proposizione Per ogni numero complesso z si ha che $|z|^2 = z\bar{z}$, e inoltre $\left|\frac{z}{|z|}\right| = 1$.
Dimostrazione La dimostrazione è lasciata come esercizio. □
Definizione Dato un numero complesso z di norma uguale a 1, l'angolo corrispondente al punto sulla circonferenza unitaria associato a z in $\mathbb{R}^2$ si chiama *argomento* di z, ed è definito a meno di aggiungere multipli di 2π. L'argomento è definito anche come quell'angolo per il quale vale (per z di norma unitaria)

$$z = cos(arg(z)) + isin(arg(z))$$

Se z è un numero complesso qualsiasi diverso da 0, definiamo $arg(z)$ come $arg(z) = arg\left(\frac{z}{|z|}\right)$.

Proposizione Dati due numeri complessi z, w diversi da 0, si ha che

$$|zw| = |z||w|,\ arg(zw) = arg(z) + arg(w)$$

Dimostrazione Se $s = arg(z)$ e $t = arg(w)$, possiamo scrivere

$$z = |z|(cos(s) + isin(s)),\quad w = |w|(cos(t) + isin(t))$$

Si ha che

$$zw = |z||w|(cos(s) + isin(s))(cos(t) + isin(t)) =$$
$$|z||w|\left((cos(s)cos(t) - sin(s)sin(t)) + (cos(s)sin(t) + sin(s)cos(t))i\right)$$

Non dimostriamo il fatto (standard) che per ogni s, t vale

$$cos(s)cos(t) - sin(s)sin(t) = cos(s + t),\quad cos(s)sin(t) + sin(s)cos(t) = sin(s + t)$$

da cui seguono immediatamente le uguaglianze cercate (esercizio). □

La proposizione precedente permette di rappresentare graficamente il prodotto di numeri complessi: dati due numeri, il loro prodotto si ottene ruotando di un angolo pari alla somma degli angoli relativi ai due numeri iniziali, e allontanandosi dall'origine di una lunghezza pari al prodotto delle lunghezze relative ai due numeri iniziali. Questo permette facilmente di dimostrare che ogni numero complesso diverso da 0 ha un inverso rispetto alla moltiplicazione. Il seguente esempio dimostra lo stesso fatto in un altro modo, ossia risolvendo un sistema lineare.

Esempio Dato un numero complesso $z = a + bi$ diverso da zero, il numero complesso $z^{-1} = x + iy$ può essere trovato risolvendo il problema

$$(a + bi)(x + iy) = 1$$

Questo implica le condizioni $ax - by = 1$ e $ay + bx = 0$. Queste due condizioni determinano un sistema

$$\begin{cases} ax - by = 1 \\ bx + ay = 0 \end{cases}$$

Se $a \neq 0$, dalla prima equazione ricaviamo $x = \frac{1}{a}(1 + by)$, e andando a sostituire nella seconda equazione $\frac{b}{a}(1 + by) + ay = 0$, da cui $y = -(a + \frac{b^2}{a})^{-1}\frac{b}{a}$ e sostituendo nella equazione per x si ottiene anche il valore di x. Se invece $a = 0$, allora deve essere $x = 0$ e $y = -\frac{1}{b}$.

- **I polinomi irriducibili in $\mathbb{R}[x]$.**

Abbiamo osservato, come conseguenza del teorema fondamentale dell'algebra, che i polinomi irriducibili in $\mathbb{C}[x]$ sono tutti e soli i polinomi di grado 1. Per quello che riguarda l'anello $\mathbb{R}[x]$, invece, la situazione viene descritta dal seguente:

Teorema I polinomi irriducibili in $\mathbb{R}[x]$ sono:

– i polinomi di grado 1,

– i polinomi di grado 2, ossia della forma $ax^2 + bx + c$, con $a \neq 0$, che hanno il discriminante < 0: $\Delta = b^2 - 4ac < 0$.

Dimostrazione Si verifica subito che i polinomi indicati sono irriducibili: per quelli di grado 1 è ovvio, per quelli di grado 2 si osserva che, poiché hanno il $\Delta < 0$, quando li vediamo come polinomi in $\mathbb{C}[x]$ hanno due radici complesse distinte e non reali. Se avessero anche una radice reale non complessa, allora sarebbero polinomi di grado 2 con almeno tre radici, assurdo.... Dunque sono polinomi di grado due senza radici in $\mathbb{R}$, e possiamo concludere (vedi paragrafo 'polinomi irriducibili e radici") che sono irriducibili in $\mathbb{R}[x]$.

Ora dobbiamo dimostrare che non ci sono altri polinomi irriducibili in $\mathbb{R}[x]$. Supponiamo di incontrare un polinomio $f(x)$ che sostiene di essere irriducibile e di non essere della forma indicata nell'enunciato del teorema. Dimostreremo che si tratta di un IMPOSTORE.

Per prima cosa $f(x)$ deve avere grado > 1, (le costanti non sono irriducibili e se avesse grado 1 allora sarebbe uno dei polinomi dell'enunciato).

Inoltre $f(x)$ non deve avere radici in $\mathbb{R}$, altrimenti non sarebbe irriducibile. Come sappiamo, però, per il teorema fondamentale dell'algebra, $f(x)$ ha certamente una radice complessa (non reale) α. Scriviamo $\alpha = a+bi$ con $a, b \in \mathbb{R}$ e $b \neq 0$. Costruiamo il polinomio

$$g(x) = (x - \alpha)(x - \overline{\alpha}) = (x - (a + bi))(x - (a - bi))$$

Questo polinomio risulta essere a coefficienti reali, ossia appartiene a $\mathbb{R}[x]$; infatti sviluppando il prodotto otteniamo:

$$g(x) = x^2 - 2ax + a^2 + b^2$$

Allora possiamo fare la divisione euclidea in $\mathbb{R}[x]$ fra $f(x)$ e $g(x)$:

$$f(x) = g(x)q(x) + r(x)$$

Mostriamo che il resto $r(x)$ deve essere 0. Infatti valutando in α otteniamo:

$$0 = f(\alpha) = 0 \; q(\alpha) + r(\alpha)$$

da cui si ricava che $r(\alpha) = 0$. Ma $r(x)$ è un polinomio del tipo $r(x) = cx + d$ con $c, d \in \mathbb{R}$ e allora possiamo scrivere $c\alpha + d = 0$. Si nota subito che se fosse $c \neq 0$ troveremmo $\alpha = -\frac{d}{c}$ che non può valere visto che α risulterebbe uguale a un numero reale (mentre sappiamo che è un complesso non reale). Dunque deve essere $c = 0$, allora la nostra equazione si riduce a $d = 0$; insomma, $r(x) = 0$ come volevamo.

Abbiamo quindi dimostrato che $g(x) \mid f(x)$ ovvero

$$f(x) = g(x)q(x)$$

Ma $f(x)$ sostiene di essere irriducibile, e questo è uno spezzamento in due fattori! Dunque uno dei fattori deve essere una costante, e sarà $q(x)$ (non certo $g(x)$, che ha grado due). Allora poniamo $q(x) = k$ con k un numero reale (che deve essere diverso da zero, altrimenti $f(x) = 0$ e $f(x)$ non sarebbe irriducibile):

$$f(x) = kg(x)$$

Quindi $f(x)$ ha grado due. Però sostiene di non essere uno dei polinomi dell'enunciato. Allora deve avere $\Delta \geq 0$, ossia deve avere almeno una radice in $\mathbb{R}$. Ma abbiamo già osservato che non può avere radici in $\mathbb{R}$ sempre perchè afferma di essere irriducibile.... Dunque lo abbiamo smascherato: $f(x)$ è davvero un impostore, non ci ha detto la verità perché un polinomio con le caratteristiche che lui sosteneva di avere non può esistere! □

Osservazione: avrete notato che il tono scherzoso della dimostrazione appena svolta è solo un camuffamento di una dimostrazione per assurdo..Per una dimostrazione lievemente diversa vedere la sezione degli esercizi.

- **I polinomi irriducibili in $\mathbb{Q}[x]$.**

Per prima cosa ricordiamo l'enunciato del Lemma di Gauss (non lo abbiamo dimostrato, chi vuole può guardare la dimostrazione sul Childs):

Lemma Sia $f(x) \in \mathbb{Z}[x]$. Se $f(x) = a(x)b(x)$ in $\mathbb{Q}[x]$ allora possiamo trovare due polinomi $a_1(x) \in \mathbb{Z}[x]$, associato a $a(x)$, e $b_1 \in \mathbb{Z}[x]$, associato a $b(x)$, tali che

$$f(x) = a_1(x)b_1(x)$$

Vediamo a cosa serve questo lemma. Prendiamo un polinomio $g(x)$ in $\mathbb{Q}[x]$ e cerchiamo di scoprire se è irriducibile in $\mathbb{Q}[x]$ o no. Intanto notiamo che questo problema è equivalente al problema di controllare se è irriducibile in $\mathbb{Q}[x]$ il polinomio $G(x) \in \mathbb{Z}[x]$ ottenuto moltiplicando $g(x)$ per il minimo comune multiplo dei denominatori dei suoi coefficienti (facile esercizio...). Ora, se $G(x)$ fosse riducibile avremmo $G(x) = h(x)t(x)$ con $h(x), t(x)$ polinomi in $\mathbb{Q}[x]$ di grado ≥ 1. Il Lemma di Gauss a questo punto ci garantisce che vale anche

$$G(x) = h_1(x)t_1(x)$$

con $h_1(x) \in \mathbb{Z}[x]$ e $t_1(x) \in \mathbb{Z}[x]$ che differiscono da $h(x)$ e $t(x)$ solo per la moltiplicazione per una costante.

Dunque, come conseguenza del Lemma di Gauss, possiamo concludere che scoprire se $g(x)$ è irriducibile in $\mathbb{Q}[x]$ o no è un problema equivalente a scoprire se $G(x)$ è irriducibile in $\mathbb{Z}[x]$ o no.

Ecco perché spesso studieremo dei polinomi a coefficienti interi: si tratta di una limitazione solo apparente del nostro campo d'azione, in realtà studiando la riducibilità dei polinomi a coefficienti interi abbiamo tutte le informazioni che ci servono per conoscere la riducibilità dei polinomi in $\mathbb{Q}[x]$. A questo riguardo, un'arma importante a nostro favore è il seguente:

Teorema ("Criterio di Eisenstein"). Sia

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \ \in \mathbb{Z}[x]$$

Se esiste un numero primo p tale che p NON divide a_n, ma $p \mid a_{n-1}$,$p \mid a_{n-2}$, ...,$p \mid a_1$, $p \mid a_0$ e inoltre p^2 NON divide a_0, allora $f(x)$ è irriducibile in $\mathbb{Z}[x]$ (e dunque in $\mathbb{Q}[x]$).

La dimostrazione non fa parte del programma (siete comunque invitati a guardarla sul Childs).

Grazie a questo criterio, possiamo facilmente costruire polinomi irriducibili in $\mathbb{Q}[x]$ di qualsiasi grado. Per esempio, se vogliamo un polinomio irriducibile di grado 1117, basterà considerare

$$x^{1117} - 2$$

Infatti il criterio di Eisenstein, applicato facendo riferimento al numero primo 2, ci garantisce che tale polinomio è irriducibile in $\mathbb{Q}[x]$. Oppure avremmo potuto prendere

$$8x^{1117} - 12x^{501} - 9x^4 - 27x^3 - 15x - 33$$

e ancora il criterio di Eisenstein (applicato con quale primo ?) ci garantisce che questo polinomio è irriducibile in $\mathbb{Q}[x]$.

- **Come costruire nuovi anelli e campi.**

Ripassiamo le congruenze fra numeri interi:

$$a \equiv b \quad (m)$$

significa che $m \mid a - b$ oppure, equivalentemente, che il resto della divisione euclidea di a per m è uguale al resto della divisione euclidea di b per m.

Questa definizione si basa dunque sulla divisione euclidea. Ma, come abbiamo visto, abbiamo una divisione euclidea anche in $K[x]$ (dove K è un campo).

Allora, dato in $K[x]$ un polinomio $m(x)$ diverso da 0, possiamo definire cosa vuol dire che due polinomi $a(x)$ e $b(x)$ sono congrui fra di loro modulo $m(x)$:

$$a(x) \equiv b(x) \quad (m(x))$$

significa che $m(x) \mid a(x) - b(x)$ oppure, equivalentemente, che il resto della divisione euclidea di $a(x)$ per $m(x)$ è uguale al resto della divisione euclidea di $b(x)$ per $m(x)$.

Continuiamo a osservare le analogie con il caso dei numeri interi. La congruenza lineare

$$ax \equiv b \quad (m)$$

ha soluzione se e solo se $MCD\ (a, m) \mid b$. Questo si otteneva utilizzando il lemma di Bezout.

Ma noi conosciamo una versione del lemma di Bezout per polinomi. Applicandolo, troviamo che, dati i polinomi $a(x)$, $b(x)$, $m(x)$, l'equazione

$$a(x)f(x) \equiv b(x) \quad (m(x))$$

ha soluzione se e solo se $MCD\ (a(x), m(x)) \mid b(x)$.

Osservazione. Qui la notazione è un po' imprecisa, perché non esiste un unico $MCD\ (a(x), m(x))$ - tutti i massimi comuni divisori differiscono fra di loro per la moltiplicazione per una costante; ovviamente intendiamo dire che ogni $MCD\ (a(x), m(x))$

divide $b(x)$.

Utilizzando le congruenze fra interi abbiamo introdotto gli anelli Z_m. Gli elementi di Z_m sono le classi $[0], [1], \ldots, [m-1]$ dove per esempio

$$[1] = \{n \in \mathbb{Z} \mid n \equiv 1 \quad (m)\}$$

ossia è l'insieme di tutti i numeri interi che sono congrui a 1 modulo m.

Estendendo un po' la notazione abbiamo deciso di indicare la classe [1] anche per esempio come $[1+m]$ o come $[1+17m]$. Insomma abbiamo convenuto che per indicare una classe non conta quale fra i suoi elementi mettiamo fra parentesi quadre (del resto i numeri interi congrui a 1 modulo m sono la stessa cosa dei numeri interi congrui a $1+m$ - o a $1+17m$ - modulo m).

Con questa notazione, la somma e la moltiplicazione in $\mathbb{Z}_m$ sono definite così:

$$[a] + [b] = [a+b]$$

$$[a][b] = [ab]$$

Si ottiene così un anello commutativo (con unità - che è la classe [1]).

Se poi $m = p$ è un numero primo, allora $\mathbb{Z}_p$ è un campo: infatti se $[a] \neq [0]$ l'equazione

$$[a][x] = [1]$$

ha sempre soluzione (perchè ? Il motivo lo abbiamo detto poche righe sopra...) e dunque ogni elemento diverso da zero è invertibile.

Vorremmo adesso, tenendo presente la costruzione di $\mathbb{Z}_m$, utilizzare le congruenze fra polinomi per costruire dei nuovi anelli e dei nuovi campi.

Prendiamo in $K[x]$ un polinomio $m(x)$, che per semplicità supponiamo di grado ≥ 1 (per il caso degenere in cui $m(x)$ è una costante diversa da zero si veda un esercizio più avanti), e costruiamo un anello che chiameremo $\dfrac{K[x]}{(m(x))}$.

Gli elementi di $\dfrac{K[x]}{(m(x))}$ sono in corrispondenza con i polinomi di $K[x]$ che sono i possibili resti della divisione euclidea per $m(x)$: si tratta dunque delle classi $[g(x)]$, dove $g(x)$ varia fra tutti i polinomi di grado strettamente minore di $m(x)$ e

$$[g(x)] = \{f(x) \in K[x] \mid f(x) \equiv g(x) \quad (m(x))\}$$

ossia è l'insieme di tutti i polinomi che sono congrui a $g(x)$ modulo $m(x)$.

Come nel caso dei numeri interi, posso rappresentare una classe mettendo fra parentesi quadre uno qualunque dei suoi elementi: per esempio se $m(x) = x^3 + 1$, la classe $[x^2]$ la posso rappresentare anche come $[x^2 + 3x(x^3+1)]$.

Analogamente al caso Z_m, la somma e la moltiplicazione in $\dfrac{K[x]}{(m(x))}$ sono definite così:

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

$$[a(x)][b(x)] = [a(x)b(x)]$$

Si verifica facilmente che $\frac{K[x]}{(m(x))}$ è un anello commutativo (con unità - che è [1]).

Se poi $m(x) = p(x)$ è un polinomio irriducibile allora $\frac{K[x]}{(p(x))}$ è un campo: infatti se $[a(x)] \neq [0]$ l'equazione

$$[a(x)][f(x)] = [1]$$

ha sempre soluzione (perchè ? Vedi sopra...) e dunque ogni elemento diverso da zero è invertibile.

Esempio 1. Da questo punto di vista, $\mathbb{C} = \frac{\mathbb{R}[x]}{(x^2+1)}$. Verificate ! Nel costruire i numeri complessi abbiamo "aggiunto" ai numeri reali una radice (che abbiamo chiamato i) di $x^2 + 1$. Questo suggerisce l'idea che quando si costruisce il campo $\frac{K[x]}{(p(x))}$ quello che in realtà stiamo facendo è aggiungere a K una radice del polinomio irriducibile $p(x)$.....come vedremo nel secondo esempio.

Esempio 2. Consideriamo $\mathbb{Q}[x]$ e il polinomio $x^5 - 7x^2 + 14$ (tale polinomio è irriducibile - potete verificarlo con Eisenstein per esempio). Costruiamo ora il campo $\frac{\mathbb{Q}[x]}{(x^5-7x^2+14)}$ e chiamiamolo K. Consideriamo il polinomio $y^5 - 7y^2 + 14$ in $K[y]$. Tale polinomio ha radici in K ? Come sappiamo non ha radici in $\mathbb{Q}$, anzi, è irriducibile in $\mathbb{Q}[x]$.

Ma in K abbiamo l'elemento $[x]$, ossia la classe $[x]$. Proviamo a vedere se è una radice del polinomio $y^5 - 7y^2 + 14$, ossia proviamo a calcolare $[x]^5 - 7[x]^2 + 14$.

Come sappiamo, viste le leggi di addizione e moltiplicazione, questo equivale a $[x^5 - 7x^2 + 14)]$. Ma la classe $[x^5 - 7x^2 + 14]$ è la stessa cosa di $[0]$ in $\frac{\mathbb{Q}[x]}{(x^5-7x^2+14)}$. Infatti il resto della divisione euclidea di $x^5 - 7x^2 + 14$ per $x^5 - 7x^2 + 14$ è 0 !

Dunque la classe $[x]$ è una radice del polinomio $y^5 - 7y^2 + 14$. Possiamo insomma pensare che abbiamo costruito il nuovo campo $\frac{\mathbb{Q}[x]}{(x^5-7x^2+14)}$ "aggiungendo" a $\mathbb{Q}$ una radice del polinomio $x^5 - 7x^2 + 14$.

Esempio 3. Consideriamo il caso in cui $K = \mathbb{Z}_p$, con p numero primo.

Per esempio prendiamo $\mathbb{Z}_7[x]$ e il polinomio x^3+2x+1. Tale polinomio è irriducibile in $\mathbb{Z}_7[x]$ (perchè ? Ha grado 3 e si verifica che non ha radici in $\mathbb{Z}_7$..).

Allora $\frac{\mathbb{Z}_7[x]}{(x^3+2x+1)}$ è un campo. Quanti elementi ha ? Come abbiamo osservato sopra, gli elementi di $\frac{\mathbb{Z}_7[x]}{(x^3+2x+1)}$ sono in corrispondenza biunivoca con i polinomi in $\mathbb{Z}_7[x]$ di grado strettamente minore a 3. Dunque sono tanti quanti i polinomi di grado ≤ 2 a coefficienti in $\mathbb{Z}_7$. Scriviamo un tale polinomio: $ax^2 + bx + c$. Abbiamo 7 scelte per a, 7 per b e 7 per c. Dunque in $\frac{\mathbb{Z}_7[x]}{(x^3+2x+1)}$ ci sono $7^3 = 343$ elementi.

Il nuovo campo che abbiamo costruito è ancora finito. L'importanza di questo esempio nasce dal fatto che tutti i campi finiti si possono ottenere così:

Teorema. Ogni campo finito si può costruire come $\frac{Z_p[x]}{(q(x))}$ *dove* p *è un numero primo e* $q(x)$ *è un polinomio irriducibile in* $Z_p[x]$.

Questo teorema non lo dimostriamo. Sappiamo però subito ricavare dal suo enunciato:

Corollario. Ogni campo finito ha cardinalità uguale alla potenza di un numero primo, ossia del tipo p^n*, dove* p *è un numero primo.*

Per completare le nostre informazioni su questo argomento, manca un ultimo teorema che enunciamo in maniera un po' informale:

Teorema (enunciato informalmente). Viceversa, per ogni potenza di un numero primo p^n*, esiste un campo finito di cardinalità* p^n*, e in un certo senso si può dire che ne esiste uno solo.*

Osserviamo che questo teorema implica un fatto notevole che nel corso non abbiamo dimostrato, ossia che, per ogni numero primo p, in $\mathbb{Z}_p[x]$ ci sono polinomi irriducibili per ogni grado $n \geq 1$ (solo grazie alla loro esistenza, infatti, potrò costruire un campo con p^n elementi). Sotto questo aspetto i campi $\mathbb{Z}_p$ si comportano come $\mathbb{Q}$ e non come $\mathbb{R}$ o $\mathbb{C}$.

Inoltre, un altro fatto notevole si cela sotto quella frase un po' informale ("e in un certo senso si può dire che ne esiste uno solo"): infatti, supponiamo di avere due distinti polinomi $q(x), t(x)$ irriducibili in $Z_p[x]$ e di grado n; allora possiamo costruire due campi con p^n elementi: $\frac{Z_p[x]}{(q(x))}$e $\frac{Z_p[x]}{(t(x))}$. Quella frase ci suggerisce allora che in realtà questi due campi sono due presentazioni diverse di uno stesso oggetto..

Esercizio. Cosa è $\frac{K[x]}{(m(x))}$ nel caso in cui facciamo la stessa costruzione con $m(x)$ uguale ad una costante (diversa da zero) ?

Esercizio. Cosa accade in $\frac{K[x]}{(m(x))}$ nel caso in cui $m(x)$ non sia irriducibile ? Per esempio: è vero che ogni elemento di $\frac{K[x]}{(m(x))}$ è invertibile ? È vero o no che $\frac{K[x]}{(m(x))}$ è un anello privo di divisori dello zero ?

Nota: chi vuole può venire a chiedere bibliografia su questo bellissimo argomento (comunque questi teoremi sono dimostrati anche sul Childs, altrimenti rimando, per una dimostrazione di sapore diverso, al testo di Herstein, Algebra). Chi ha passato bene gli scritti può sostituire l'orale classico facendo una breve presentazione di questi

teoremi.