Appunti di Algebra II

Leonardo Ruzzante

"Per l'algebra, palazzo dai precisi cristalli."
Jorge Luis Borges, Poesia dei doni.

Indice

Note

Questi appunti seguono il programma del corso Algebra 2 tenuto dal professor A. Logar all'università degli studi di Trieste nell'AA 2021/22. Li ho scritti come parte della mia preparazione per l'esame, ma anche come un'attività stimolante che consiglio. Posso dire di averne già tratto beneficio e per questo motivo ho deciso di renderli disponibili gratuitamente a chiunque voglia leggerli. I riferimenti indicati dal professore sono:

1. L. Childs, A concrete introduction to higer algebra (III edizione) Springer, 2009.
2. N. Jacobson, Basic algebra, I Freeman and Company, 1974.
3. I. N. Herstein, Algebra, Editori Riuniti, 1992.
4. J. Rose, A course on Group theory, Cambridge University Press, 1978.
5. I. Stewart, Galois Theory, Champam & Hall, 2004.

Nonostante la mia attenzione nella stesura, ci saranno imprecisioni ed errori, quindi leggete con spirito critico. Questi appunti non sono stati corretti o in generale "sistemati". Sto cercando aiuto per la correzione di questi appunti, così come quelli di Geometria 3A e Geometria 3B. Per segnalare errori o per offrire un aiuto nella correzione scrivete a leonardo.ruzzante@yahoo.it.
Buono studio!

1 Richiami e primi approfondimenti

1.1 Gruppi e omomorfismi

Introduciamo anzitutto le due notazioni classiche per i gruppi:

Notazione additiva: Indichiamo con $(G, +)$ un *gruppo*, con 0 il suo *elemento neutro* e con -a *l'inverso dell'elemento a.* L'elemento $a + a + \cdots + a$ ottenuto applicando l'operazione $+$ *ad a n volte* verrà denotato come $n \cdot a$ o più semplicemente na. Per convenzione si pone inoltre $0 \cdot x = 0x = 0$.
La notazione additiva viene spesso utilizzata se il gruppo trattato risulta essere abeliano.

Notazione moltiplicativa: $(G, \cdot)$ per indicare un *gruppo*, 1 per indicare il suo *elemento neutro*, a^{-1} per indicare *l'inverso di a.*
L'elemento $a \cdot a \cdot \cdots \cdot a$ ottenuto applicando l'operazione $\cdot$ *ad a n volte* verrà denotato come a^n. Per convenzione si pone inoltre $a^0 = 1$. Si può scrivere ab intendendo $a \cdot b$.

Definizione 1.1.1. Sia G un insieme non vuoto; $\cdot : G \times G \to G$ un'operazione associativa, con elemento neutro, e che ammette inversi in G. La struttura $(G, \cdot)$ si dice *gruppo*. Se inoltre $\cdot$ risulta commutativa il gruppo si dice *abeliano*. Un sottoinsieme $S \subset G$ si dice *sottogruppo di* G se è esso stesso un gruppo con $\cdot$.

Osservazione 1.1.1. Se G è un gruppo allora $S \subset G$ è un suo sottogruppo se e solo se $S \neq \emptyset$ e per ogni $a, b \in S$ vale $a \cdot b^{-1} \in S$.

Definizione 1.1.2. Sia $(G, \cdot)$ un gruppo ed H un suo sottogruppo. Per ogni $a \in G$; il corrispondente insieme $aH \equiv \{a \cdot h \mid h \in H\}$ si dice *laterale sinistro di H*. L'elemento $a = a \cdot 1_G \in aH$ si dice *rappresentante canonico della classe aH*. Analogamente si definiscono i *laterali destri* come $Ha \equiv \{h \cdot a \mid h \in H\}$.

Osservazione 1.1.2.

1. Necessitiamo di due notazioni diverse in quanto $\cdot$ potrebbe non essere commutativa. Nel caso che lo sia, ovvero $aH = Ha$, diremo che H è un *sottogruppo normale*.

2. Se G è un gruppo abeliano ogni suo sottogruppo è normale.

3. I laterali, in genere, non sono sottogruppi in quanto non contengono l'elemento neutro di G.

4. $aH = bH$ se e solo se $a^{-1} \cdot b \in H$.

Definizione 1.1.3. Sia G un gruppo e siano H, K due suoi sottogruppi. Se esiste un elemento $g \in G$ tale che $H = \{gkg^{-1},\ k \in K\}$ allora H e K si dicono *sottogruppi coniugati di G*.

Osservazione 1.1.3. Un sottogruppo normale è coniugato soltanto con se stesso.

Definizione 1.1.4. Si dice *ordine di un gruppo A*, e si denota con $|A|$, il numero di elementi di A. Un gruppo si dice *finito* se il suo ordine è tale, altrimenti si dice *infinito*.

Definizione 1.1.5. Sia X un insieme. Si dice *partizione di X* una famiglia di insiemi $\{A_i\}_{i \in I}$ tale che

1. $A_i \neq \emptyset;\ \forall i \in I$

2. $\bigcup_{i \in I} A_i = X$

3. $A_i \bigcap A_j \neq \emptyset \iff A_i = A_j$.

Definizione 1.1.6. Siano X, Y due insiemi. Si dice *relazione su X ed Y* un sottoinsieme $\mathfrak{R} \subset X \times Y$ del loro insieme prodotto. La coppia $(a, b) \in \mathfrak{R} \subset X \times Y$ si denota come $a\mathfrak{R}b$ e si legge *a è in relazione con b.*

Definizione 1.1.7. Una relazione $\sim$ su $X \times X$ si dice *relazione di equivalenza su X* se per ogni $x, y, z \in X$ valgono

1. $x \sim x$

2. $x \sim y \Rightarrow y \sim x$

3. $x \sim y,\ y \sim z \Rightarrow x \sim z$

Se su X è definita un'operazione $*$, $\sim$ si dice *compatibile* con $*$ se per ogni $a, a', b, b' \in X$ vale $(a \sim b \wedge a' \sim b') \Rightarrow a * a' \sim b * b'$.

Osservazione 1.1.4. Sia H un sottogruppo normale di G. Allora H induce una relazione di equivalenza $\sim_H$ su G definita da $a \sim_H b \iff ab^{-1} \in H$.

Definizione 1.1.8. Sia X un insieme e $\sim$ una relazione di equivalenza su X. Si dicono *classi di equivalenza* di X gli insiemi $[a]_\sim = \{x \in X \mid x \sim a\}$. L'elemento a si dice *rappresentante della classe* $[a]_\sim$.
L'insieme $X/_\sim = \{[a]_\sim \mid a \in X\}$, i cui elementi sono le classi di equivalenza di X rispetto a $\sim$, si dice *quoziente di X*, o anche X *quozientato su* $\sim$. Solitamente si scrive $[a]$ al posto di $[a]_\sim$ per alleggerire le notazioni.

Osservazione 1.1.5. Una relazione di equivalenza induce una partizione.

Definizione 1.1.9. Sia $(G, *)$ un gruppo e $\sim$ una relazione di equivalenza **compatibile** su G. Si dice *gruppo quoziente* il gruppo $(G/_{\sim}, *_{\sim})$ dove l'operazione $*_{\sim}$ viene definita da $[a] *_{\sim} [b] = [a * b]$.

Osservazione 1.1.6. Se G è un gruppo e H è un suo sottogruppo normale allora si scrive G/H intendendo $G/_{\sim_H}$. L'elemento neutro del gruppo G/H è $[h]_H$; $h \in H$. G/H può anche essere visto come il gruppo i cui elementi sono i laterali di H in G e con elemento neutro H.

Osservazione 1.1.7. $(\mathbb{Z}, +)$ è un gruppo abeliano e i suoi sottogruppi sono tutti e soli gli insieme della forma $m\mathbb{Z} = \{ma | a \in \mathbb{Z}\}$ con $m \in \mathbb{Z}$ fissato.

Teorema 1.1.1 (di Lagrange)**.** Sia $(G, *)$ un gruppo **finito** e sia H un suo sottogruppo. Allora la cardinalità di H divide la cardinalità di G. Inoltre, se $|G| = n$ e $|H| = m$ il numero naturale $\frac{n}{m}$ corrisponde al numero di laterali di H in G, ovvero: $|G/H| = |G|/|H|$

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

Dimostrazione (abbozzo)
Siano G un gruppo ed H un suo sottogruppo di cardinalità m. Anzitutto si osserva che G/H costituisce una partizione di G (Osservazione 9 ed esercizio E11); successivamente si dimostra che ogni laterale aH ha la stessa cardinalità di H. Segue subito la tesi.

Omomorfismi Vediamo ora velocemente alcune definizioni e risultati relativi agli omomorfismi tra gruppi.

Definizione 1.1.15 Siano $(A, \cdot)$ e $(B, \odot)$ due gruppi. Denotiamo con 1 l'elemento neutro di $\cdot$ in A e con ① il neutro di $\odot$ in B. Una funzione $f : A \to B$ si dice *omomorfismo tra i gruppi A e B se:*

i) $f(1) = ①$

ii) $f(\alpha \cdot \beta) = f(\alpha) \odot f(\beta); \quad \forall \alpha, \beta \in A$

iii) $f(\alpha^{-1}) = f(\alpha)^{(-1)}$. Qui α^{-1} è l'inverso di α rispetto all'operazione $\cdot$ ed appartiene ad A, mentre $f(\alpha)^{(-1)}$ è l'inverso di $f(\alpha)$ rispetto all'operazione $\odot$ e sta in B.

Se f è un omomorfismo:

suriettivo, f si dice anche *epimorfismo*

iniettivo, f si dice anche *monomorfismo*

biiettivo, f si dice anche *isomorfismo.*

Definizione 1.1.16 Sia $f : A \to B$ un omomorfismo di gruppi. Si dice *nucleo di f*, e si denota con *ker f*, la controimmagine dell'elemento neutro di B. In simboli: $ker\ f = \{x \in A \mid f(x) = b\}$ dove b denota il neutro dell'operazione del gruppo B.

E3 *Verificare che ker f è un sottogruppo con l'operazione indotta da A.*

E4 *Verificare che f è un monomorfismo se e solo se ker* $f = \{a\}$ *con a elemento neutro di A.*

Teorema 1.1.17 (I teorema di omomorfismo)

Sia $f\colon A \to B$ un omomorfismo di gruppi; allora f si può fattorizzare come composto di un epimorfismo ed un monomorfismo.

Dimostrazione Data f definiamo la relazione di equivalenza $\sim$ tale che $a \sim b \iff f(a) = f(b)$. Costruiamo il gruppo quoziente $A/\sim$.
Si definisca ora $\pi : A \to A/\sim$ che manda ogni elemento di A nella sua classe di equivalenza rispetto a $\sim$. π è banalmente suriettiva.
Si definisce poi $m : A/\sim \to B$ che manda ogni classe di $A/\sim$ nell'immagine di un suo elemento attraverso f. m è iniettiva. Inoltre abbiamo $f = \pi \circ m$.

Osservazione 1.1.18 Tenendo conto dell'Osservazione 4.iii, della definizione 17 e dell'esercizio E18 si ha che $\sim$ è la relazione indotta dal sottogruppo ker f di A.

Teorema 1.1.19 (II teorema di omomorfismo) Sia $f\colon A \to B$ un omomorfismo di gruppi; allora $A/ker\ f \simeq f(A)$
Dimostrazione Dall'osservazione precedente e recuperando il monomorfismo $m : A/\sim = A/ker\ f \to B$, restringendone il codominio ad f(A)si ottiene che m è un isomorfismo.

Osservazione 1.1.20
i) Risulta equivalente la seguente formulazione: Se $f : A \to B$ è un omomorfismo di gruppi e se $\alpha = \{S | ker\ f \subset S \subset A\}$; $\beta = \{T | T \subset f(G) \subset B\}$ sono gli insiemi i cui elementi sono i sottogruppi contenenti il nucleo di f e i sottogruppi contenuti nell'immagine di G attraverso f, rispettivamente; allora α e β sono in biiezione.

ii) Tutti e soli i sottogruppi normali del quoziente G/H sono della forma K/H. Consideriamo la proiezione canonica $\pi : G \to G/H$ che ad ogni g associa l'elemento $[g]_H$. Per la formulazione al punto i) otteniamo $\{S | H \subset S \subset G\} \simeq$

$\{T|\, T \subset G/H\}$. Prendiamo quindi un generico sottogruppo K di G/H; K è immagine attraverso π di un qualche sottogruppo J del dominio: $\pi^{-1}(K) = J$ ed essendo π suriettiva abbiamo anche $K = \pi(\pi^{-1}(K)) = \pi(J) = J/H$ dove la prima uguaglianza segue da una nota proprietà delle funzioni suriettive mentre la seconda dalla definizione di π.

iii) Se $f : A \to B$ è un monomorfismo allora $A \simeq f(A) \subseteq B$. Infatti f è iniettiva se e solo se il suo nucleo è banale (E19) e per il II teorema di omomorfismo $A/ker\, f = A \simeq f(A) \subseteq B$.

1.1.1 Gruppi ciclici

Definizione 1.1.1.1 Si dice *ordine di un elemento g* il più piccolo numero naturale $n > 0$ per il quale:
i) $g^n = 1$ (se si tratta di un gruppo con notazione moltiplicativa)
ii) $ng = 0$ (se si tratta di un gruppo con notazione addittiva).
Qualora tale n non esistesse diremo che g ha *ordine infinito*.

Definizione 1.1.1.2 Dato un gruppo (G,+) ed un suo elemento x definiamo il *sottogruppo generato da x* come $\langle x \rangle = \{nx \mid n \in \mathbb{Z}\}$.
Se n è un numero negativo, ad esempio -4, con $nx = (-4)x$ si intende l'elemento $(-x) + (-x) + (-x) + (-x)$.
Analogamente, con notazione moltiplicativa: $\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$. Se n è negativo, con x^n si intende l'elemento $(x^{-1})^{-n}$.

Definizione 1.1.1.3 Un gruppo G si dice *gruppo ciclico* se esiste un elemen-

to $a \in G$ tale che $G = \langle a \rangle$.
L'elemento a si dice *generatore di G.*

Osservazione 1.1.1.4

i) L'ordine di $\langle a \rangle$ coincide con l'ordine di a.

ii)Se G è un gruppo finito di ordine n, ogni suo elemento ha per ordine un numero m divisore di n. Si prenda infatti un elemento $g \in G$ e si consideri $\langle g \rangle = \{1, g, g^2, \ldots, g^n\}$. Per la chiusura del gruppo rispetto al prodotto abbiamo che $\langle g \rangle \subseteq G$ e per il teorema di Lagrange tale gruppo ha ordine m divisore di n.

I gruppi ciclici possono essere finiti oppure infiniti, e si ha la seguente caratterizzazione:

Teorema 1.1.1.5 Ogni gruppo ciclico infinito è isomorfo a $\mathbb{Z}$. Ogni gruppo ciclico finito di ordine n è isomorfo a $\mathbb{Z}n$.

Dimostrazione Consideriamo un generico gruppo ciclico $G = \langle g \rangle$ e sia $f : \mathbb{Z} \to G$ una funzione tale che $f(n) = g^n$, si ha che f è un epimorfismo. Inoltre:
i)Il suo nucleo è banale se e solo se g ha ordine infinito. Si ha dunque $\mathbb{Z}/ker\ f = \mathbb{Z}/\{0\} = \mathbb{Z}$. Dal secondo teorema di omomorfismo si ha che $\mathbb{Z}/ker f \simeq G$. Combinando questi due risultati otteniamo $\mathbb{Z} \simeq G$. Si conclude

che ogni gruppo ciclico infinito è isomorfo a $\mathbb{Z}$.

ii)Se g ha ordine n allora $ker\ f \simeq n\mathbb{Z} = \{nh \mid h \in \mathbb{Z}\}$, e ancora per il II teorema di omomorfismo, abbiamo $G \simeq \mathbb{Z}/ker\ f = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}n$. Si conclude che ogni gruppo ciclico di ordine n è isomorfo a $\mathbb{Z}_n$.
Abbiamo così dimostrato il teorema.

Osservazione 1.1.1.6 Ogni gruppo finito di ordine primo p è ciclico, e per il teorema precedente è isomorfo a $\mathbb{Z}_p$. Infatti se G è un gruppo e $|G| = p$ allora esiste un elemento $g \neq 1 \in G$. Considerando il sottogruppo $H = \langle g \rangle$ per il Teorema di Lagrange abbiamo che $|H| \,|\, |G|$ ovvero $|\langle g \rangle| \,|\, p$ ma questo può avvenire se e solo se H ha ordine p. Per il teorema precedente abbiamo poi che $G = H = \langle g \rangle \simeq \mathbb{Z}_p$.

Si tornerà in seguito sui gruppi ciclici, enunciando altre proprietà alla luce della teoria sviluppata.

1.2 Anelli, domini d'integrità e campi

Definizione 1.2.1 Siano: A un insieme non vuoto.
$+ : A \times A \to A$ un'operazione associativa, commutativa, con elemento neutro 0 e che ammette inversi in A.
$\cdot : A \times A \to A$ un'operazione associativa.
Se inoltre le due operazioni sono legate dalle proprietà distributive:
i) $a \cdot (b + c) = a \cdot b + a \cdot c$
ii) $(a + b) \cdot c = a \cdot c + b \cdot c$

la struttura $(A, +, \cdot)$ si dice *anello.*

Se esiste 1 elemento neutro di $\cdot$ l'anello si dice *unitario.*

Se $\cdot$ risulta commutativo l'anello si dice *commutativo.*

D'ora in avanti si tratterà solamente di anelli unitari e commutativi.

Osservazione 1.2.2 Risulta equivalente dire che:

i)(A,+) è un gruppo abeliano

ii)$(A \setminus \{0\}, \cdot)$ è un semigruppo associativo.

Definizione 1.2.3 Un sottoinsieme S di A si dice *sottoanello* se $(S, +, \cdot)$ è a sua volta un anello.

Definizione 1.2.4 Un sottoinsieme $I \subset A$ si dice *ideale sinistro di A* se:

i) I è un sottogruppo di $(A, +)$

ii_s) $\forall x \in I, \forall a \in A$ si ha che $x \cdot a \in I$.

Analogamente si definisce un *ideale destro* sostituendo ii_s con:

ii_d) $\forall x \in I, \forall a \in A$ si ha che $a \cdot x \in I$.

La proprietà ii_s e ii_d si dicono *proprietà di assorbimento.*

Definizione 1.2.5 Quando varranno contemporaneamente ii_s) e ii_d) parleremo di *ideale bilaterale* o più semplicemente di *ideale.*

Osservazione 1.2.6 Un qualsiasi ideale di un anello commutativo è bilaterale.

Definizione 1.2.7 Dato un anello $(A, +, \cdot)$ ed una relazione di equivalenza $\sim$ compatibile con le due operazioni si può definire l'*anello quoziente* come

l'insieme $A/\sim = \{[a]_\sim \mid a \in A\}$ con le operazioni:

i) $+_\sim$ tale che $[a] +_\sim [b] = [a+b]$

ii)$\cdot_\sim$ tale che $[a] \cdot_\sim [b] = [a \cdot b]$

Le operazioni dovranno essere legate dalla proprietà distributiva:

$[a] \cdot_\sim ([b] +_\sim [c]) = [a \cdot b + a \cdot c]$.

Dato I ideale di A si può costruire l'anello quoziente A/I.

Definizione 1.2.8 Un anello $(A, +, \cdot)$ unitario e commutativo si dice *dominio di integrità* se $\forall x, y \in A$ si ha che $x \cdot y = 0 \Rightarrow x = 0 \vee y = 0$

Comunemente si dice che A *non ha divisori dello zero.*

Osservazione 1.2.9 In un dominio d'integrità vale la legge di cancellazione: $a \cdot b = a \cdot c \Rightarrow b = c$. Infatti siano $a, b, c \in A$ tali che $a \neq 0$ e $ab = ac$, segue che $ab - ac = a(b-c) = 0$ e dalla definizione *(b-c)=0; ovvero b=c.*

Definizione 1.2.10 Un anello $(A, +, \cdot)$ unitario, commutativo e che ammette inversi rispetto a $\cdot$ in $A \setminus \{0\}$ si dice *campo.*

E37 *Dimostrare che un campo è sempre un dominio di integrità.*

Teorema 1.2.11 Se $(A, +, \cdot)$ è un campo i suoi unici ideali sono l'insieme $\{0\}$ e l'intero anello A.

Dimostrazione Sia $I \subset A$ un ideale. Nel caso in cui $I = \{0\}$ abbiamo la prima parte della tesi. Altrimenti prendiamo $a \in I$; $a \neq 0$. Essendo A un campo $\exists a^{-1} \in A$ inverso di a. Per la legge di assorbimento $a \cdot a^{-1} = 1 \in I$. Applicando nuovamente la legge di assorbimento otteniamo $\forall x \in A$, $1 \cdot x = x \in I$. Segue che I=A.

(E) *Dimostrare che vale il viceversa.*

Definizione 1.2.12 Siano $(A, +, \cdot)$ e $(B, \oplus, \odot)$ due anelli. Una funzione $f : A \to B$ si dice *omomorfismo di anelli* se:
i) $f(a + b) = f(a) \oplus f(b)$
ii) $f(a \cdot b) = f(a) \odot f(b)$.

I teoremi di omomorfismo si estendono al caso degli anelli osservando che, dato un omomorfismo $f : A \to B$, $ker\, f$ è un ideale di A.

Definizione 1.2.13 Dato un anello $(A, +, \cdot)$ ed un suo sottoinsieme $X \in A$ si definisce l'*ideale generato da X* come il più piccolo ideale di A (in senso insiemistico) che contiene X. Per indicare questo ideale scriveremo (X).

Osservazione 1.2.14 Sia $J_X = \{I \mid X \subset I,\, I\, ideale\}$ l'insieme i cui elementi sono tutti e soli gli ideali contenenti X. L'ideale $\overline{I} = \bigcap_{I \in J_x} I$ coincide con l'ideale (X).
Infatti esiste quantomeno l'ideale banale $A \supseteq X$ e ciò implica che $J_X \neq \emptyset$.
Vogliamo ora verificare che $\overline{I}$ sia effettivamente un ideale:
Presi due elementi $a, b \in \overline{I}$ abbiamo che, per ogni ideale $I \in J_X$,
$a, b \in I$. Essendo I ideali essi sono in particolare sottogruppi con la somma, e quindi $a - b \in I$, ciò implica che $a - b \in \overline{I}$ e ricordando l'esercizio E1, questo ci garantisce che $\overline{I}$ è un sottogruppo di A con la somma.
La proprietà di assorbimento si verifica in modo analogo. Dunque l'intersezione di ideali è a sua volta un ideale. Rimane ora da verificare che $\overline{I}$ è il più piccolo ideale contenente X. Per fare ciò supponiamo che esista un ideale $\widehat{I}$ tale che $X \subseteq \widehat{I} \subseteq \overline{I}$, ma ciò significa che $\widehat{I} \in J_X$, e dalla definizione di $\overline{I}$ otteniamo $\overline{I} \subseteq \widehat{I}$ e quindi $\overline{I} = \widehat{I}$.

Osservazione 1.2.15 (X) si può esprimere anche attraverso la formula:
$(X) = \{\sum_{i=1}^{n} a_i \cdot x_i \mid a_i \in A, x_i \in X, n \in \mathbb{N}\}$.
Se $X = \{x_1, x_2, \ldots, x_k\}$ allora $(X) = \{\sum_{i=1}^{k} a_i \cdot x_i \mid a_i \in A\}$.

Definizione 1.2.16

i) L'ideale generato da un insieme composto da un solo elemento si dice *ideale principale.* Si scriverà *(x)* intendendo $(\{x\})$.

ii) Un ideale $I \subseteq A$ si dice *massimale* se esso è il più grande ideale (in senso insiemistico) di A. Ovvero se esiste un ideale J tale che $I \subseteq J \Rightarrow J = I \vee J = A$.

iii) Un ideale $I \subseteq A$ si dice *primo* se $\forall a, b \in A$ si ha $ab \in I \Rightarrow a \in I \vee b \in I$.

Definizione 1.2.17 Un dominio d'integrità si dice *dominio ad ideali principali* (in breve PID) se ogni suo ideale è principale.

Osservazione 1.2.18

i) Gli ideali banali $\{0\}$ ed A si possono scrivere come *(0)* e *(1)* rispettivamente.

ii) $(\mathbb{Z}, +, \cdot)$ è un dominio d'integrità e i suoi ideali sono tutti e soli i sottoanelli della forma $(m) = m\mathbb{Z} = \{ma | a \in \mathbb{Z}\}$ con $m \in \mathbb{Z}$ fissato, cioè $\mathbb{Z}$ è un PID.

Osservazione 1.2.19 Se A è un anello ed $I \subseteq A$ è un suo ideale allora:

i) I è ideale primo $\iff$ A/I è domnio d'integrità

ii) I è ideale massimale $\iff$ A/I è un campo.

Definizione 1.2.20 Sia $(A, +, \cdot)$ un anello. Un elemento $a \in A$ si dice *unitario o invertibile* se esiste a^{-1} inverso per $\cdot$.

COSTRUZIONE CAPO DEI QUOZIENTI

2 Domini d'integrità e l'anello degli interi

2.1 MCD e divisione euclidea

Definizione 2.1.1 Sia $(A, +, \cdot)$ un dominio d'integrità. Un elemento non unitario $a \in A$; $a \neq 0$ si dice:
i) *irriducibile* se $a = f \cdot g \Rightarrow f$ *unitario oppure* g *unitario.*
ii)*primo* se $[a|f \cdot g] \Rightarrow a|f$ oppure $a|g$.

Osservazione 2.1.2 Se a è primo allora a è irriducibile.
Infatti sia a primo. Supponiamo sia $a = fg$, $a|fg$ banalmente. Per ipotesi a divide f o g. Supponiamo divida f. Allora $\exists m \in A$ tale che $f = am$, sfruttando questa espressione troviamo che $a = (am)g = a(mg)$. Per l'osservazione 35 si ottiene $1 = mg$, per cui m è l'inverso di g e dunque g è unitario.

Definizione 2.1.3 Sia A un dominio d'integrità. Presi due elementi $a, b \in A$ si dice *massimo comun divisore* di a e b un elemento $d \in A$ tale che $d|a$ e $d|b$ ed inoltre $\forall \delta$ con la stessa proprietà si ha che $\delta|d$. In simboli si scriverà $MCD(a, b) = d$.

Definizione 2.1.4 Sia A un dominio d'integrità. Due elementi $a, b \in A$ si dicono *associati* se esiste un elemento unitario $u \in A$ tale che $a = ub$.
Osservazione 2.1.5 In $\mathbb{Z}$ gli unici elementi unitari sono 1 e -1, dunque tutte e sole le coppie di elementi associati in $\mathbb{Z}$ sono della forma a, -a.

Osservazione 2.1.6 Il massimo comun divisore di due numeri è unico a

meno di elementi associati. Infatti siano $a, b \in A$ e sia $MCD(a,b) = d = \delta$. Abbiamo per definizione che $d|\delta$ e anche $\delta|d$. Esistono allora due elementi a, α tali che $d = \alpha\delta$ e $\delta = ad$. Combinando le due identità otteniamo $d = \alpha ad$, ed essendo in un dominio d'integrità vale la cancellazione: $1 = \alpha a$. Dunque a, α sono elementi unitari, ricordando che $d = \alpha\delta$ e $\delta = ad$ si ha che $d \ e \ \delta$ sono per definizione associati.

Teorema 2.1.7 (Divisione euclidea) Siano $a, b \in \mathbb{Z}$; $b \neq 0$, allora esistono $q, r \in \mathbb{Z}$ con $0 \leq r < |b|$ tali che $a = qb + r$. Inoltre q, r sono unici.

Dimostrazione (abbozzo) Sia $S = \{a - nb \mid n \in \mathbb{Z},\ a - nb \geq 0\}$.
Abbiamo $S \neq \emptyset$. Definiamo $r = \min S$. r così definito soddisfa la prima parte della tesi. Inoltre se q è tale che $(a - qb) = r$ otteniamo $a = qb + r$. Per dimostrare l'unicità supponiamo che esista una seconda espressione $a = \overline{q}b + \overline{r}$. Avremmo che $[qb + r = \overline{q}b + \overline{r}] \Rightarrow |b||q - \overline{q}| = |r - \overline{r}|$. Ricordando che per ipotesi $r, \overline{r} < |b|$ otteniamo la maggiorazione:
$|b||q - \overline{q}| < |b|$ che implica, sfruttando la cancellazione in $\mathbb{N}$ (la quale è ereditata da $\mathbb{Z}$), $|q - \overline{q}| < 1$. Essendo $|q - \overline{q}| \in \mathbb{N}$ si conclude che $|q - \overline{q}| = 0$. Ritornando ora all'equazione $|b||(q - \overline{q})| = |r - \overline{r}|$ concludiamo che pure $|r - \overline{r}| = 0$.

Osservazione 2.1.8 Dati due numeri $a, b \in \mathbb{Z}$, l'insieme $D = \{d : d|a \ e \ d|b\}$ dei divisori di (a,b) è uguale all'insieme $\Delta = \{\delta : \delta|(a - b) \ e \ \delta|b\}$ dei divisori di (a-b,b).
Infatti preso un divisore $d \in D$ si ha: $a = t_1 d$, $b = t_2 d$.
Allora $a - b = t_1 d - t_2 d = (t_1 - t_2)d$, cioè d divide a-b.
Viceversa preso un divisore $\delta \in \Delta$, si ha $a - b = \tau_1\delta$, $b = \tau_2\delta$. Allora

$a = a - b + b = \tau_1\delta + \tau_2\delta = (\tau_1 - \tau_2)\delta$, cioè δ divide a.

In particolare $MCD(a,b) = maxD = max\Delta$. E dunque $MCD(a,b) = MCD(a-b,b)$. Per di più, ponendo $a = q_0b+r_0$, e applicando ripetutamente questo risultato otteniamo:
$MCD(a,b) = MCD(a-b,b) = MCD(a-2b,b) = \cdots = MCD(a-q_0b,b)$.
Dunque $MCD(a,b) = MCD(r_0,b)$ dove r_0 è il resto della divisione euclidea e si ha $0 \leq r_0 < |b|$.

Teorema 2.1.9 (Algoritmo di Euclide) Per ogni coppia di elementi $a, b \in \mathbb{Z}$ esiste il loro massimo comun divisore.
Dimostrazione Dati $a, b \in \mathbb{Z}$, dal Teorema 52 possiamo scrivere $a = q_0b + r_0$ mentre dall'Osservazione 53 abbiamo che $MCD(a,b) = MCD(a-b,b) = MCD(a-2b,b) = \cdots = MCD(a-q_0b,b)$. Dunque $MCD(a,b) = MCD(r_0,b)$ dove r_0 è il resto della divisione euclidea e si ha $0 \leq r_0 < |b|$.
Possiamo ora ripetere il procedimento in questo modo: avremo $b = q_1r_0 + r_1$ e $MCD(r_0,b) = MCD(r_0,b-r_0) = MCD(r_0,b-2r_0) = \cdots = MCD(r_0,b-q_1r_0) = MCD(r_0,r_1)$ con $0 \leq r_1 < r_0$. In generale troveremo che $MCD(a,b) = MCD(r_i,r_{i+1})$. Trovandoci in $\mathbb{Z}$ e osservando che la successione $\{r_i\}_i$ è strettamente decrescente e limitata inferiormente da 0 avremo che dopo un numero finito di passaggi si otterrà $MCD(a,b) = MCD(r_j,0) = r_j$.

Quella appena vista è una dimostrazione costruttiva, a titolo di esempio si mostra una applicazione di questo algoritmo per la ricerca di MCD(54,16):

i)$54 = 3 \cdot 16 + 6 \rightarrow MCD(54,16) = MCD(6,16)$,
ii)$16 = 2 \cdot 6 + 4 \rightarrow MCD(6,16) = MCD(6,4)$,

iii)$6 = 1 \cdot 4 + 2 \rightarrow MCD(6,4) = MCD(4,2)$,

iv)$4 = 2 \cdot 2 + 0 \rightarrow MCD(4,2) = MCD(2,0) = 2 = MCD(54,16)$.

Definizione 2.1.10 Due elementi $a, b \in \mathbb{Z}$ si dicono *coprimi* se non hanno fattori comuni, ovvero se $MCD(a,b) = 1$.

Teorema 2.1.11 (Identità di Bezout) Siano $a, b \in \mathbb{Z}$ e sia $d = MCD(a,b)$. Allora esistono $\alpha, \beta \in \mathbb{Z}$ tali che $d = \alpha a + \beta b$.

Guida per la dimostrazione Ripercorriamo all'indietro l'algoritmo di Euclide. Ad ogni passaggio possiamo scrivere il resto i-esimo in funzione dei resti precedentemente comparsi, risalendo fino all'inizio dell'algoritmo abbiamo un'espressione in cui compaiono i due numeri di partenza, manipolando quell'identità otteniamo quella di Bezout.

Forti di queste ultime nozioni riprendiamo l'Osservazione 47 e dimostriamo che nell'anello degli interi vale anche il viceversa:

Teorema 2.1.12 Se $p \in \mathbb{Z}$ è un elemento irriducibile, allora p è primo.

Dimostrazione Sia p irriducibile. Vogliamo vedere che se p divide un prodotto ab allora divide uno dei fattori. A tal fine consideriamo $d = MCD(a,p)$, il quale esiste per il Teorema 54. Per l'identità di Bezout si ha inoltre che $\exists \alpha, \beta \in \mathbb{Z}$ per i quali $d = \alpha a + \beta p$. Per costruzione si ha anche che $d|p$ e ciò implica che $\exists u \ : p = du$. Essendo p irriducibile si ottiene che d è unitario oppure u è unitario. Consideriamo i due casi.

i) Se d è unitario consideriamo l'identità $d = \alpha a + \beta p$ e moltiplicando ambo i membri per d^{-1} otteniamo: $1 = (\alpha a + \beta p)d^{-1} = d^{-1}\alpha a + d^{-1}\beta p$.
Moltiplichiamo ora ambo i membri per b: $b = d^{-1}\alpha \boldsymbol{ab} + d^{-1}\beta \boldsymbol{p}b$. Osserviamo che grazie ai due fattori in grassetto entrambi gli addendi sono divisibili per p e dunque l'intera espressione è divisibile per p. Dunque $p|b$.
ii)Se u è unitario consideriamo la fattorizzazione $p = du$ e moltiplicando ambo i membri per u^{-1} otteniamo: $d = pu^{-1}$. Per costruzione d divide a, e quindi $pu^{-1}|a$ ovvero $\exists c\, a = pu^{-1}c$ ed in particolare $p|a$. Dunque in entrambe i), ii) si conclude che p è un elemento primo.

2.2 Gli anelli $\mathbb{Z}_m$, teoremi di Eulero e Fermat

Proseguiamo ora con delle strutture già accennate nelle pagine precedenti e che ora studieremo più approfonditamente.

Costruzione degli anelli $\mathbb{Z}_m$ Per ogni $m > 1$ consideriamo la relazione d'equivalenza compatibile ρ_m sull'anello $\mathbb{Z}$ per la quale, se $a = qm + r$; $b = q'm + r'$, $a\rho_m b \iff r = r'$. Ovvero i numeri interi a,b sono in relazione se e solo se hanno lo stesso resto nella divisione per m. L'anello quoziente $\mathbb{Z}/\rho_m$ è rappresentato dal simbolo $\mathbb{Z}_m$ e i suoi elementi sono le classi $[0]_{\rho_m}, [1]_{\rho_m}, \ldots, [m-1]_{\rho_m}$.

Osservazione 2.2.1

i) $[0]_{\rho_m}$ è un sottogruppo normale con la somma.
ii) Le classi $[1]_{\rho_m}, \ldots, [m-1]_{\rho_m}$ sono laterali di $[0]_{\rho_m}$
iii) $a\rho_m b \iff (a-b)|m$. (Osservazione 4.iii)

iv) $m\mathbb{Z} = \{x \,:\, x \in [0]_{\rho_m}\}$ (Si riveda il Teorema 26).

Definizione 59 Fissato un numero m definiamo $U_m = \{[a]_{\rho_m} \in \mathbb{Z}_m \,:\, \exists([a]_{\rho_m})^{-1}\}$ come l'insieme degli elementi di $\mathbb{Z}_m$ invertibili rispetto al prodotto.

Osservazione 60

i) Un elemento $[a]_{\rho_m} \in \mathbb{Z}_m$ appartiene ad $U_m \iff MCD(a, m) = 1$, ovvero se e solo se *a,m* sono coprimi.

ii)U_m è un gruppo rispetto al prodotto di $\mathbb{Z}_m$.

Più in generale: Se $(A, +, \cdot)$ è un anello, l'insieme U dei suoi elementi invertibili rispetto al prodotto è un gruppo con tale operazione.

SISTEMARE, aggiungere sezione su congruenze e moduli Definizioni; Z/mZ==Zm, congruenze classi, congruenza tra angoli e multipli di 2pi...

Definizione 61 Se $|U_m|$ è la cardinalità del sottogruppo degli elementi invertibili di $\mathbb{Z}_m$ definiamo $\varphi : \mathbb{N} \setminus \{0\} \to \mathbb{N} \setminus \{0\}$ come la funzione data da $\varphi(1) = 1$ e $\varphi(m) = |U_m|$.
Tale funzione si chiama *funzione di Eulero.*

Osservazione 62

i)Dall'Osservazione 60.i abbiamo $|U_m| = \#$ elementi coprimi con m.
ii) Se p è un numero primo $\varphi(p) = p - 1$

iii) Dal punto precedente si ricava che se p è primo allora $\mathbb{Z}_p$ è un campo, infatti $\mathbb{Z}_p$ non ha divisori dello zero e ammette inverso per il prodotto per ogni elemento diverso da 0.

Ricordiamo che se G è un gruppo finito di ordine n allora $g^n = 1$; $\forall g \in G$. Utilizzando questo risultato sui gruppi finiti U_m, il cui ordine è $\varphi(m)$, otteniamo il seguente:

Teorema 63 (Teorema di Eulero) Sia $m \in \mathbb{Z}$ un numero, allora per ogni a coprimo con m si ha $([a]_{\mathbb{Z}_m})^{\varphi(m)} = [1]_{\mathbb{Z}_m}$.

Oppure, più semplicemente: $a^{\varphi(m)} \equiv 1_{mod\, m}$ $\forall a$ coprimo con m.

Un caso particolare del Teorema di Eulero è il seguente:

Teorema 64 (Piccolo teorema di Fermat) Se p è un numero primo allora $a^{\varphi(p)} \equiv 1_{mod\, p}$ per ogni a che non sia multiplo di p.

Osservazione 65 Se p è un numero primo allora:

i) Possiamo liberarci della condizione "a non multiplo di p" ottenendo $a^p \equiv a_{mod\, p}\, \forall a \in \mathbb{Z}$.

Infatti per l'Osservazione 62.ii $\varphi(p) = p - 1$, da cui $a^{\varphi(p)} = a^{p-1} \equiv 1_{mod\, p}$ e moltiplicando entrambi i membri per a si ottiene il risultato sotto le stesse ipotesi del Teorema di Fermat, mentre se a fosse multiplo di p otterremmo la congruenza banale $0 \equiv 0_{mod\, p}$.

ii)Una riformulazione del piccolo teorema di Fermat è la seguente:

In $\mathbb{Z}_p$ $[a]^p = [a^p] = [a]$.

2.2.1 Applicazioni dei teoremi di Eulero e Fermat

Sfruttando questi due ultimi teoremi abbiamo la capacità di risolvere problemi del tipo:

i) Trovare l'ultima cifra di 7^{143}

Chiedere l'ultima cifra di un numero sottende la scelta di un sistema numerico. Ovviamente non essendo specificato si assume per convenzione sia quello decimale. Vogliamo quindi calcolare la congruenza modulo 10 del numero in questione. (Per trovare le ultime due cifre dovremmo usare la congruenza mod 100)

Calcoliamo dunque $\varphi(10) = 4$ e notiamo inoltre che 7 è primo con 10, dunque $7^4 \equiv 1_{mod\,10}$ per il teorema di Eulero.
Sfruttando la divisione euclidea per 4 otteniamo: $143 = 35 \cdot 4 + 3$ e per le usuali proprietà delle potenze abbiamo che : $7^{143} = (7^4)^{35} \cdot 7^3$.
Sappiamo che $(7^4)^{35} \equiv 1_{mod\,10}$ e quindi $7^{143} \equiv 1 \cdot 7^3_{mod\,10}$. Il problema si è ora ridotto al calcolo dell'ultima cifra di 7^3. Lo si può fare con la forza bruta o in alternativa utilizzando le congruenze:
$7^3 = 7^2 \cdot 7$;
$7^2 = 49 \equiv 9_{mod\,10}$;
$9 \cdot 7 = 63 \equiv 3_{mod\,10}$.

ii) Provare che $3n^7 + 4n^{19} + 2n + 5n^{31}$ *è divisibile per 7 per ogni numero n.*
Vogliamo considerare la congruenza mod 7. Osserviamo anzitutto che 7 è primo e dunque ci sono i presupposti per l'utilizzo del teorema di Fermat.

Dall'Osservazione 65 possiamo dire che

(I termine) $3n^7 \equiv 3n_{mod\,7}$

(II termine) Utilizzzando la divisione euclidea per 7 otteniamo $19 = 2 \cdot 7 + 5$ e per le proprietà delle potenze $4n^{19} = 4 \cdot (n^7)^2 \cdot n^5$ che per l'Osservazione 65

$\equiv 4n^2 \cdot n^5_{mod\,7} \equiv 4n^7_{mod\,7} \equiv 4n_{mod\,7}$

(IV termine) Analogamente a quanto sopra $5n^{31} = 5 \cdot (n^7)^4 \cdot n^3 \equiv 5n^4 \cdot n^3_{mod\,7} \equiv 5n^7_{mod\,7} \equiv 5n_{mod\,7}$

Ci riconduciamo dunque alla divisibilità per 7 di:
$3n + 4n + 2n + 5n = 14n$ che è banalmente vero.

iii) Provare che 511 non è un numero primo.

Supponiamo che esso sia primo e dunque $\varphi(511) = 510$ (Osservazione 62.ii), consideriamo $2^{\varphi(511)} = 2^{510}$ (ovvero 2^{p-1}), dovremmo avere per Fermat che:
$2^{510} \equiv 1_{mod\,511}$.
Osserviamo che $511 = 512 - 1 = 2^9 - 1$, quindi $2^9 - 1 \equiv 0_{mod\,511}$, ovvero:
$2^9 \equiv 1_{mod\,511}$.

D'altra parte, usando la divisione euclidea per 9, abbiamo $510 = 9 \cdot 56 + 6$ e quindi:
$2^{510} = (2^9)^{56} \cdot 2^6 \equiv 2^6_{mod\,511}$ Il che è assurdo perchè comporterebbe $1 = 2^6$.

2.3 Il teorema cinese dei resti

Teorema 66 (Teorema cinese dei resti) Siano $m_1, \dots m_r \in \mathbb{N}$ a due a due coprimi. Siano inoltre $a_1, \dots a_r \in \mathbb{Z}$. Allora il sistema di congruenze nell'incognita x:

$$\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \\ \qquad\qquad\qquad \vdots \\ x \equiv a_r \mod m_r. \end{cases}$$

ammette una soluzione y_1. Inoltre, se y_2 è un'altra soluzione si ha $y_1 \equiv y_2 \mod M$ con $M = m_1 \cdot m_2 \cdot \dots \cdot m_r$.

Dimostrazione Consideriamo dapprima il sistema:

$$\begin{cases} x \equiv 1 \mod m_1 \\ x \equiv 0 \mod m_2 \\ \qquad\qquad\qquad \vdots \\ x \equiv 0 \mod m_r. \end{cases}$$

Dalle ipotesi si ha che m_1 è coprimo con tutti gli altri m_i e dunque m_1 è anche coprimo con $M_1 = M/m_1 = m_2 \cdot \dots \cdot m_r$. Ovvero $MCD(m_1, M_1) = 1$.

Per l'identità di Bezout $1 = \alpha m_1 + \beta M_1$; $1 - \alpha m_1 = \beta M_1$.

Osserviamo che $x_1 = 1 - \alpha m_1$ è soluzione del sistema. Infatti esso è congruo ad $1_{mod\, m_1}$ ma è anche uguale a βM_1 il quale è congruo a $0_{mod\, m_i}$ per ogni i=2,. . . ,r.

Consideriamo ora i sistemi:

$$\begin{cases} x \equiv 0 \ _{mod\, m_1} \\ x \equiv 1 \ _{mod\, m_2} \\ x \equiv 0 \ _{mod\, m_3} \\ \\ \\ x \equiv 0 \ _{mod\, m_r}. \end{cases} \quad \begin{cases} x \equiv 0 \ _{mod\, m_1} \\ x \equiv 0 \ _{mod\, m_2} \\ x \equiv 1 \ _{mod\, m_3} \\ \\ \\ x \equiv 0 \ _{mod\, m_r}. \end{cases} \quad \begin{cases} x \equiv 0 \ _{mod\, m_1} \\ x \equiv 0 \ _{mod\, m_2} \\ x \equiv 0 \ _{mod\, m_3} \\ \\ \\ x \equiv 1 \ _{mod\, m_r}. \end{cases}$$

Con analoghe considerazioni troviamo le soluzioni $x_2, x_3, \ldots, x_r$ dei rispettivi sistemi.

Ritornando ora al sistema originale:

$$\begin{cases} x \equiv a_1 \ _{mod\, m_1} \\ x \equiv a_2 \ _{mod\, m_2} \\ \\ \\ x \equiv a_r \ _{mod\, m_r}. \end{cases}$$

Una sua soluzione è $y_1 = \sum_{i=1}^{r} a_i x_i$, inoltre aggiungendo un multiplo di M le congruenze rimangono invariate. Verifichiamo che esse siano le sole soluzioni.

Siano $y_1; y_2$ due soluzioni. Si verifichi che $y_1 - y_2$ è una soluzione di

$$\begin{cases} x \equiv 0 \mod m_1 \\ x \equiv 0 \mod m_2 \\ \qquad\qquad \vdots \\ x \equiv 0 \mod m_r. \end{cases}$$

Allora $y_1 - y_2$ è divisibile per ogni m_i, dunque, essendo $m_1, \ldots, m_r$ coprimi, M divide $y_1 - y_2$.

Osservazione 67

i) Nell'ultima parte della dimostrazione sfruttiamo la proprietà: Se $m, n \in \mathbb{N}$ sono coprimi e se per qualche $a \in \mathbb{Z}$ vale che $m|a$ ed $n|a$ allora $m \cdot n|a$.

ii) Se conosciamo una soluzione particolare y_1 allora l'insieme delle soluzioni del sistema ha la forma $S = \{y|\ y = y_1 + kM; k \in \mathbb{Z}\}$

Teorema 68 (Formulazione alternativa del teorema cinese dei resti)
Se $m_1, \ldots, m_n \in \mathbb{N}$ sono numeri a due a due coprimi ed $M = m_1 \cdot m_2 \cdot \cdots \cdot m_n$ allora $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$ è isomorfo a $\mathbb{Z}_M$.

Dimostrazione Consideriamo l'omomorfismo $\varphi : \mathbb{Z} \to \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$ tale che $\varphi(x) = ([x]_{m_1}, [x]_{m_2}, \ldots, [x]_{m_n})$ (Le operazioni nel codominio sono definite componente per componente).
Tale applicazione è suriettiva: per ogni n-upla $R = ([a_1]_{m_1}, [a_2]_{m_2}, \ldots, [a_n]_{m_n})$ esiste, per il teorema 66, un elemento x tale che $\varphi(x) = R$. Inoltre, per il II teorema di omomorfismo tra anelli: $\mathbb{Z}/ker\ \varphi \simeq \varphi(\mathbb{Z}) = \mathbb{Z}_1 \times \cdots \times \mathbb{Z}_n$. Dove

l'ultima uguaglianza segue dal fatto che φ è un epimorfismo.
$ker\,\varphi = \{x \mid \varphi(x) = ([0]_{m_1}, [0]_{m_2}, \ldots, [0]_{m_n})\}$ e $x \in ker\,\varphi \iff x = kM$ con k intero; ovvero $ker\,\varphi =_M \mathbb{Z}$.

Si conclude che $\mathbb{Z}/ker\,\varphi = \mathbb{Z}/_M\mathbb{Z} \simeq \mathbb{Z}_M \simeq \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$

3 L'inversione del teorema di Lagrange

3.1 Caso dei gruppi ciclici e abeliani, teorema di Cauchy

In questa sezione riprendiamo in considerazione il Teorema 15 (di Lagrange), in particolare vogliamo studiare se e sotto quali ipotesi vale il viceversa.

Vediamo subito una situazione in cui ciò avviene:

Lemma ?? Se G è un gruppo ciclico di ordine n e se $m|n$ allora esiste H sottogruppo di G di ordine m.

Dimostrazione Sia $G = \langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$ un gruppo ciclico di ordine n. Supponiamo $n = m \cdot d$. Consideriamo il sottogruppo $H = \langle g^d \rangle$ i cui elementi sono del tipo $g^{d^0}, g^{d^1}, \ldots, g^{d^i}$. Per le proprietà delle potenze possiamo scrivere più semplicemente i suoi elementi come $g^{d \cdot i}$. Per ipotesi abbiamo poi che $g^{d \cdot m} = g^n = 1$. Dunque H ha al più m elementi; ne avrebbe di meno se per qualche $r_1, r_2 < m$ distinti si avesse $g^{dr_1} = g^{dr_2}$. Supponiamo allora che esistano $r_1, r_2 < m$ tali che $g^{d \cdot r_1} = g^{d \cdot r_2}$ vogliamo osservare che $r_1 = r_2$

ovvero che $g^{d(r_1-r_2)} = g^0 = 1$. Nell'ambiente ciclico indotto da G questo accade se e solo se $d(r_1 - r_2)$ è un multiplo di n. Si ha dunque la condizione $n = md|d(r_1 - r_2)$ cioè $m|(r_1 - r_2)$ ed essendo questi entrambi minori di m si deve avere $r_1 - r_2 = 0$.

Per continuare la nostra indagine avremo bisogno del seguente:

Teorema 69 (Teorema di Cauchy) Sia G un gruppo abeliano finito di ordine n. Sia p un numero primo divisore di n. Allora in G esiste un elemento di ordine p.

Dimostrazione Per induzione completa sull'ordine n di G:

Per n=1: banale.

Per n=2 o n=3: Tutti i gruppi di ordine primo p sono isomorfi a $\mathbb{Z}_p$ ed in particolare sono ciclici (Osservazione 27) e per il lemma visto sopra soddisfano la tesi.

Sia dunque $n \geq 4$ e sia p primo tale che $p|n$. Supponiamo vera la tesi per ogni $m < n$. Prendiamo $h \neq 1 \in G$ e consderiamo $H = \langle h \rangle$; si presentano tre casi:

i) H=G, G è ciclico e dal lemma visto sopra segue la tesi.

ii) $H \neq G$, p divide l'ordine di H. H è ciclico e per il lemma visto sopra esiste un suo sottogruppo di ordine p, ovvero generato da un elemento h' di ordine p.

iii) Supponiamo infine $H \neq G$ e che p non divida $m = |H|$. Consideriamo il gruppo quoziente G/H. Per Lagrange sappiamo che $|G/H| = |G|/|H| = n/m = a$.

Abbiamo quindi che $n = pb = ma$; per ipotesi p è primo e non divide m,

allora dovrà dividere a, possiamo allora scrivere $p\frac{b}{m} = a$ sapendo che la quantità $\frac{b}{m}$ è intera, cioè p divide a o ancora p divide $|G/H|$.

L'ordine di G/H è strettamente minore di n, quindi possiamo sfruttare l'ipotesi induttiva: esiste un elemento $[x] \in G/H$ di ordine p.
Poniamo quindi $[x]^p = [1]$ che implica $x^p \in H$; ovvero esiste un r tale che $x^p = h^r$.

Posto $d = MCD(m, r)$ vogliamo provare che l'elemento $x^{\frac{m}{d}}$ ha ordine p.
Anzitutto $x^{\frac{m}{d}} \neq 1$. Infatti se fosse $x^{\frac{m}{d}} = 1$ avremmo in particolare che $[x]^{\frac{m}{d}} = [1]$, il che comporterebbe che $\frac{m}{d}$ è un qualche multiplo di $p = ord\,[x]$; contro l'ipotesi "p NON divide l'ordine di H".
Concentriamoci ora sulla catena di uguaglianze:
$(x^{\frac{m}{d}})^p = (x^p)^{\frac{m}{d}} = (h^r)^{\frac{m}{d}} = (h^{\frac{r}{d}})^m$.
$\frac{r}{d}$ è un numero intero per costruzione di d. Dunque $h^{\frac{r}{d}} \in H$ e siccome H è ciclico di ordine m e per le proprietà delle potenze: $(x^{\frac{m}{d}})^p = (h^{\frac{r}{d}})^m = 1$. Se $x^{\frac{m}{d}}$ elevato alla p fa 1 allora l'ordine di $x^{\frac{m}{d}}$ è un divisore di p, ma essendo p un numero primo esso è il suo unico divisore. L'ordine di $x^{\frac{m}{d}}$ è p e ciò conclude la dimostrazione.

Possiamo ora provare il seguente risultato:
Teorema ? Se G è un gruppo abeliano finito e se $m|n$ allora esiste H sottogruppo di G di ordine m.

La dimostrazione si fa anche in questo caso per induzione completa su n. Tenendo conto del Lemma? e dell'osservazione 27 (?) possiamo già dire che il risultato ?????è vero per numeri primi??????????, supponiamo dunque n

non primo. Sia m divisore di n. Sia p primo tale che $p|m$ (naturalmente si ha anche $p|n$). Per il teorema di Cauchy $\exists h$ di ordine p e dunque $H = \langle h \rangle \subset G$ è sottogruppo di ordine p. A questo punto consideriamo G/H, il quale è un gruppo finito con meno elementi di G ed ha ordine $\frac{n}{p}$ e siccome $p|m$, $m|n$ otteniamo $\frac{m}{p}|\frac{n}{p}$. Per induzione G/H ha un sottogruppo di ordine $\frac{m}{p}$. Ricordando l'Osservazione ?? (II teor omomorf) abbiamo che tutti i sottogruppi di G/H sono della forma K/H. Poniamo dunque $|K/H| = \frac{m}{p}$ e, per Lagrange, $= |K|/|H| = |K|/p$ dunque $|K| = m$ è un sottogruppo di G di ordine m.

Osservazione 80 Negli ultimi due teoremi l'ipotesi che G sia abeliano è fondamentale, infatti è necessaria questa proprietà affinchè H sia senza dubbio un sottogruppo normale di G e si possa così costruire il quoziente G/H.

3.2 I teoremi di Sylow

Proseguiamo ora con tre importanti teoremi di cui si omette la dimostrazione.

Teorema (I teorema di Sylow) Sia G un gruppo finito di ordine n e sia p primo tale che p^α divida n. Allora G ha un sottogruppo di ordine p^α

Osservazione Per $\alpha = 0$ abbiamo $p^\alpha = 1$; esso divide l'ordine di qualsiasi gruppo finito e il corrispondente sottogruppo è quello banale $\{1\}$.
Se $\alpha = 1$ si ottiene un risultato simile al teorema di Cauchy.

Definizione Sia p primo e $\alpha \in \mathbb{N}$. Un gruppo finito di ordine p^α si dice *p-gruppo*. Se G è un gruppo finito ed H è un suo sottogruppo di ordine p^α

esso si dice *p-sottogruppo di G.*

Definizione Siano G un gruppo finito di ordine n, p primo ed $\alpha \in \mathbb{N}$ tale che $p^\alpha | n$ ma $p^{\alpha+1} \nmid n$. Un p-sottogruppo di G di ordine p^α si dice *p-sottogruppo di Sylow* (CONTROLLA DEFINIZIONE)

Teorema (II teorema di Sylow) Sia G un gruppo finito di ordine n e sia p primo.
i) Ogni p-sottogruppo di G è contenuto in un p-sottogruppo di Sylow.
ii) Tutti i p-Sylow sottogruppi sono tra loro coniugati.

Teorema (III teorema di Sylow) Sia G un gruppo finito di ordine n e sia p primo. Definiamo $N_p :=$ # p-Sylow sottogruppi di G (numero dei p-Sylow sottogruppi di G). Se $n = p^\alpha m$ e $m \nmid p$ allora $N_p \mid m$ e $N_p \equiv 1_{mod\, p}$.

3.2.1 Applicazioni dei teoremi di Sylow

Sfruttando i teoremi di Sylow possiamo risolvere problemi del tipo:

Sia G un gruppo finito di ordine 303, quanti sono i suoi sottogruppi normali?

Anzitutto ci chiediamo che ordine può avere un qualsiasi sottogruppo di G:

Dal teorema di Lagrange sappiamo che ogni sottogruppo di G deve avere un ordine che divida 303. Osserviamo che gli unici divisori di 303 sono 1, 3, 101 e 303. Ai numeri 1 e 303 corrispondono i sottogruppi banali 1 e G. Restano

da considerare 3 e 101, per ora sappiamo che se H è un sottogruppo proprio di G esso ha ordine 3 oppure 101.

3 e 101 sono primi e per il I teorema di Sylow esistono dei sottogruppi di G di tali ordini.

Quanti sottogruppi di G hanno ordine 3? Poichè $3|303$ e $3^2 \nmid 303$ otteniamo che ogni sottogruppo di ordine 3 è un 3-sottogruppo di Sylow. Per sapere quanti ce ne sono dovremo valutare N_3. Per il III teorema di Sylow deve essere $N_3 \equiv 1_{mod\,3}$ il che ci fa ottenere come candidati $N_3 = 1, 4, \ldots, 1 + 3k$. Per determinare quale tra questi è il corretto utilizziamo ancora il Teorema III, questa volta la seconda parte: $N_3 \mid 101$ ed essendo 101 primo si conclude che $N_3 = 1$. Dunque esiste un unico 3-sottogruppo di Sylow e in questo caso esso è per di più l'unico sottogruppo di ordine 3 di G. Lo chiamiameremo H.

H è normale? A tale scopo utilizziamo il II teorema di Sylow: Prendiamo $g \in G$ e consideriamo il coniugio $g^{-1}Hg$; esso è un 3-sottogruppo di Sylow, per l'unicità dimostrata sopra $H = g^{-1}Hg$. Questo accade se e solo se H è commutativo, ovvero normale.

Analogamente per 101:
1) 101^2 non divide 303, dunque tutti i sottogruppi sono 101-Sylow sottogruppi.
2) Per calcolare N_{101} ci serviamo del teorema III e osserviamo che $N_{101} = 1$; esiste un unico K di ordine 101.
3) Considerando il coniugio di K utilizzando il II teor. e l'unicità concludiamo che tale sottogruppo è normale.

In conclusione: I sottogruppi normali di G sono in tutto 4: 1, H, K, G.

Si può dimostrare che $G \simeq \mathbb{Z}_{303} \simeq \mathbb{Z}_3 \times \mathbb{Z}_{101}$ e da qui osservare che esso è ciclico e abeliano.

Suggerimento: Abbiamo trovato che gli unici sottogruppi propri di G sono H e K di ordini 3 e 101 rispettivamente.

Si consideri la funzione $\varphi\colon G \to G/H \times G/K$ definita da $\varphi(g) = ([g]_H, [g]_K)$...

Vogliamo trovare alcune informazioni sui sottogruppi di S_4.

Si veda l'Appendice per le nozioni di base sui gruppi di permutazioni.

In analogia con quanto fatto sopra cerchiamo i possibili ordini tramite il teorema di Lagrange. $|S_4| = 4! = 24 = 2^3 \cdot 3$. Possiamo avere sottogruppi di ordine 1, 2, 3, 4, 6, 8, 12, 24. Ad 1 e 24 corrispondono i sottogruppi banali. Per Sylow abbiamo che esistono sottogruppi di ordine $2, 2^2, 2^3$ *e* 3. In particolare i sottogruppi di ordine 2^3 sono dei 2-Sylow sottogruppi e quelli di ordine 3 sono 3-Sylow sottogruppi.

Per il III teorema di Sylow:

i) $N_2 \equiv 1_{mod\,2}$ e $N_2|3$. Dunque $N_2 = 1$ oppure $N_2 = 3$.
C'è un solo gruppo di ordine 8 oppure ce ne sono 3.

ii)$N_3 \equiv 1_{mod\,3}$ e $N_3|2$. Dunque $N_3 = 1$ oppure $N_3 = 4$
C'è un solo gruppo di ordine 3 oppure ce ne sono 4.

Quelle sottolineate sono le informazioni che siamo riusciti a ricavare da questa trattazione.

Consideriamo il gruppo S_3 e il gruppo ciclico $C_2 = \{1, a\}$ (dove $a^2 = 1$).

Vogliamo studiare i sottogruppi del gruppo $G = S_3 \times C_2$

G ha 12 elementi e $12 = 2^2 \cdot 3$. Dunque per Sylow sappiamo che ci sono sottogruppi propri di G di ordine 2, 3 e 4.
I sottogruppi di ordine 2^2 e quelli di ordine 3 sono p-Sylow sottogruppi di G.
Con considerazioni analoghe a quelle degli esercizi precedenti otteniamo che:
i)C'è un solo gruppo di ordine 4 oppure ce ne sono 3.
ii)C'è un solo gruppo di ordine 3 oppure ce ne sono 4.

Vogliamo studiare come sono fatti questi sottogruppi, ci concentriamo soltanto su quelli di ordine 4. Ci chiediamo se essi possono essere ciclici.

Ricordando l'osservazione (26circa) possiamo dire che se $H \subset G$ ha ordine 4 allora ogni suo elemento ha un ordine che divide 4.

Iniziamo chiedendoci se gli elementi di H hanno ordine 4, questo implicherebbe che H è ciclico. Supponiamo quindi esista un sottogruppo ciclico di G di ordine 4, esso sarà generato da un elemento (σ, α); $\sigma \in S_3$, $\alpha \in C_2$. e sarà della forma $\langle(\sigma, \alpha)\rangle = \{(1, 1),\ (\sigma, \alpha),\ (\sigma^2, \alpha^2),\ (\sigma^3, \alpha^3)\}$. Abbiamo inoltre la condizione $(\sigma^4, \alpha^4) = (1, 1)$.
Qualunque sia $\alpha \in C_2$ esso avrà ordine 1 oppure 2, in entrambe i casi va bene.
Per σ invece non possiamo dire altrettanto: Dovremmo avere σ di ordine 4

ma ciò è impossibile, infatti per Lagrange $\langle\sigma\rangle \subset S_3$ deve avere un ordine divisore di $S_3 = 3! = 6$, quindi in particolare non può essere $|\langle\sigma\rangle| = 4$.
Il sottogruppo (o i tre sottogruppi) di ordine 4 non può essere ciclico.

Abbiamo appena visto che nessun elemento di H può avere ordine 4, un elemento di ordine 1 c'è sempre: l'unità. L'unico ordine che resta possibile è dunque 2.

Gli elementi di ordine 2 in G sono tutte e sole le coppie in cui almeno una delle entrate ha ordine 2 e nessuna ne ha ordine superiore. In S_3 gli unici elementi di ordine 2 sono gli scambi, mentre l'unico di ordine 1 è l'identità, che denotiamo con (1). In C_2 1 ha ordine 1 ed a ha ordine 2. L'insieme degli elementi di G di ordine 2 è
$G_2 = \{((1), a), ((1,2), 1), ((1,2), a), ((1,3), 1), ((1,3), a), ((2,3), 1), ((2,3), a)\}$.
Mentre il neutro è ((1),1)

Costruiamo ora un sottogruppo $H \subset G$ di ordine 4 utilizzando questi elementi, senza dubbio ci serve il neutro e un primo elemento arbitrario in G_2, ad esempio ((1,2), 1). Si capisce che una volta preso questo primo elemento potremmo essere in qualche modo vincolati nel scegliere i seguenti in modo opportuno, si potrebbe proseguire per tentativi, ma è una via poco elegante. Cerchiamo piuttosto di capire come procedere in generale:

Prendiamo due elementi $(\sigma, \alpha), (\tau, \beta) \in G_2$. Vogliamo costruire un gruppo H di 4 elementi che li contenga: $(\sigma, \alpha), (\tau, \beta) \in H$ In particolare vogliamo la chiusura con l'operazione di G. Imponiamo dunque $(\sigma, \alpha) * (\tau, \beta) = (\sigma\tau, \alpha\beta) \in H$. Si verifica facilmente che $(\sigma\tau, \alpha\beta) \neq (\sigma, \alpha) \neq (\tau, \beta)$, che anche esso

appartiene a G_2 e che $(\sigma\tau, \alpha\beta) * (\sigma, \alpha) = (\tau, \beta)$. Abbiamo quindi trovato un insieme di tre elementi chiuso con l'operazione, aggiungendo l'unità siamo capaci di dire che H è della forma $\underline{H = \{((1), 1),\ (\sigma, \alpha),\ (\tau, \beta),\ (\sigma\tau, \alpha\beta)\}}$.

Questo comporta che l'insieme $\{1, \sigma, \tau, \sigma\tau\}$ è un sottogruppo di S_3, ma per ragionamenti sugli ordini (Lagrange, $|S_3| = 6 \dots$) dobbiamo avere che due o tre di questi elementi coincidono. Questo ci porta all'ulteriore condizione $\underline{\sigma = \tau \text{ sono scambi oppure } \sigma = (1) \vee \tau = (1).}$

Secondo queste direttive possiamo costruire tutti i sottogruppi di G di 4 elementi:

$\underline{H_1 = \{((1), 1),\ ((1, 2), 1),\ ((1, 2), a),\ ((1), a)\}}$
$\underline{H_2 = \{((1), 1),\ ((1, 3), 1),\ ((1, 3), a),\ ((1), a)\}}$
$\underline{H_3 = \{((1), 1),\ ((2, 3), 1),\ ((2, 3), a),\ ((1), a)\}}$
In particolare ora sappiamo $\underline{N_2 = 3}$.

4 L'anello dei polinomi

4.1 Costruzione dell'anello dei polinomi in una variabile

Sia $(A, +, \cdot)$ un anello unitario e commutativo. Sia $B = \{(a_n)_n \mid a_n \in A \wedge \exists \overline{n} \in \mathbb{N} : a_n = 0 \, \forall n > \overline{n}\}$ l'insieme delle successioni a valori in A i cui termini non si annullano soltanto per un numero finito di indici.

Sia + una somma in B definita termine per termine.

Sia $\cdot$ un prodotto in B definito da $(a_n)_n \cdot (b_n)_n = (c_n)_n$ dove, per ogni i, $c_i = \sum_{j=0}^{i} a_j b_{i-j}$.

Si verifica facilmente che:

i) La somma è commutativa, associativa ed ha come elemento neutro la successione nulla.

ii) Il prodotto è commutativo, associativo e il suo elemento neutro è la successione il cui primo termine è 1 e i successivi sono nulli.

iii) Le due operazioni sono legate dalla proprietà distributiva $(a_n + b_n)c_n = a_n c_n + b_n c_n$; $\forall a_n, b_n, c_n \in B; \forall n \in \mathbb{N}$

Da quanto detto sopra $(B, +, \cdot)$ risulta essere un anello commutativo e unitario.

La proprietà $\exists \overline{n} \in \mathbb{N} \ : a_n = 0 \, \forall n > \overline{n}$ si esprime a parole dicendo che la successione si annulla *per quasi ogni n* o che *esiste soltanto un numero finito di valori per i quali non vale la condizione.*

Definizione 4.1.1 Il prodotto dell'anello B si dice *prodotto di Cauchy.*

Osservazione 4.1.2 Il prodotto di Cauchy è un'operazione interna all'anello, infatti, se $(a_n)_n, (b_n)_n \in B$ sono due successioni abbiamo $(a_n)_n \cdot (b_n)_n = (c_n)_n$ dove per definizione $c_i = \sum_{j=0}^{i} a_i b_{i-j}$.
Siccome $(a_n)_n, (b_n)_n \in B$ allora $\exists \overline{p}, \overline{q} \in \mathbb{N} \mid \forall p > \overline{p}$ si ha $a_p = 0$ e $\forall q > \overline{q}$ si ha $b_q = 0$. Posto $\overline{r} = \overline{p} + \overline{q}$ abbiamo anche $c_r = 0,\ \forall r > \overline{r}$ e quindi $(c_n)_n \in B$.

Al fine di esplicitarne i termini una successione $(a_n)_n \in B$ verrà indicata con la scrittura $(a_0, a_1, \dots, a_n, \dots)$.

Osservazione 4.1.3 L'anello A è isomorfo ad un sottoanello $\tilde{A} \subseteq B$. Infatti la funzione $j : A \to B$ definita da $a \mapsto (a, 0, 0, \dots)$ è un monomorfismo e dunque (per osservazione II teorema di omomorfismo): $A \simeq j(A) = \tilde{A}$.
D'ora in poi un elemento $(a, 0, \dots)$ (con $a \in A$) di $\tilde{A} \subseteq B$ verrà denotato semplicemente come a.

In B esistono alcuni elementi con particolari proprietà. Tra questi rientrano senza dubbio $(0, 0, \dots, 0, \dots)$ elemento neutro della somma e $(1, 0, \dots, 0, \dots)$ unità del prodotto. Un altro elemento fondamentale è $x = (0, 1, 0, 0, \dots)$ la cui proprietà riguarda le sue potenze:
$x^0 = (1, 0, 0, \dots)$
$x = (0, 1, 0, 0, \dots)$
$x^2 = (0, 0, 1, 0, 0, \dots)$
$x^3 = (0, 0, 0, 1, 0, \dots)$
$\vdots$
$x^n = (0, 0, \dots, 1, 0, \dots)$ dove 1 sta al posto *n+1*-esimo.

Osservazione 4.1.4 Un qualunque elemento $(a_0, a_1, a_2, \dots, a_n, 0, 0, \dots)$ di B si può scrivere come $(a_0, 0, 0, \dots) + (0, a_1, 0, \dots) + \dots + (0, \dots 0, a_n, 0, \dots)$
D'altra parte abbiamo anche che:
$(a_0, 0, 0, \dots) \cdot x^0 = (a_0, 0, 0, \dots)$
$(a_1, 0, 0, \dots) \cdot x = (0, a_1, 0, \dots)$
$(a_2, 0, 0, \dots) \cdot x^2 = (0, 0, a_2, 0, \dots)$
$(a_3, 0, 0, \dots) \cdot x^3 = (0, 0, 0, a_3, 0, \dots)$
$\vdots$
$(a_n, 0, 0, \dots) \cdot x^n = (0, \dots, 0, a_n, 0, \dots)$ dove a_n sta al posto *n+1*-esimo.

Segue in modo naturale che

$$(a_0, a_1, a_2, \dots, a_n, 0, 0, \dots) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$$

Definizione 4.1.5 L'anello B come sopra definito si dice *anello dei polinomi con coefficienti in A nella variabile x* e si indica con $A[x]$. I suoi elementi sono espressioni della forma $a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$ e si dicono *polinomi.*

Osservazione 4.1.6 (Principio d'identità dei polinomi) Due polinomi in $A[x]$ sono uguali se e solo se i loro coefficienti sono ordinatamente uguali.

4.2 Proprietà dei polinomi

Per completezza ripetiamo la definizione precedente:
Definizione 4.2.1 L'anello B costruito nel precedente paragrafo si dice *anello dei polinomi con coefficienti in A nella variabile x* e si indica con $A[x]$. I suoi elementi sono espressioni della forma $a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$ e si

dicono *polinomi*. Per indicare un generico polinomio nella variabile x si può usare l'usuale notazione per le funzioni $f = f(x) = a_0+a_1x+a_2x^2+\cdots+a_nx^n$.

Definizone 4.2.2

i) Sia $g = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ un polinomio, esso si dice essere *di grado n* se a_n è il suo ultimo termine non nullo e si denota con *deg g*.
ii) Sia $g = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ un polinomio, il termine a_0 si dice *termine noto del polinomio* e il termine a_n si dice *termine direttivo del polinomio* e si indica con il simbolo $lc(g)$.
iii) Un polinomio avente coefficiente direttivo 1 si dice *monico*.
iv) Il polinomio nullo non ha grado anche se talvolta si dice avere grado -1 o $-\infty$
v) Un polinomio costituito dal solo termine noto si dice *polinomio costante* ed ha grado 0.
vi) Si dicono *radici* o *zeri* di un polinomio $f(x)$ i valori di x per i quali $f(x) = 0$.

Osservazione 4.2.3

i) Scrivere un polinomio come fatto nella Definizione 4.2.1 è molto utile anche perchè permette di tornare agevolmente alla notazione introdotta inizialmente. Così per dimostrare che la somma di due polinomi è a sua volta un polinomio si può procedere riscrivendo $(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) + (b_0 + b_1x + b_2x^2 + \cdots + b_px^p$ come $(a_0, a_1, \ldots, a_n, 0\ldots) + (b_0, b_1, \ldots, b_p, 0, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots, a_n + b_n, b_{n+1}, \ldots, b_p, 0\ldots)$ per poi ritornare a $(a_0+b_0)+(a_1+b_1)x+\cdots+(a_n+b_n)x^n+b_{n+1}x^{n+1}+\cdots+b_px^p$

dove si è supposto $n < p$.
ii) Se f è un polinomio monico allora esso non ha altri polinomi monici associati oltre ad f stesso. Infatti un polinomio è sempre associato a se stesso (il neutro del prodotto è sempre invertibile). Non ce ne sono altri in quanto se $f = a_0 + a_1x + \cdots + x^n$ per qualunque unitario $u \neq 1$ per il quale lo si moltiplichi il polinomio prodotto avrà coefficiente direttivo $u \neq 1$.
iii) Ogni polinomio p è associato ad uno ed un solo polinomio monico, se il coefficiente direttivo di p è invertibile. Infatti se $p = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ allora il polinomio $\overline{p} = a_n^{-1}p$ è monico, non ce ne sono altri per il punto precedente.

Osservazione 4.2.4 Riprendiamo l'Osservazione 4.1.2: il numero $\overline{r}$ di cui ci siamo serviti riflette una nota proprietà: Presi due polinomi $(a_n)_n, (b_n)_n$ di grado $\overline{p}$ e $\overline{q}$ rispettivamente il loro prodotto $(c_n)_n$ ha grado $\overline{r} = \overline{p} + \overline{q}$. Tuttavia questa proprietà, in generale, è falsa. La proprietà corretta è piuttosto:
Se $(a_0, a_1, \dots, a_p, 0, \dots), (b_0, b_1, \dots, b_q, 0, \dots)$ sono due polinomi di grado p e q rispettivamente allora il loro prodotto $(c_i)_i$ ha grado $r \leq p + q$.

Si pensi ad esempio ai polinomi $(1 + 2x), (3 + 3x^3) \in \mathbb{Z}_6[x]$, i quali hanno grado 1 e 3 rispettivamente. Il loro prodotto è $(1 + 2x), (3 + 3x^3) = 3 + 6x + 3x^3 + 6x^4 \equiv (3 + 3x^3)_{mod\,6}$ che ha grado 3.

È naturale chiedersi quando sussista l'uguaglianza, abbiamo come risposta il seguente risultato.

Teorema 4.2.5 Se A è un dominio d'integrità allora due polinomi appartenenti a $A[x]$ di grado m ed n rispettivamente hanno per prodotto un

polinomio di grado $m + n$.

Guida per la dimostrazione Prendere due elementi $f, g \in A[x]$, scriverli in forma di successione per poter applicare la definizione del prodotto di Cauchy, al termine direttivo della successione prodotto possiamo applicare il fatto che in A non ci sono divisori dello zero osservando che i fattori che lo costituiscono sono non nulli per ipotesi.

Osservazione 4.2.6

i) Più in generale si ha che: Se $f, g \in A[x]$ sono due polinomi di cui almeno uno ha coefficiente direttivo invertibile allora sussiste l'uguaglianza $deg(f \cdot g) = deg\ f + deg\ g$.
ii) Se A è un dominio d'integrità, allora l'anello dei polinomi $A[x]$ è a sua volta un dominio d'integrità. Infatti siano $f, g \in A[x]$ due elementi non nulli, per il teorema precedente il loro prodotto ha grado $n+m$ e dunque tale elemento è a sua volta diverso dal polinomio nullo.

Definizione 4.2.7 Sia A un anello, $A[x]$ l'anello dei polinomi e sia $a \in A$ fissato. L'omomorfismo di anelli $v_a : A[x] \to A$ definito da $(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) \mapsto (a_0 + a_1a + a_2a^2 + \cdots + a_na^n)$ si dice *omomorfismo di valutazione.*

Talvolta un polinomio di $A[x]$ può essere indicato con la scrittura $f(x), g(x), \ldots$ Con questa notazione abbiamo $v_a(f(x)) = f(a) \in A$

Teorema 4.2.8 (Teorema di estensione) Siano A e B due anelli, $b \in B$ fissato. Sia inoltre $\varphi : A \to B$ un omomorfismo di anelli. Allora esiste un

unico omomorfismo di anelli $\Phi : A[x] \to B$ tale che $\Phi(a) = \varphi(a)\ \forall a \in A$ e $\Phi(x) = b$.

Dimostrazione. Supponiamo che una tale funzione esista, cerchiamo di capire come dovrebbe essere fatta. Si richiede che Φ sia un omomorfismo, quindi

$$\Phi(a_k x^k) = \Phi(a_k)\Phi(x^k) = \Phi(a_k)\Phi(x \cdot \cdots \cdot x) = \Phi(a_k)\Phi(x)^k$$

Inoltre $\Phi(x) = b$, e $\Phi(a_k) = \varphi(a_k)$. Troviamo allora che il generico monomio $a_k x^k$ deve necessariamente andare in $\Phi(a_k x^k) = \Phi(a_k)\Phi(x)^k = \varphi(a_k)b^k$. Si dovranno poi conservare anche le somme di monomi e quindi, preso un polinomio $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ la sua immagine attraverso Φ sarà

$$\Phi(a_0+a_1x+a_2x^2+\cdots+a_nx^n) = \Phi(a_0)+\Phi(a_1)\Phi(x)+\Phi(a_2)\Phi(x)^2+\cdots+\Phi(a_n)\Phi(x)^n = \\ = \varphi(a_0) + \varphi(a_1)b + \varphi(a_2)b^2 + \cdots + \varphi(a_n)b^n$$

Abbiamo quindi che, se esiste Φ tale da soddisfare le condizioni del teorema, non può che essere quella appena descritta.

Per dimostrare l'esistenza è sufficiente verificare che Φ come costruita sopra sia un omomorfismo di anelli. Presi due polinomi *f,g* si scrivono per esteso $\Phi(f+g), \Phi(fg)$ e sfruttando l'ipotesi che φ è un omomorfismo si conclude. □

Corollario 4.2.9 Se $\varphi : A \to B$ è un omomorfismo di anelli e $A[x]$, $B[y]$ sono anelli di polinomi allora esiste un unico omomorfismo $\Phi : A[x] \to B[y]$ tale che $\Phi(a) = \varphi(a)$ e $\Phi(x) = y$.

Dimostrazione Per l'Osservazione 4.1.3 attraverso j possiamo immergere B in $B[x]$ e applicando il risultato precedente otteniamo la tesi.

In simboli si può scrivere $A \xrightarrow{\varphi} B \xhookrightarrow{j} B[y]$ così da ottenere $A \xrightarrow{\varphi} B[y]$, e applicando il Teorema 4.2.8: $\exists! \Phi \mid A[x] \xrightarrow{\Phi} B[y]$.

Teorema 4.2.10 (Divisione di polinomi) Sia A un anello e siano $f, g \in A[x]$ due polinomi.
Se $g \neq 0$ ed il coefficiente direttivo di g è unitario in A allora $\exists! q, r \in A[x]$ tali che $f = qg + r$, con $deg\, r < deg\, g$.

Dimostrazione Se $deg\, g > deg\, f$ allora si ha $f = 0g + f$; consideriamo quindi il caso $deg\, g \leq deg\, f$.

La dimostrazione si svolge per induzione completa sul grado di f.
Consideriamo i due polinomi $f = a_0 + a_1x + \cdots + a_nx^n$ e $g = b_0 + b_1x + \cdots + b_mx^m$ con $b_m \neq 0$ invertibile. Per sfruttare l'ipotesi induttiva vorremmo trovare un polinomio correlato ad f ma di grado minore. Definiamo $f_1 = f - (a_n \cdot b_m^{-1} \cdot x^{n-m})g$. Osserviamo che il polinomio così definto ha grado inferiore ad f, possiamo così sfruttare l'ipotesi induttiva ottenendo $f_1 = q_1g + r_1$ con $deg\, r_1 < deg\, q_1$. Esprimendo ora f attraverso f_1 si ottiene: $f = f_1 + (a_nb_m^{-1}x^{n-m})g = (q_1g + r_1) + (a_nb_m^{-1}x^{n-m})g = (q_1 + a_nb_m^{-1}x^{n-m})g + r_1$.

Posti $q_1 + a_nb_m^{-1}x^{n-m} = q$ e $r = r_1$ si ha l'esistenza. Resta da verificare l'unicità: Supponiamo che il polinomio f abbia due espressioni: $f = qg + r = q'g + r'$ con $deg\, r, deg\, r' < deg\, q$. Si ha quindi anche $g(q - q') = r' - r$. Osserviamo che $r' - r$ ha grado minore di g mentre $g(q - q')$, per l'Osservazione 4.2.6, ha grado maggiore o uguale a g. Queste due condizioni sono soddisfatte contemporaneamente se e solo se $q - q' = r' - r = 0$. Dunque q,r sono unici.

Osservazione 4.2.11 Se l'anello dei coefficienti risulta essere un campo allora ogni suo elemento è invertibile, quindi in K[x] si può sempre effettuare la divisione tra polinomi.

4.3 Polinomi a coefficienti in un campo

D'ora in poi tratteremo soltanto di polinomi a coefficienti in un campo, per evidenziare ciò scriveremo K[x] al posto di A[x]. Troveremo molte analogie tra l'anello degli interi e l'anello K[x], come del resto abbiamo già potuto osservare per il Teorema 4.2.10 (unito all'Osservazione 4.2.11) e il Teorema 2.1.9.

Teorema 4.3.1 (Teorema di Ruffini) Sia $f \in K[x]$ un polinomio. Allora il resto della divisione di f per il polinomio $x - a$ è dato da $f(a)$.

Dimostrazione

Per il Teorema 4.2.10 abbiamo $f(x) = q(x)(x - a) + r(x)$. Valutando il polinomio in a otteniamo $f(a) = q(a)(a - a) + r(a) = r(a)$ con $deg\, r < 1$, ovvero r è un polinomio costante e $r(a) = r$. Dunque $f(a) = r$.

Teorema 4.3.2 $f \in K[x]$ è divisibile per $(x - a)$ se e solo se $f(a) = 0$.
Dimostrazione f è divisibile per $(x - a)$ se e solo se il resto della divisione è 0, se e solo se $f(a) = 0$.

Da questo Teorema segue che un polinomio $f \in K[x]$ di grado 2 o 3 è irriducibile se e solo se per ogni $a \in K$ si ha $f(a) \neq 0$. Infatti se f fosse

riducibile avrebbe un fattore di grado 1.

Teorema 4.3.4 (Teorema di D'Alambert) Sia $f \in K[x]$ un polinomio di grado n; $f \neq 0$. Allora f ha al massimo n radici.

Dimostrazione La dimostrazione si svolge per induzione sul grado di *f*.

Se $deg\ f = 0$ allora f è una costante e per ipotesi è diversa da 0. f ha 0 radici.

Sia $deg\ f = n > 0$. Sia $a \in K$ una radice di *f*. Per il Teorema 4.3.2 $f = f_1(x - a)$. Trovandoci in un campo ed essendo *deg (x-a)=1* deduciamo che $deg\ f_1 = n - 1$. Possiamo applicare l'ipotesi induttiva e dire che f_1 ha m radici, con $m \leq n - 1$. Ricordando la fattorizzazione $f = f_1(x - a)$ concludiamo che f ha m radici, con $m + 1 \leq n$.

Osservazione 4.3.5 i) Come conseguenza si ha che: Se K è un campo infinito e se $f, g \in K[x]$ sono due polinomi tali che $f(a) = g(a)$; $\forall a \in K$ allora *f=g*.

Preso il polinomio $h = f - g$, se per assurdo fosse diverso dal polinomio nullo 0 ci ricondurremmo al teorema precedente e si avrebbe che h ha un numero finito di radici ma per ipotesi $f(a) - g(a) = 0$; $\forall a \in K$, cioè ogni elemento a è radice di h, essendo K infinito si ha un assurdo.

ii) Questo risultato si può rendere più generale sostituendo l'ipotesi $f(a) = g(a)$; $\forall a \in K$ con l'ipotesi $f(a) = g(a)$; per infiniti $a \in K$.

iii) Tale risultato non vale in generale, come si vede osservando, ad esempio, i polinomi $(x + 1), (x^2 + 1) \in \mathbb{Z}_2$.

Definizione 4.3.6 Si dice *Massimo comun divisore* tra i polinomi $f, g \in K[x]$ il polinomio $d \in K[x]$ tale che $d|f$; $d|g$ e $\forall \delta$ che soddisfa la stessa condizione si ha $\delta|d$.

Osservazione 4.3.7 Dati due polinomi $f, g \in K[x]$, l'insieme $D = \{d : d|f \ e \ d|g\}$ dei divisori di *f,g* è uguale all'insieme $\Delta = \{\delta : \delta|(f-g) \ e \ \delta|g\}$ dei divisori dei polinomi *f-g,g*.
Infatti preso un divisore $d \in D$ si ha: $f = t_1 d$, $g = t_2 d$.
Allora $f - g = t_1 d - t_2 d = (t_1 - t_2)d$, cioè d divide *f-g*.
Viceversa preso un divisore $\delta \in \Delta$, si ha $f - g = \tau_1 \delta$, $g = \tau_2 \delta$. Allora $f = -g + g = \tau_1 \delta + \tau_2 \delta = (\tau_1 - \tau_2)\delta$, cioè δ divide *f*.

In particolare $MCD(f, g) = maxD = max\Delta$. E dunque $MCD(f, g) = MCD(f-g, g)$. Per di più, ponendo $f = q_0 g + r_0$, e applicando ripetutamente questo risultato otteniamo:
$MCD(f, g) = MCD(f - g, g) = MCD(f - 2g, g) = \cdots = MCD(f - q_0 g, g)$.
Dunque $MCD(f, g) = MCD(r_0, g)$ dove r_0 è il polinomio resto della divisione e si ha $deg\, r_0 < deg\, g$.

Teorema 4.3.8 Per ogni coppia di polinomi $f, g \in K[x]$ esiste l loro massimo comun divisore.
Dimostrazione Dati $f, g \in K[x]$, se uno dei due polinomi è il polinomio nullo la tesi segue banalmente: $MCD(f, 0) = f$. Evitiamo di studiare il caso in cui entrambi i polinomi sono nulli. Siano quindi $f, g \neq 0$. Possiamo applicare l'Osservazione precedente e ripercorrere, con le opportune accortezze, la dimostrazione dell'analogo Teorema 2.1.9. **E**.

Per proseguire in analogia con il capitolo 2 viene naturale enunciare i seguenti risultati:

Teorema 4.3.9 (Identità di Bezout) Siano $f, g \in K[x]$ e sia $d = MCD(f, g)$.

Allora esistono $\alpha, \beta \in K[x]$ tali che $d = \alpha f + \beta g$.

Teorema 4.3.10 In K[x] tutti gli ideali sono principali, cioè sono della forma $(f) = \{gf | g \in K[x]\}$ con $f \in K[x]$ ($K[x]$ è un PID).
Dimostrazione Sia $I \subset K[x]$ un ideale; $I \neq (0)$. Allora esiste un polinomio $g \in I$ tale che $g \neq 0$ e $deg\ g \leq deg\ f\ \ \forall f \in K[x]$ (questo perchè il grado di un polinomio è un numero naturale e dunque esiste un polinomio di grado minimo). Vogliamo osservare che $I = (g)$. Per la proprietà d'assorbimento degli ideali si ha naturalmente che $(g) \subseteq I$, resta da dimostrare che $I \subseteq (g)$. A tal fine prendiamo $h \in I$ e consideriamo la divisione di h per g: $h = qg + r$ con $deg\ r < deg\ g$. Siccome $h, g \in I$ abbiamo anche $r = h - qg \in I$. Per definizione r ha grado minore di g, il quale per costruzione ha grado minimo, dunque $r = 0$.

Teorema 4.3.11 Sia $f \in K[x]$ irriducibie $\Rightarrow f$ primo.
Dimostrazione **E**

Osservazione 4.3.12 i) Se A è un dominio d'integrità allora tutti e soli i polinomi unitari in A[x] sono quelli di grado 0. Infatti per definizione un polinomio $f \in A[x]$ è unitario se e solo se $\exists g \in K[x] | fg = 1$. Osservando che il polinomio 1 ha grado 0 e ricordando il Teorema 4.2.5 abbiamo che $deg(fg) = deg\ f + deg\ g = 0$ e ciò avviene se e solo se $deg\ f = deg\ g = 0$, essendo il grado di un polinomio un numero non negativo.
ii) Come conseguenza si ha che in A[x] tutti i polinomi di grado 1 sono irriducibili.
Tuttavia questi non sono necessariamente gli unici; si pensi ad esempio al polinomio $x^2 - 2 \in \mathbb{Q}[x]$. Esso ha grado 2, vogliamo mostare che è irriducibile.

Se per assurdo non fosse irriducibile esisterebbero due polinomi non invertibili f,g tali che $x^2 - 2 = fg$. Per il punto i) sappiamo che f,g hanno grado strettamente maggiore di 0. Ragionando sui gradi, essendo $\mathbb{Q}[x]$ un campo, si dovrà avere che f,g hanno entrambi grado 1. Potremmo dunque fattorizzare x^2-2 come prodotto di due polinomi di primo grado a coefficienti in $\mathbb{Q}$: $x^2 - 2 = (\alpha x+\beta)(\gamma x+\delta)$. Ricercando le radici del polinomio usando l'espressione a primo membro troviamo i numeri $\pm\sqrt{2}$, mentre ricercandole usando la fattorizzazione al secondo membro otteniamo $-\frac{\beta}{\alpha}, -\frac{\delta}{\gamma}$. Troviamo così che $\sqrt{2} \in \mathbb{Q}$; assurdo.

Definizione 4.3.13 Siano $f, g, h \in K[x]$ tre polinomi. Si dice che g *è congruo ad h modulo f* (e si scrive $g \equiv h_{mod\, f}$) se $\exists a \in K[x] \ : \ f \mid (g - h)$

Definizione 4.3.14 Due polinomi $f, g \in K[x]$ si dicono *coprimi* se $MCD(f, g)$ è un polinomio di grado 0, cioè una costante.

Osservazione 4.3.15 Da quanto ricavato fino ad ora possiamo dire che fissato un numero naturale n, un campo K e il corrispondente anello di polinomi $K[x]$ allora l'insieme $K_n[x] = \{f \in K[x] | deg\, f \leq n\}$ dei polinomi di $K[x]$ di grado minore o uguale ad n è un K-spazio vettoriale con la somma di $K[x]$ e il prodotto per uno scalare. Una sua base è formata dai vettori $(x^0, x, x^2, \ldots, x^{n-1})$.

4.4 Caratteristica di un anello e derivato di un polinomio

Definizione 4.4.1 Sia $(A, +, \cdot)$ un anello commutativo e unitario. Posto 1_A il neutro del prodotto si dice *caratteristica di A* l'ordine finito dell'elemento 1_A nel gruppo $(A, +)$, se tale ordine è invece infinito allora la caratteristica è 0.

Osservazione 4.4.2

i) Utilizzando la notazione additiva la caratteristica di $(A, +, \cdot)$ è il numero naturale $min\{n \in \mathbb{N} | n1_A = 1_A + 1_A + \cdots + 1_A = 0\}$, se tale numero non esiste allora la caratteristica è definita 0.

Osservazione 4.4.3 Sia $(A, +, \cdot)$ un anello commutativo unitario. Sia $\varphi : \mathbb{Z} \to A$ l'applicazione tale che $\varphi(n) = n1_A$. Si verifica che essa è un omomorfismo di anelli. Per il II Teorema di omomorfismo abbiamo che $\mathbb{Z}/_{ker\,\varphi} \simeq \varphi(\mathbb{Z}) \subseteq A$. Inoltre sappiamo che $ker\ \varphi$ è un ideale di $\mathbb{Z}$ ed è quindi della forma $ker\ \varphi = (n)$, dove $n \in \mathbb{N}$.

1) Se $ker\ \varphi = (0)$, cioè φ è iniettiva, allora la caratteristica di A è 0.

2) Se $ker\ \varphi \neq (0)$ allora $\exists m > 0 \in \mathbb{N}$ tale che $ker\ \varphi = (m)$ e quindi tale m è la caratteristica dell'anello A.

Osservazione 4.4.4

i) Da quanto discusso sopra otteniamo che un qualsiasi anello A, non necessariamente numerico, contiene nondimeno una copia isomorfa di $\mathbb{Z}$ o di $\mathbb{Z}_n$. Infatti per il II teorema di omomorfismo di anelli abbiamo che $\exists B \subseteq A | \, B \simeq$

$\mathbb{Z}/_{ker\,\varphi}$.

ii) Se K è un campo di caratteristica 0 allora contiene una copia isomorfa di $\mathbb{Z}$, inoltre per ogni elemento diverso da 0 esiste il suo inverso, in particolare attraverso l'isomorfismo che abbiamo individuato K conterrà anche gli inversi di $\mathbb{Z}$, il che comporta che se K è un campo d caratteristica 0 allora $\exists C$ insieme tale che $c \simeq \mathbb{Q} \wedge C \subseteq K$.

iii) Un anello di caratteristica 0 è necessariamente infinito in quanto contiene un insieme infinito.

Teorema 4.4.5 Se A è un dominio d'integrità allora la caratteristica di A è 0 o è un numero primo.

Dimostrazione Sia $r > 0$ la caratteristica di A. Se per assurdo r non fosse primo esso sarebbe prodotto di due numeri a,b non unitari e li supponiamo positivi. Per definizione di caratteristica si pone $r1 = (ab)1 = 0$. Notiamo che $(ab)1 = (a1)(b1) = 0$ e trovandoci in un dominio otteniamo $a1 = 0 \vee b1 = 0$. In entrambe i casi questo implica che la caratteristica di A non è r ma uno tra a,b i quali sono più piccoli, assurdo.

Corollario 4.4.6 Se K è un campo allora la sua caratteristica è 0 o è un numero primo. Infatti un campo è anche un dominio d'integrità.

Teorema 4.4.7 Se A è un anello commutativo unitario di caratteristica p primo allora $\forall a, b \in A$ vale $(a+b)^p = a^p + b^p$.

Dimostrazione Per la formula del binomio di Newton otteniamo $(a+b)^p = \sum_{k=0}^{p} \binom{n}{k} a^k b^{p-k}$. $\forall 1 \leq k \leq p-1$ si ha inoltre $p|\binom{p}{k}$ (Si veda Appendice), possiamo quindi dedurre che per $k \neq 0; k \neq p$ tutti gli addendi della somma sono divisibili per p. Trovandoci in un anello di caratteristica p ciò implica

che tali addendi si annullano. Abbiamo dunque $(a+b)^p = \binom{p}{0}a^0b^{p-0} + 0 + \cdots + 0 + \binom{p}{p}a^pb^{p-p} = a^p + b^p$.

Definizione 4.4.8 Sia K un campo di caratteristica p primo. L'applicazione $\varphi : K \to K$ definita da $\varphi(a) = a^p$ per ogni $a \in K$ si dice *omomorfismo di Frobenius.*

Osservazione 4.4.9

i) Grazie al Teorema 4.4.7 è facile verificare che φ è un omomorfismo di anelli: $\varphi(a+b) = (a+b)^p = a^p + b^p = \varphi(a) + \varphi(b)$ e anche $\varphi(ab) = (ab)^p = a^pb^p = \varphi(a)\varphi(b)$.

ii) In particolare $\varphi(1) = 1$ quindi possiamo dire che $ker\ \varphi \neq K$. Siccome il nucleo di φ è un ideale di K, per il Teorema 1.2.11 abbiamo che $ker\ \varphi = (0)$ e dunque φ è iniettiva.

Definizione 4.4.10 Se $\varphi : K \to K$ è un isomorfismo allora il campo K si dice *campo perfetto* e φ si dice *automorfismo di Frobenius.*

Osservazione 4.4.11 Un campo K è perfetto se e solo se $\forall b \in K\ \exists a \in K$ tale che $a^p = b$. In altre parole: Per ogni elemento in un campo perfetto esiste la sua radice p-esima.

Teorema 4.4.12 Se p è un numero primo allora $\mathbb{Z}_p$ è un campo perfetto e l'Automorfismo di Frobenius associato è l'identità.

Dimostrazione $\forall [a] \in \mathbb{Z}_p$ si ha che $\varphi([a]) = [a]^p$ e per il Piccolo teorema di Fermat (Osservazione 65 ii) $\varphi([a]) = [a]$.

Osservazione 4.4.13 Se K è un campo finito allora K è perfetto. Infatti

l'omomorfismo di Frobenius è sempre iniettivo e per una nota proprietà un endomorfismo iniettivo è anche suriettivo.

Definizione 4.4.14 Sia A[x] un anello di polinomi ed $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ appartenente ad $A[x]$. Il polinomio $Df = a_1 + 2a_2x + \cdots + na_nx^{n-1}$ si dice *derivato del polinomio f.*

Osservazione 4.4.15 L'usuale costruzione delle derivate fa uso della nozione di limite ed è quindi vincolata ad un ambiente metrico. Ponendo invece questa come definizione ed avendo in mente che ia_i significa $a_i + a_i + \cdots + a_i$ per i volte e + è la somma nell'anello A[x] possiamo generalizzare questa nozione ad un anello di polinomi qualsiasi.

Teorema 4.4.16 (Proprietà del derivato) Sia $A[x]$ è un anello di polinomi. Se $f, g \in A[x]$ allora:
i) $D(f + g) = Df + Dg$
ii) $D(f \cdot g) = Df \cdot g + f \cdot Dg$
iii) $D(f(g(x))) = Df(g(x))Dg(x)$

Dimostrazione (Abbozzo)
i) Si tratta di una semplice verifica
ii) Verifichiamo anzitutto la validità della formula per due monomi $f = a_nx^n$, $g = b_mx^m$. Per definizione di derivato abbiamo $D(f \cdot g) = D(a_nb_mx^{n+m}) = (n + m)a_nb_mx^{n+m-1}$. D'altra parte $Df \cdot g = na_nx^{n-1} \cdot b_x^m$ e $f \cdot Dg = a_nx^n mb_mx^{m-1}$. Si verifica che in questo caso vale effettivamente il punto ii).
Sia ora $f = a_0 + a_1x + \cdots + a_nx^n$ e $g = b_mx^m$. La tesi si prova per induzione

osservando che f è la somma dei due polinomi $f_1 = (a_0 + a_1x + \cdots + a_{n-1}x^{n-1})$ e $f_2 = a_nx^n$. Dunque per la proprietà distributiva $D(fg) = D((f_1 + f_2)g) = D(f_1g + f_2g)$ e per il punto i) otteniamo $D(f_1g + f_2g) = D(f_1g) + D(f_2g)$. Per il primo addendo si sfrutterà l'ipotesi induttiva mentre il secondo ha per fattori dei monomi e dunque la tesi sussiste. A questo punto si userà ancora l'induzione ponendo $f = f_1 + f_2$ e $g = b_0 + b_1x + \cdots + b_mx^m = g_1 + g_2$ e sfruttando quanto trovato fino ad ora.
iii) omessa.

Teorema 4.4.17 Sia K un campo e sia $f \in K[x]$ un polinomio tale che $Df = 0$, allora:
i) Se K ha caratteristica 0 allora f è un polinomio costante.
ii) Se K è perfetto di caratteristica p allora $\exists g \in K[x]$ tale che $f = g^p$.

Dimostrazione i) Sia $f = a_0 + \cdots + a_nx^n$ un polinomio in $K[x]$ e sia $Df = a_1 + \cdots + (n-1)a_{n-1}x^{n-2} + na_nx^{n-1} = 0$ il suo derivato. Per il Principio d'identità dei polinomi tutti i coefficienti di Df sono uguali a 0, otteniamo così le seguenti condizioni:
$a_1 = (1_A \cdot 1)a_1 = 0$
$2a_2 = (2 \cdot 1_A)a_2 = 0$
$\vdots$
$na_n = (n \cdot 1_A)a_n = 0$

Se K è un campo di caratteristica 0 allora i vari $i \cdot 1_A$ sono tutti diversi da 0, dunque trovandoci in un dominio dovremo avere $a_i = 0$; $\forall i \geq 1 \in \mathbb{N}$, l'unico termine non necessariamente nullo è così il solo termine noto a_0 e ciò prova che $f = a_0$ è un polinomio costante.

ii) Ragionando analogamente a quanto sopra otteniamo le condizioni:

$a_1 = (1_A \cdot 1)a_1 = 0$

$\vdots$

$pa_p = (p \cdot 1_A)a_p = 0$

$\vdots$

$2pa_{2p} = (2p \cdot 1_A)a_{2p} = 0$

$\vdots$

$mpa_{mp} = (mp \cdot 1_A)a_{mp} = 0$

$\vdots$

$na_n = (n \cdot 1_A)a_n = 0$

Se K è un campo di caratteristica p primo allora per ogni i che non sia multiplo di p il fattore $i \cdot 1_A$ è non nullo e quindi trovandoci in un dominio $[(i \cdot 1_A)a_i = 0 \wedge i \cdot 1_A \neq 0] \Rightarrow a_i = 0$. Per j multiplo di p invece il fattore $(j \cdot 1_A) = 0$ e ciò lascia privi di condizioni i rispettivi a_j. Dunque f sarà della forma $f = a_0 + a_p x^p + a_{2p} x^{2p} + \cdots + a_{mp} x^{mp}$. Se inoltre K è un campo perfetto allora esistono le radici p-esime, ovvero: $\exists b_0, b_1, \ldots, b_m | b_0^p = a_0$, $b_1^p = a_p$, $b_2^p = a_2 p, \ldots,$ $b_m^p = a_m p$. Il teorema 4.4.7 ci legittima a dire che il polinomio $g = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m$ è tale che $f = g^p$.

Teorema 4.4.18 Sia K un campo di caratteristica 0 oppure un campo perfetto di caratteristica p. Allora $f \in K[x]$ non costante ha fattori multipli (cioè è della forma $f = h^r k$) se e solo se $MCD(f, Df)$ non è un elemento unitario di $K[x]$.

Dimostrazione Sia $f \in K[x]$ avente fattori multipli, cioè $f = h^r k$ per qualche $h, k \in K[x]; r > 1 \in \mathbb{N}$. Calcolando il derivato di f otteniamo $Df =$

$rh^{r-1}Dh \cdot k + h^r \cdot Dk = h^{r-1}(rDh \cdot k + hDk)$. Facendo il massimo comun divisore tra $f = h^r k$ e $h^{r-1}(rDh \cdot k + hDk)$ tale polinomio non potrà essere costante (e quindi unitario) in quanto h^{r-1} è un fattore comune ad entrambi e quindi dividerà anche il loro MCD.
Viceversa sia $MCD(f, Df)$ non unitario, cioè un polinomio non costante. Trovandoci in un campo siamo in particolare in un dominio a fattorizzazione unica (Teorema 5.1.9) e quindi esiste un polinomio q irriducibile che divide il polinomio $MCD(f, Df)$, quindi dovrà essere $q|f$. Allora $f = qh$ e quindi per le proprietà del derivato $Df = Dq \cdot h + q \cdot Dh$. D'altra parte si ha anche $q|Df = Dq \cdot h + q \cdot Dh$. Naturalmente q divide il secondo addendo e così consegue che $q|Dq \cdot h$. Ma q è irriducibile e quindi anche primo, cioè $q|Dq \vee q|h$. Nel primo caso l'unica possibilità coerente con la condizione dei gradi $deg\, q > deg\, Dq$ è quella in cui Dq sia il polinomio nullo, allora:
(nell'ipotesi in cui K è un campo di caratteristica 0, per il Teorema * ii) q sarebbe costante e quindi non irriducibile, assurdo.
(Nell'ipotesi in cui K è un campo perfetto di caratteristica p, per il Teorema * i) $q = g^p$, quindi non irriducibile, assurdo.

In entrambi i casi rimane possibile solo che $q|h$, cioè $h = qk$ e si ha che $f = qh = q^2k$ e ciò soddisfa la tesi.

4.5 Quozienti di un anello di polinomi

Teorema 4.5.1 Sia K un campo e K[x] il rispettivo anello dei polinomi. Sia $f \in K[x]$ un polinomio di grado n e $(f) \subseteq K[x]$ un ideale. Allora

l'anello quoziente $K[x]/(f)$ è della forma $K[x]/(f) = \{[r]\,|deg\, r < deg\, f\}$. In particolare l'insieme $K[x]_f = \{g \in K[x]|deg\, g < deg\, f\}$ è in corrispondenza biunivoca con l'insieme $K[x]/(f)$.

Dimostrazione Per il Teorema 4.3.10 sappiamo che tutti gli ideali di K[x] sono principali. I quozienti di K[x] sono dunque della forma $K[x]/(f)$ e gli elementi sono le classi di resto dei polinomi nella divisione per *f*. Ricordando la divisione tra polinomi si ha che per ogni $g \in K[x]$ $\exists q, r \in K[x]$ (con $deg\, r < deg\, f$) tali che $g = qf + r$ e passando alle classi di equivalenza otteniamo $[g] = [qf + r] = [q][f] + [r] = [r]$. Osserviamo che $r \in K[x]$ è un rappresentante della classe di g di grado minore di f e che esso è l'unico tale rappresentante, ciò deriva dall'unicità del resto nella divisione per un polinomio. Dunque per ogni elemento in $K[x]/(f)$ è associato uno ed un solo polinomio di grado inferiore a quello di *f*.

Osservazione 4.5.2

i) Sia K un campo ed $f, f' \in K[x]$ due polinomi associati. Allora $K[x]/(f) = K[x]/(f')$. Ciò vale in particolare se uno dei due polinomi è monico.

ii) Sia $\varphi : K \to K[x]/(f)$ la funzione definita da $a \mapsto [a]$. Tale funzione è un monomorfismo, dunque $K \simeq \varphi(K)$ e possiamo identificare un elemento $[a] \in K[x]/(f)$ con l'elemento $a \in K$.

Teorema 4.5.3 Sia K un campo, $f \in K[x]$ un polinomio di grado n. Allora il quoziente $K[x]/(f)$ è uno spazio vettoriale di dimensione n.

Dimostrazione Sia $g \in K[x]$ un qualsiasi polinomio della forma $g = b_0 + b_1x + \cdots + b_mx^m$, con $m < n$. Allora $[g] = [b_0 + b_1x + \cdots + b_mx^m] = [b_0] + [b_1][x] + \cdots + [b_m][x^m]$. Per l'Osservazione 4.5.2 ii) ciò equivale a $[g] = b_0[1] + b_1[x] +$

$\cdots + b_m[x^m]$. Si verifica facilmente che $[1], [x], \ldots, [x^{n-1}]$ sono un sistema di generatori di $K[x]/(f)$. Al fine di vederne la lineare indipendenza poniamo una loro combinazione lineae pari a 0: $\lambda_0[1] + \lambda_1[x] + \cdots + \lambda_{n-1}[x^{n-1}] = [0]$. A tale successione di λ_i è associato uno ed un solo polinomio Λ di grado minore di quello di f, applicando il Teorema 4.5.1 otteniamo che $[\lambda_0 + \lambda_1 x + \cdots + \lambda_{n-1}x^{n-1}] = [0]$ se e solo se $\lambda_0 = \lambda_1 = \cdots = \lambda_{n-1} = 0$. In alternativa si può ragionare come segue: $[\lambda_0 + \lambda_1 x + \cdots + \lambda n - 1 x^{n-1}] = [0] \iff f|(\lambda_0 + \lambda_1 x + \cdots + \lambda n - 1 x^{n-1})$. Essendo $deg\,\Lambda < deg\,f$ ciò avviene se e solo se $\Lambda = 0$.

Teorema 4.5.4 Se K è un campo allora $K[x]/(f)$ è un campo se e solo se $f \in K[x]$ è un polinomio irriducibile (o primo).

Dimostrazione Sia $K[x]/(f)$ un campo. Se per assurdo f non fosse irriducibile esisterebbero due polinomi $g, h \in K[x]$ non unitari tali che $f = gh$. Per ipotesi $[f] = [gh] = [g][h] = 0$ e trovandoci in un campo otteniamo $[g] = 0 \vee [h] = 0$. Naturalmente $deg\,g < deg\,f$ e anche $deg\,h < deg\,f$ e ciò ci porta ad un assurdo. Viceversa se f è irriducibile, essendo K campo per il Teorema 4.3.11 $f \in K[x]$ è anche primo. Per qualunque polinomio $g \in K[x]$ (che non sia multiplo di f) si ha $MCD(f, g) = 1$. Sfruttando l'identità di Bezout si ha dunque che esistono $\alpha, \beta \in K[x]$ tali che $\alpha f + \beta g = 1$. Passando ora al quoziente otteniamo $[\alpha f + \beta g] = [\alpha f] + [\beta g] = [\beta g] = [\beta][g] = [1]$. Chiaramente $[\beta]$ è l'inverso di $g \in K[x]/(f)$. Per l'arbitrarietà di g abbiamo che per ogni elemento diverso da [0] in $K[x]/(f)$ esiste il suo inverso, cioè $K[x]/(f)$ è un campo.

Osservazione 4.5.4 Se $f \in K[x]$ è irriducibile allora l'ideale (f) è massimale.

D'altra parte in un $K[x]$ con K campo f è irriducibile se e solo se f è primo, ed f è primo se e solo se l'ideale (f) è primo. Dunque in $K[x]$ un ideale è primo se e solo se è massimale.

Teorema 4.5.5 (Teorema cinese dei resti per polinomi) Siano $m_1, \dots m_r \in K[x]$ polinomi a due a due coprimi. Siano inoltre $a_1, \dots a_r \in K[x]$ dei polinomi qualunque. Allora il sistema di congruenze nell'incognita t:

$$\begin{cases} t \equiv a_1 \mod m_1 \\ t \equiv a_2 \mod m_2 \\ \qquad\qquad \vdots \\ t \equiv a_r \mod m_r \end{cases}$$

ammette una soluzione T_1. Inoltre, se T_2 è un'altra soluzione si ha
$T_1 \equiv T_2 \mod M$ con $M = m_1 \cdot m_2 \cdot \dots \cdot m_r$.
Dimostrazione Analoga a quella del corrispondente teorema per gli interi.

Osservazione 4.5.6
i) Sia $m \in K[x]$ un polinomio della forma $m = x - \alpha$, con $\alpha \in K$. Allora $g \equiv h \mod m \iff (x-\alpha)|(g-h) \iff g(\alpha) = h(\alpha)$ (per il Teorema di Ruffini).
ii) Se $m_1 = (x-\alpha_1), \dots, m_k = (x-\alpha_k)$ allora m_i è coprimo con m_j se e solo se $\alpha_i \neq \alpha_j$.

Osservazione 4.5.7 Dall'Osservazione precedente possiamo formulare un

caso particolare del Teorema cinese dei resti:
Siano $\alpha_1, \dots \alpha_r \in K$ delle costanti tutte distinte. Siano inoltre $a_1, \dots a_r \in K[x]$ dei polinomi qualunque. Allora il sistema di uguaglianze nell'incognita t:

$$\begin{cases} t(\alpha_1) & = a_1(\alpha_1) \\ t(\alpha_2) & = a_2(\alpha_2) \\ & \vdots \\ t(\alpha_r) & = a_r(\alpha_r) \end{cases}$$

ammette una soluzione $T_1 \in K[x]$. Inoltre, se $T_2 \in K[x]$ è un'altra soluzione si ha $T_1 \equiv T_2 \ _{mod\, M}$ con $M = (x - \alpha_1) \cdot (x - \alpha_2) \cdot \dots \cdot (x - \alpha_r)$.

5 Fattorizzazione di polinomi, I Parte

5.1 Domini a fattorizzazione unica e l'anello $\mathbb{Z}[x]$

Definizione 5.1.1 Sia A un dominio d'integrità. Esso si dice *dominio a fattorizzazione unica* (in breve UFD) se $\forall a \in A; a \neq 0$ non unitario, esso è prodotto di elementi irriducibili e inoltre i fattori di tale prodotto sono unici a meno di permutazioni ed associati.
Quest'ultima condizione si esprime dicendo che se $a = f_1 f_2 \dots f_n = g_1 g_2 \dots g_m$ allora m=n ed esiste una permutazione σ tale che f_i è associato a $g_{\sigma(i)}$.

Ad esempio l'elemento $x^2 - 1 \in \mathbb{Q}[x]$ è un elemento che soddisfa le condizioni richieste: $x^2 - 1 = (x+1)(x-1) = (7x-7)(\frac{1}{7}x + \frac{1}{7})$. Gli elementi $(x-1), (7x-7)$ sono associati, come anche $(x+1)$ e $(\frac{1}{7}x + \frac{1}{7})$. (Più in generale vedremo che $\mathbb{Q}[x]$ è un dominio a fattorizzazione unica.)

Teorema 5.1.2 (Teorema fondamentale dell'aritmetica) Ogni numero naturale n è prodotto di un numero finito di numeri primi, inoltre tale fattorizzazione è unica a meno di permutazioni.
Dimostrazione Ricordando le Osservazioni 2.1.2, 2.1.5 e il Teorema 2.1.12 e osservando che $\mathbb{N} \subset \mathbb{Z}$ abbiamo che $p \in \mathbb{N}$ è primo se e solo se è irriducibile se e solo se esso è divisibile solamente per 1 e per se stesso. La dimostrazione procede per induzione completa su $a \in \mathbb{N}$. Sia $a > 1$, se esso è primo la tesi è banale. Viceversa supponiamo ci siano dei divisori di a; scriviamo $a = a_1 b$, con $a_1 < a; b < a$. Possiamo quindi applicare l'ipotesi induttiva e provare che a è prodotto di primi. Per dimostrare l'unicità supponiamo che

esista un elemento a che si può fattorizzare in due modi diversi. Poniamo $a = p_1p_2 \dots p_r = q_1q_2 \dots q_s$ con p_i, q_j primi. Posto $m = max\{r, s\}$ procediamo ancora per induzione su m. p_r è un divisore di a, quindi in particolare $p_r|q_1q_2 \dots q_s$. Essendo p_r un elemento primo che divide un prodotto, esso divide uno dei fattori, e siccome questi sono tutti primi otteniamo che $p_r = q_j$ per qualche j, ad esempio $p_r = q_s$. Tenendo a mente ciò possiamo cancellare p_r e q_s dai rispettivi membri dell'uguaglianza $p_1p_2 \dots p_r = q_1q_2 \dots q_s$ ottenendo $p_1p_2 \dots p_{r-1} = q_1q_2 \dots q_{s-1}$, il che riduce il valore di m e si può applicare l'ipotesi induttiva.

Teorema 5.1.3 $\mathbb{Z}$ è un dominio a fattorizzazione unica.

Dimostrazione Si ricordano di nuovo le Osservazioni 2.1.2, 2.1.5 e il Teorema 2.1.12. Sia $a \neq 0 \in \mathbb{Z}$ un elemento non unitario, dunque $|a| > 1$ e possiamo applicare il teorema precedente all'elemento $|a|$. Posto $|a| = p_1 \dots p_r$ possiamo dire che tali fattori sono primi, ovvero irriducibili, e positivi. Se a è maggiore di 0 allora si potrà cambiare il segno ad un numero pari di fattori tra $p_1, \dots, p_r$. Se a è negativo si potrà cambiare il segno ad un numero dispari di fattori tra $p_1, \dots, p_r$. In entrambi i casi la fattorizzazione è unica a meno dei segni dei fattori, per l'Osservazione 2.1.5 ciò significa che la fattorizzazione è unica a meno di elementi associati. $\mathbb{Z}$ è un UFD.

Teorema 5.1.9 Se K è un campo allora K[x] è un dominio a fattorizzazione unica.

Dimostrazione Sia $f \in K[x]$ un polinomio non nullo di grado $deg\ f \geq 1$. Vogliamo provare che f è prodotto di irriducibili in un unico modo a meno di permutazioni ed elementi associati.

Dimostriamo anzitutto che f può essere espresso attraverso un prodotto, la dimostrazione procede per induzione completa sul grado di f. Se $deg\ f = 1$ la tesi è banale essendo f irriducibile per il secondo punto dell'Osservazione 4.3.13. Sia ora f di grado n, se è irriducibile soddisfa la tesi, supponiamo dunque f non irriducibile.
(f irriducibile significa $\forall a, b \mid f = ab \Rightarrow \exists a^{-1} \vee \exists b^{-1}$; la sua negazione è dunque $\exists a, b \mid f = ab$; $\nexists a^{-1} \ \wedge \ \nexists b^{-1}$.)
Sia quindi $f = ab$, dove a,b non sono invertibili, cioè entrambi hanno grado maggiore o uguale ad 1.. Trovandoci in un campo dovremo avere inoltre $deg\, a < deg\, f$ e anche $deg\, b < deg\, f$; possiamo così applicare le ipotesi induttive ai polinomi a,b. Si ha che a,b sono prodotti di irriducibili, quindi anche $f = ab$ lo è.
Dimostriamo ora l'unicità: Sia $f = p_1 \dots p_r = q_1 \dots q_r$ con p_i, q_j elementi irriducibili. Sia $m = max\{r, s\}$ e procediamo per induzione su m. Consideriamo p_r, $p_r | f \Rightarrow p_r | q_1 \dots q_s$. Siccome K è un campo abbiamo che un elemento è irriducibile se e solo se è primo. Segue che se p_r divide un prodotto di fattori primi allora divide uno dei fattori, ad esempio q_s, ed in particolare $p_r = q_s$. Dunque $f = p_1 \dots p_r = q_1 \dots q_{s-1} p_r$ e cancellando p_r otteniamo un polinomio di grado minore di m; si conclude applicando l'ipotesi induttiva. In conclusione K[x] è un UFD.

Osservazione 5.1.5 Sia $f \in K[x]$, allora $\exists! u, q_1, \dots, q_r \in K[x]$ tali che $f = u q_1 \dots q_r$ con u unitario e q_i monico per ogni i. Inoltre tali q_i sono unici. Infatti dal Teorema precedente abbiamo $f = p_1 \dots p_r$; dove i polinomi p_i sono irriducibili. Ciascuno dei fattori p_i può essere riscritto come $p_i = u_i q_i$ dove u_i è un elemento unitario e q_i è monico e irriducibile. (In particolare

se $p_i = a_{0,i} + a_{1,i}x + \cdots + a_{n,i}x^n$ allora $u_i = a_{n,i}$ e $q_i = p_i u_i^{-1}$). Dunque $f = u_1 \dots u_r q_1 \dots q_r$. Il prodotto di unitari è ancora unitario, posto $u = u_1 \dots u_r$ abbiamo l'esistenza dei fattori. Per quanto riguarda l'unicità: il polinomio (costante) u è ovviamente unico, essendo tali i suoi fattori. Se esistesse un'altra scrittura di f: $f = uq_1 \dots q_r = t_1 \dots t_s$ avremmo che $r{=}s$ e che ogni q_i sarebbe associato ad un t_j, per il secondo punto dell'Osservazione 4.2.3 polinomi monici associati coincidono.

Osservazione 5.1.6 L'anello $\mathbb{Z}[x]$ non è un PID. Infatti, ad esempio, l'ideale $I = (2, x) = \{2f + xg | f, g \in \mathbb{Z}[x]\}$ (generato dal polinomio costante 2 e dal polinomio x) non è principale. Se per assurdo I fosse generato da un polinomio $h \in \mathbb{Z}[x]$ avremmo che $2 \in (h) = I$ ovvero $\exists k \in \mathbb{Z}[x] | 2 = hk$.
$\mathbb{Z}$ è un dominio d'integrità, e quindi per l'Osservazione 4.2.6 ii anche $\mathbb{Z}[x]$ è un dominio. Utilizzando il Teorema 4.2.5 possiamo dire che h deve avere grado 0. Si vede facilmente che h può essere soltanto -2,-1,1,2. Siccome gli ideali (-1) ed (1) coincidono, e anche (-2) e (2) coincidono possiamo limitarci a studiare i casi $h = 1, h = 2$.
Se $h = 1$ allora $I = (2, x) = (1) = \mathbb{Z}[x]$, che è assurdo.
Se $h = 2$ consideriamo il polinomio x, vorremmo che $x \in (2)$, cioè che esista un polinomio della forma $(\alpha + x\beta) \in \mathbb{Z}[x]$ tale che $x = 2(\alpha + x\beta) = 2\alpha + 2x\beta$. Si trova in pochi passaggi che $\beta = 2^{-1}$, assurdo essendo $\beta \in \mathbb{Z}$.

Definizione 5.1.7 Sia $f = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ un polinomio. Esso si dice *primitivo* se $MCD(a_0, a_1, \dots, a_n) = 1$, cioè se i suoi coefficienti sono coprimi tra loro.

Osservazione 5.1.8

i) $\mathbb{Z}[x] \subset \mathbb{Q}[x]$; dunque un polinomio $f \in \mathbb{Z}[x]$ può anche essere interpretato come appartenente a $\mathbb{Q}[x]$. Se $f \in \mathbb{Q}[x]$ ha coefficienti interi lo possiamo interpretare come appartenente a $\mathbb{Z}[x]$.
ii) Se $f = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Q}[x]$ ha coefficienti interi allora f si può fattorizzare come prodotto di un polinomio unitario e di un polinomio primitivo ponendo $\eta = MCD(a_0, a_1, \ldots, a_n)$ e scrivendo $f = \eta f_1$, dove f_1 è primitivo per costruzione ed è associato ad f.
iii) Per ogni $f \in \mathbb{Q}[x]$ esiste un polinomio primitivo g ad esso associato. Infatti se $f = \frac{N_0}{D_0} + \frac{N_1}{D_1}x + \cdots + \frac{N_n}{D_n}x^n$ è un polinomio a coefficienti razionali allora posti $\delta = (D_0D_1 \ldots D_n)$ il prodotto dei denominatori ed $\eta = MCD(N_0, N_1, \ldots, N_n)$ possiamo scrivere $f = \frac{\delta}{\eta}f_1$ dove il polinomio $\frac{\delta}{\eta}$ è unitario mentre $f_1 = \frac{\eta}{\delta}f$ è primitivo per costruzione.

Teorema 5.1.9 Se $f, g \in \mathbb{Q}[x]$ sono due polinomi primitivi allora il polinomio fg è primitivo.

Dimostrazione Se per assurdo fg non fosse primitivo avremmo che il massimo comun divisore dei suoi coefficienti (che sono numeri interi) è maggiore di 1, in particolare esisterebbe un numero primo p che divide tutti i coefficienti di *fg*. Con l'aiuto del Corollario 4.2.9 definiamo l'omomorfismo $\phi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ tale che $\phi(a) = [a]; \forall a \in \mathbb{Z}$ e $\phi(x) = x$ di modo che $\phi(a_0 + a_1x + \cdots + a_nx^n) = [a_0] + [a_1]x + \cdots + [a_n]x^n$. Siccome abbiamo supposto che i coefficienti di *fg* sono divisibili per p otteniamo $\phi(fg) = \phi(f)\phi(g) = [0]$. Ricordando l'Osservazione 62.iii abbiamo che $\mathbb{Z}_p$ è un campo e per l'Osservazione 4.2.6 ii) $\mathbb{Z}_p[x]$ è un dominio. Dunque se $\phi(f)\phi(g) = 0 \Rightarrow \phi(f) = 0 \vee \phi(g) = 0$ ma ciò è assurdo in quanto ciò comporterebbe che i coefficienti di uno dei due polinomi siano tutti divisibili per p, contraddicendo l'ipotesi *f,g* primitivi.

Teorema 5.1.10 (Lemma di Gauss) Sia $f \in \mathbb{Q}[x]$ a coefficienti interi, $deg f \geq 1$. Se $f = ab$ allora $\exists a_1, b_1$ polinomi a coefficienti interi tali che $f = a_1 b_1$, con a, a_1 e b, b_1 associati.

Dimostrazione Supponiamo anzitutto che f sia primitivo. Poniamo $f = ab$ con $a, b \in \mathbb{Q}[x]$, per il terzo punto dell'Osservazione 5.1.8 abbiamo che $\exists \alpha, \beta \in \mathbb{Z}[x]$ primitivi e $\exists r, s \in \mathbb{Q}[x]$ invertibili tali che $a = r\alpha$; $b = s\beta$. In particolare a è associato ad α e b è associato a β. Abbiamo quindi $f = rs\alpha\beta$. Per il Teorema precedente il prodotto $\alpha\beta$ è primitivo, f lo è per ipotesi e quindi affinchè l'uguaglianza sia coerente dovremo avere $rs = \pm 1$. Posto $a_1 = rs\alpha$, $b_1 = \beta$ otteniamo la tesi.

Se f non è primitivo invece possiamo applicare il procedimento esposto nell'Osservazione 5.1.8 ii e scrivere $f = \delta f_1$ con $\delta \in \mathbb{Z}[x]$ polinomio invertibile (quindi una costante) e $f_1 \in \mathbb{Z}[x]$ primitivo. Abbiamo $f = ab = df_1$, quindi $f_1 = abd^{-1}$ ed essendo f_1 primitivo possiamo ricondurci a quanto visto sopra e affermare che $\exists a_1, b_1 \in \mathbb{Z}[x]$ associati a $\frac{1}{d}a$ e b rispettivamente tali che $f_1 = a_1 b_1$. Segue che $f = da_1 b_1$, essendo tutti fattori interi abbiamo $da_1, b_1 \in \mathbb{Z}[x]$ soddisfano la tesi.

Corollario 5.1.11 Sia $f \in \mathbb{Z}[x]$ primitivo di grado strettamente maggiore di 0, allora f è irriducibile in $\mathbb{Z}[x]$ se e solo se lo è in $\mathbb{Q}[x]$.

Dimostrazione Supponiamo che f sia irriducibile in $\mathbb{Z}[x]$ e poniamo $f = ab \in \mathbb{Q}[x]$, vogliamo provare che a è unitario o b è unitario. Per il lemma di Gauss esistono $a_1, b_1 \in \mathbb{Z}[x]$ associati ad a,b tali che $f = a_1 b_1 \in \mathbb{Z}[x]$, qui il polinomio è irriducibile e quindi $a_1 = \pm 1 \vee b_1 = \pm 1$ (unici elementi invertibili in $\mathbb{Z}[x]$), sia ad esempio a_1 unitario, esso è associato ad a, dunque pure a è

unitario. Viceversa se f è irriducibile in $\mathbb{Q}[x]$ e ricordando che $\mathbb{Z}[x] \subset \mathbb{Q}[x]$ abbiamo subito che $f \in \mathbb{Z}[x]$ è irriducibile.

Lemma 5.1.12 Sia $f \in \mathbb{Z}[x]$ un polinomio primitivo. Allora $\exists q_1, \ldots, q_r \in \mathbb{Z}[x]$ irriducibili tali che $f = q_1 \ldots q_r$. Inoltre se $\exists t_1 \ldots t_s \in \mathbb{Z}[x]$ primitivi tali che $f = t_1 \ldots t_s$ allora $r = s$ e i polinomi q_i, t_i sono uguali a meno di segno e permutazioni.

Dimostrazione Interpretiamo f come appartenente a $\mathbb{Q}[x]$, per il Teorema 5.1.9 $\mathbb{Q}[x]$ è un UFD e possiamo quindi porre $f = \overline{q_1} \ldots \overline{q_r}$ dove i polinomi $\overline{q_i} \in \mathbb{Q}[x]$ sono irriducibili. Per il lemma di Gauss $\exists q_1, \ldots, q_r \in \mathbb{Z}[x]$ associati a $\overline{q_1}, \ldots, \overline{q_r}$ tali che $f = q_1..q_r$. Essendo f primitivo dovremo avere $q_1, \ldots, q_r$ primitivi ed essendo questi associati a polinomi irriducibili lo sono anch'essi. Dall'unicità della fattorizzazione in $\mathbb{Q}[x]$ discende quella in $\mathbb{Z}[x]$, a meno di permutazioni ed elementi associati, polinomi associati in $\mathbb{Z}[x]$ differiscono soltanto dal segno.

Teorema 5.1.13 L'anello dei polinomi $\mathbb{Z}[x]$ è un dominio a fattorizzazione unica.

Dimostrazione Sia $f \in \mathbb{Z}[x]$. Se f è una costante ci riconduciamo al Teorema 5.1.3, altrimenti per l'Osservazione 5.1.8 ii possiamo porre $f = df_1$ con $d \in \mathbb{Z}; f_1$ primitivo e per il lemma precedente abbiamo che f_1 si fattorizza attraverso i polinomi $q_1, \ldots, q_r$ irriducibili in $\mathbb{Z}[x]$ mentre d è una costante e si fattorizza attraverso i numeri primi irriducibili $p_1, \ldots, p_s$. Dunque $f = p_1 \ldots p_s q_1 \ldots q_r$ è fattorizzato in modo unico a meno di permutazioni ed associati (ovvero segni). $\mathbb{Z}[x]$ è un UFD.

5.2 Fattorizzazione di polinomi a coefficienti in $\mathbb{R}$ e $\mathbb{C}$

Fattorizzazione in $\mathbb{C}[x]$

(Si danno per note le proprietà di base dei numeri complessi.)

Teorema 5.2.1 (Teorema degli zeri) Se $f : [a, b] \to \mathbb{R}$ è una funzione continua e $f(a) < 0; f(b) > 0$ allora $\exists \xi \in (a, b)$ tale che $f(\xi) = 0$

Corollario 5.2.2 Un polinomio $f \in \mathbb{R}[x]$ di grado dispari ha almeno una radice. Infatti per $a < 0$ sufficientemente piccolo e per $b > 0$ sufficientemente grande si avrà $f(a) < 0, f(b) > 0$, si può così applicare il teorema degli zeri.

Teorema 5.2.3 (Teorema fondamentale dell'algebra) Se $f \in \mathbb{C}[x]$ allora $\exists a \in \mathbb{C}$ tale che $f(a) = 0$.

Dimostrazione (Cenno) Come si saprà $\mathbb{C} \simeq \mathbb{R}^2$, così $f \in \mathbb{C}[x]$ può essere pensato come appartenente a $\mathbb{R}^2[x]$. Sia $a_0 \in \mathbb{R}^2$; consideriamo $f(a_0) = (x_0, y_0)$. Consideriamo poi una serie di circonferenze concentriche $\gamma_0, \gamma_1, \ldots, \gamma_n, \ldots$ centrate in a_0 di raggi $r_0 < r_1 < \cdots < r_n < \ldots$.

Essendo f un polinomio se esso viene pensato come funzione risulta continuo e quindi $f(\gamma_i)$ risulterà essere una curva chiusa e al crescere di i, queste curve saranno via via più distanti dal punto $f(x_0, y_0)$. In particolare per r_i sufficientemente grande esisterà un punto (x_1, y_1) di coordinate di segno opposto a quelle di $f(a_0) = (x_0, y_0)$. Quindi per qualche punto a_1 si avrà $f(a_1) = (0, 0)$.

Un bel video su questa dimostrazione

Osservazione 5.2.4 Se $f \in \mathbb{C}[x]$; $deg\, f \geq 1$ allora per il teorema precedente

$\exists a_1 \in \mathbb{C}$ tale che $f(a_1) = 0$ e per il Teorema 4.3.2 $\exists f_1 \in \mathbb{C}[x]$, di grado $deg\ f_1 = deg\ f - 1$ tale che $f(x) = f_1(x)(x - a_1)$. Se f_1 ha grado maggiore di 0 potremo riapplicare il teorema ottenendo $f = f_2(x)(x - a_1)(x - a_2)$. Iterando questo processo finchè il grado di f_i scenderà a 0 otteniamo $f = f_i(x-a_1)(x-a_2)\dots(x-a_i)$ dove $f_i \in \mathbb{C}$ è un polinomio costante. Si ottiene così che ogni polinomio appartenente a $\mathbb{C}[x]$ può essere fattorizzato attraverso polinomi di grado 1, che sono dunque gli unici elementi irriducibili in $\mathbb{C}[x]$.

Teorema 5.2.5 Se $f(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{C}[x]$ ha una radice della forma $\alpha + i\beta$ allora anche il suo coniugato $\alpha - i\beta$ è radice di *f*.
Dimostrazione Per ipotesi abbiamo $f(\alpha+i\beta) = a_0+a_1(\alpha+i\beta)+\dots+a_n(\alpha+i\beta)^n = 0$. Coniugando ambo i membri dell'uguaglianza questa sussiste. Il coniugato di 0 è se stesso, a secondo membro, sfruttando le proprietà dei coniugati, otteniamo che $\overline{\alpha + i\beta} = \alpha - i\beta$ è radice di *f*.

Fattorizzazione in $\mathbb{R}[x]$

Osservazione 5.2.6

i) $\mathbb{R}[x] \subset \mathbb{C}[x]$.
ii)Il polinomio $x^2+1 \in \mathbb{R}[x]$ è irriducibile (se fosse riducibile avremmo $\sqrt{-1} \in \mathbb{R}$).
iii) Più in generale abbiamo che un polinomio $ax^2 + bx + c$ di grado 2 è irriducibile in $\mathbb{R}[x]$ se e solo se il suo discriminante $b^2 - 4ac$ è minore di 0.
iv) Per il Corollario 5.2.2 e il Teorema 4.3.2 un polinomio di grado dispari è riducibile.

Teorema 5.2.7 Un polinomio $f \in \mathbb{R}[x]$ di grado maggiore di 2 è riducibile.
Dimostrazione Per induzione completa sul grado di f: Per il punto iv) dell'Osservazione precedente se f ha grado 3 la tesi sussiste. Sia $f \in \mathbb{R}[x]$ di grado maggiore di 3. Per l'Osservazione 5.2.6 i) lo possiamo pensare appartenente a $\mathbb{C}[x]$ e per i Teoremi 5.2.3, 5.2.5 esso ha due radici coniugate in $\mathbb{C}[x]$, possiamo dunque applicare il procedimento illustrato nell'Osservazione 5.2.4 ottenendo $f(x) = f_1(x)(x - (\alpha + i\beta))(x - (\alpha - i\beta))$ con $f_1(x) \in \mathbb{C}[x]$. Notiamo che $(x-(\alpha+i\beta))(x-(\alpha-i\beta)) = x^2-2\alpha x+\alpha^2+\beta^2 \in \mathbb{R}[x]$ e che tale polinomio divide f, siccome la divisione di due polinomi a coefficienti reali è ancora un polinomio a coefficienti reali e $f_1(x)$ è il risultato di tale divisione possiamo concludere che $f_1(x) \in \mathbb{R}[x]$. Tale polinomio ha naturalmente grado minore di f, possiamo applicare l'ipotesi induttiva.

6 Fattorizzazione di polinomi a coefficienti in $\mathbb{Z}$ e $\mathbb{Q}$

6.1 Elementi irriducibili in $\mathbb{Z}[x]$ e $\mathbb{Q}[x]$, Criterio di Eisenstein

Teorema 6.1.1 Sia $f \in \mathbb{Q}[x]$, sia $g(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ il polinomio primitivo associato ad f. Se il numero razionale (ridotto ai minimi termini) $\frac{p}{q}$ è radice di f,g allora $p|a_0$ e $q|a_n$.

Dimostrazione Per l'Osservazione 5.1.8 iii) e il Teorema 5.1.10 possiamo ri-

condurci ad un polinomio a coefficienti interi $g(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$. Supponiamo che esista un numero razionale $\frac{p}{q}$ ridotto ai minimi termini che sia radice del polinomio g, ovvero $g(\frac{p}{q}) = a_0 + a_1\frac{p}{q} + \cdots + a_n(\frac{p}{q})^n = 0$. Moltiplicando ambo i membri per q^n si ottiene $a_0q^n + a_1pq^{n-1} + \cdots + a_{n-1}p^{n-1}q + a_np^n = 0$.

Mettendo in evidenza il fattore q a primo membro otteniamo $q(a_0q^{n-1} + a_1pq^{n-2} + \cdots + a_{n-1}p^{n-1}) = -a_np^n$. I numeri p,q sono coprimi (in quanto abbiamo supposto $\frac{p}{q}$ ridotta ai minimi termini), dunque q è coprimo anche con p^n, si deve dunque avere che $q|a_n$.

In modo analogo, mettendo in evidenza il fattore p otteniamo $p(a_1q^{n-1} + \cdots + a_{n-1}p^{n-2}q + a_np^{n-1}) = -a_0q^n$ troviamo che $p|a_0$.

Osservazione 6.1.2 Quello esposto nel Teorema precedente è un criterio necessario per avere radici razionali di un polinomio, ma non sufficiente. Si pensi ad esempio al polinomio $x^2 + 1$: il criterio ci suggerisce che le possibili radici razionali sono ± 1 ma nessuna di esse annulla il polinomio.

Inoltre applicare tale criterio può richiedere molto tempo, si pensi ad esempio al semplice polinomio $2x^3+x^2+x-15$ o al polinomio $x^2+x+135465864235654$: Nel primo caso se esiste una radice razionale $\frac{p}{q}$ di tale polinomio si dovrà avere $p \in \{-15, -5, -3, -1, 1, 3, 5, 15\}$ e $q \in \{-2, -1, 1, 2\}$. Le candidate radici razionali sono quindi i numeri $\pm\frac{1}{1}, \pm\frac{3}{1}, \pm\frac{5}{1}, \pm\frac{15}{1}, \pm\frac{1}{2}, \pm\frac{3}{2}, \pm\frac{5}{2}, \pm\frac{15}{2}$. Si dovranno verificare una ad una prima di concludere che $\frac{3}{2}$ è l'unica radice razionale del polinomio.

Nel secondo caso la fattorizzazione del termine noto richiederà un po' di tempo e si dovranno poi verificare uno ad uno i possibili candidati (per altro senza nemmeno la certezza di trovare una radice tra essi).

Teorema 6.1.3 (Criterio di irriducibilità di Eisenstein)
Sia $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ un polinomio primitivo di grado almeno 2. Se $\exists p$ numero primo tale che:

i) $p|a_0, a_1, \ldots, a_{n-1}$,

ii) $p \nmid a_n$,

iii) $p^2 \nmid a_0$

allora f è irriducibile.

Dimostrazione (Abbozzo) Sia $f = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ un polinomio primitivo di grado $n \geq 2$ e p un numero primo che soddisfi le condizioni i), ii), iii). Supponiamo per assurdo che f sia prodotto di due polinomi non unitari (quindi di grado maggiore di 0) $b_0 + b_1x + \cdots + b_rx^r$ e $c_0 + c_1x + \cdots + c_sx^s$ e supponiamo senza perdita di generalità $r \geq s$. Trovandoci in un dominio poniamo inoltre $n = r + s$. Da come è definito il prodotto di polinomi otteniamo le seguenti uguaglianze:

$$a_0 = b_0c_0$$
$$a_1 = b_0c_1 + b_1c_0$$
$$a_2 = b_0c_2 + b_1c_1 + b_2c_0$$
$$\vdots$$
$$a_{n-1} = b_{r-1}c_s + b_rc_{s-1}$$
$$a_n = b_rc_s$$

Per la condizione i) poniamo:

$p|b_0c_0$

$p|b_0c_1 + b_1c_0$

$p|b_0c_2 + b_1c_1 + b_2c_0$

$\vdots$

$p|b_{r-1}c_s + b_r c_{s-1}$

Se $p|b_0c_0$ allora $p|b_0$ oppure $p|c_0$; supponiamo $p|b_0$. Per la condizione iii) e per quanto abbiamo supposto otteniamo inoltre $p \nmid c_0$.

Siccome $p|b_0 \Rightarrow p|b_0c_1$ allora $[p|b_0c_1 + b_1c_0] \Rightarrow p|b_1c_0$. Abbiamo già osservato che $p \nmid c_0$ e concludiamo così che $p|b_1$.

$[(p|b_0c_2 + b_1c_1 + b_2c_0) \wedge p|b_0 \wedge p|b_1] \Rightarrow p|b_2c_0$.
$[p|b_2c_0 \wedge p \nmid c_0] \Rightarrow p|b_2$.

In generale proseguendo troviamo che $p|b_0, b_1, \ldots, b_{r-1}, b_r$. Il fatto che $p|b_r$ è però una contraddizione con la condizione ii) in quanto $a_n = b_r c_s$ sarebbe divisibile per p.

Corollario 6.1.4 Negli anelli dei polinomi a coefficienti in $\mathbb{Z}$ e $\mathbb{Q}$ esistono infiniti polinomi irriducibili per qualunque grado maggiore di 0.
Dimostrazione Per il Criterio di Eisenstein i polinomi della forma $x^n + p$ con p primo sono irriducibili in $\mathbb{Z}[x]$ (e quindi anche in $\mathbb{Q}[x]$, per il Corollario 5.1.11), dunque in $\mathbb{Z}[x]$ ed in $\mathbb{Q}[x]$ esistono polinomi irriducibili di qualunque grado maggiore o uguale a 2. Per di più ricordando che esistono infiniti numeri primi e che polinomi di primo grado sono sempre irriducibili si ottiene la tesi.

Osservazione 6.1.5 Il criterio di Eisenstein è una condizione sufficiente ma non necessaria, ad esempio il polinomio $x^2 + 1$ è irriducibile in $\mathbb{Z}[x]$ ma non lo si può verificare tramite il criterio.

6.2 Fattorizzazione in $\mathbb{Z}_p[x]$

6.2.1 I e II teorema di Berlekamp

Osservazione 6.2.1.1

i) Siano $a, b \in \mathbb{Z}_p[x]$ due polinomi coprimi. Sia $f \in \mathbb{Z}_p[x]$ un polinomio. Allora $MCD(f, ab) = MCD(f, a) \cdot MCD(f, b)$.

ii) Il polinomio $f = (x^p - x) \in \mathbb{Z}_p[x]$ ha per zeri tutti gli elementi di $\mathbb{Z}_p$. Infatti per il Piccolo teorema di Fermat abbiamo che $a^p \equiv a_{mod\, p}$; $\forall a \in \mathbb{Z}$ e dunque $f(a) = a^p - a_{mod\, p} = 0_{mod\, p}$. Come conseguenza abbiamo la fattorizzazione $f = x(x-1)(x-2)\dots(x-p+1)$.

iii) Sia $g \in \mathbb{Z}_p[x]$ un polinomio. Allora per il Teorema di estensione 4.2.8 $F : \mathbb{Z}_p[x] \to \mathbb{Z}_p[x]$ tale che $x \mapsto g(x)$; $a \mapsto a; \forall a \in \mathbb{Z}_p$ definisce un omomorfismo di anelli. Dal punto precedente sappiamo che $x^p - x = x(x-1)\dots(x-p+1)$; considerando la sua immagine attraverso l'omomorfismo F otteniamo che $g^p - g = g(g-1)\dots(g-p+1)$

iv) I polinomi $(g-i), (g-j)$ sono coprimi per ogni $i \neq j$ (con $i, j \in \{0, 1, \dots, p-1\}$). Infatti per l'Osservazione 4.3.7 $MCD(g-i, g-j) = MCD(g-i-(g-j), g-j) = MCD(j-i, g-j)$ ed essendo j-i una costante non nulla allora anche il massimo comun divisore non può essere altro che una costante.

Teorema 6.2.1.2 (I teorema di Berlekamp) Sia $f \in \mathbb{Z}_p[x]$ di grado d. Sia $g \in \mathbb{Z}_p[x]$ tale che $1 \leq deg\, g < deg\, f = d$ e tale che $f | (g^p - g)$. Allora $f = MCD(f, g) \cdot MCD(f, g-1) \cdot \dots \cdot MCD(f, g-p+1)$ e tale fattorizzazione di f è effettiva, ovvero ci sono fattori non costanti e di grado minore di

d.

Dimostrazione Siccome $f|(g^p - g)$ allora $MCD(f, g^p - g) = f$. D'altra parte ricordando l'Osservazione 6.2.1.1 il polinomio $g^p - g$ si può fattorizzare come $g(g-1)\dots(g-p+1)$ per il punto iii) e tali fattori sono coprimi per il punto iv). Siamo quindi nella condizione di poter applicare il punto i) imponendo $MCD(f, g^p - g) = f = MCD(f, g) \cdot MCD(f, g-1) \cdot \dots \cdot MCD(f, g-p+1)$. Per dimostrare che la fattorizzazione è propria basta osservare che per ipotesi $deg g < deg f$ e dunque i polinomi $MCD(f, g), MCD(f, g-1), \dots, MCD(f, g-p+1)$ avranno tutti grado minore di d=$deg\ f$ (quindi in particolare nessuno di essi coincide con f); non possono essere tutti di grado 0 in quanto ci troviamo in un campo, il grado di un prodotto è pari alla somma dei gradi dei fattori ed f ha grado maggiore di 0.

Osservazione 6.2.1.3

i) Se f è un polinomio irriducibile il teorema precedente non si può applicare in quanto la condizione $1 \leq deg\ g \leq d-1$ limita il campo di applicazione di questo teorema a polinomi riducibili. (In altre parole: Se f è irriducibile non esiste alcun g non costante che soddisfa le condizioni richieste). Naturalmente se ammettessimo che g possa essere di grado 0, per il Piccolo teorema di Fermat avremmo $g^p - g = 0 \in \mathbb{Z}_p$ per ogni costante $g \in \mathbb{Z}_p$. Allora $f|(g^p - g)$ è equivalente a dire $f|0$ (il che è sempre vero) ma la tesi invece non viene soddisfatta per f irriducibili in quanto troveremmo una fattorizzazione di f attraverso polinomi tutti di grado 0 così che anche f avrà grado 0 ed in contraddizione con l'ipotesi di irriducibilità, e l'ipotesi $deg\ g \leq deg\ f - 1$.

ii) Questa fattorizzazione non è necessariamente fatta tramite polinomi irriducibili ma solo di grado più basso rispetto a quello di partenza d, si potrà

eventualmente riapplicare questo risultato ai fattori che esprimono f.

Dato $f \in \mathbb{Z}_p[x]$ vediamo ora come trovare $g \in \mathbb{Z}_p[x]$ di modo da poter applicare il primo teorema di Berlekamp.
Anzitutto fissiamo $f \in \mathbb{Z}_p[x]$ di grado $deg\ f = d$ e imponiamo la condizione $deg\ g < d$ (omettiamo per ora la condizione $1 \leq deg\ g$ di modo da poter proseguire, si imporrà successivamente una condizione analoga), dunque g sarà della forma $g = b_0 + b_1x + \cdots + b_{d-1}x^{d-1}$. Per il Principio d'identità dei polinomi trovare g è equivalente a trovare i suoi coefficienti b_j, che quindi saranno le nostre incognite nella trattazione. Vogliamo poi che g soddisfi la condizione $f|(g^p - g)$, quindi per cominciare cerchiamo un'espressione del polinomio $(g^p - g)$ in funzione delle incognite $b_0, \ldots, b_{d-1}$.
$g^p - g = (b_0 + b_1x + \cdots + b_{d-1}x^{d-1})^p - (b_0 + b_1x + \cdots + b_{d-1}x^{d-1})$. Trovandoci in un campo di caratteristica p primo possiamo sfruttare il Teorema 4.4.7 ottenendo $g^p - g = b_0^p + (b_1x)^p + \cdots + (b_{d-1}x^{d-1})^p - (b_0 + b_1x + \cdots + b_{d-1}x^{d-1})$. Applicando il Piccolo teorema di Fermat (Osservazione 65 ii) ci riconduciamo all'equazione $g^p - g = b_0 + b_1 \cdot x^p + \cdots + b_jx^jp + \cdots + b_{d-1}x^{p(d-1)} - (b_0 + b_1x + \cdots + b_jx^j + \cdots + b_{d-1}x^{d-1})$.

Il nostro obiettivo è dividere tale polinomio per f. A tale scopo osserviamo che i monomi b_0, b_1x, $\ldots$, b_jx^j, $\ldots$, $b_{d-1}x^{d-1}$ hanno tutti grado minore di d e quindi effettuando la loro divisione per f otteniamo $b_jx^j = f \cdot 0 + b_j$. Ci restano da considerare ora i soli $x^{jp}_{(j=0,1,\ldots,d-1)}$ e li dividiamo per f ottenendo le condizioni $x^{jp} = (q_jf + r_j)$ al variare di j. (Con $r_j \in \mathbb{Z}_p[x]$ tutti di grado minore di d. In seguito li scriveremo in forma estesa con un doppio indice).

Possiamo dunque porre $g^p - g = [(b_j(q_jf + r_j)) - (b_j)]_{j=0,1,\ldots,d-1)}$ oppure per

esteso

$b_0r_0 + b_1(q_1f + r_1) + \cdots + b_j(q_jf + r_j) + \cdots + b_{d-1}(q_{d-1}f + r_{d-1}) - (b_0 + b_1x + \cdots + b_{d-1}x^{d-1})$.

Manipolando questa uguaglianza (sfruttando in particolare la distributività) otteniamo che $g^p - g$ è uguale a

$f(b_0q_0 + \cdots + b_{d-1}q_{d-1}) + b_0r_0 + b_1r_1 + \cdots + b_{d-1}r_{d-1} - b_0 - b_1x - \cdots - b_{d-1}x^{d-1}$

Notiamo che abbiamo così scritto $g^p - g$ nella forma $fq + r$.

Come già osservato i polinomi resto $r_j \in \mathbb{Z}_p[x]$ hanno tutti grado al più $d-1$, scrivendoli in forma estesa sfruttando un doppio indice (il primo indica la successione dei coefficienti, il secondo indica il polinomio r_j che si sta considerando) otteniamo

$r_0 = r_{0,0} + r_{1,0}x + \cdots + r_{d-1,0}x^{d-1}$

$r_1 = r_{0,1} + r_{1,1}x + \cdots + r_{d-1,1}x^{d-1}$

$\vdots$

$r_{d-1} = r_{0,d-1} + r_{1,d-1}x + \cdots + r_{d-1,d-1}x^{d-1}$

(Dove $r_{i,j} \in \mathbb{Z}_p$ sono i coefficienti i-esimi del polinomio resto j-esimo (della divisione di x^{jp} per f)).

Sostituendo questa scrittura estesa a quella compatta otteniamo che $r =$

$b_0(r_{0,0} + r_{1,0}x + \cdots + r_{d-1,0}x^{d-1}) +$

$b_1(r_{0,1} + r_{1,1}x + \cdots + r_{d-1,1}x^{d-1}) +$

$\cdots +$

$b_{d-1}(r_{0,d-1} + r_{1,d-1}x + \cdots + r_{d-1,d-1}x^{d-1}) +$

$$- b_0 - b_1 x - \cdots - b_{d-1} x^{d-1}$$

e sfruttando la distributività

$r = b_0(r_{0,0} - 1 + r_{1,0}x + \cdots + r_{d-1,0}x^{d-1}) +$

$b_1(r_{0,1} + (r_{1,1} - 1)x + \cdots + r_{d-1,1}x^{d-1}) +$

$\cdots +$

$b_{d-1}(r_{0,d-1} + r_{1,d-1}x + \cdots + (r_{d-1,d-1} - 1)x^{d-1})$ ed infine

$r = (b_0(r_{0,0} - 1) + b_1 r_{0,1} + \cdots + b_{d-1} r_{0,d-1})x^0 +$

$(b_0 r_{1,0} + b_1(r_{1,1} - 1) + \cdots + b_{d-1} r_{1,d-1})x +$

$\ldots +$

$(b_0 r_{d-1,0} + b_1 r_{d-1,1} + \cdots + b_{d-1}(r_{d-1,d-1} - 1))x^{d-1}$

Tenendo a mente la condizione $f|(g^p - g)$ imponiamo che il resto r di tale divisione sia 0, cioè che il polinomio r sia nullo, ovvero avente tutti i coefficienti pari a 0, abbiamo così il seguente sistema lineare.

$$\begin{cases} b_0(r_{0,0} - 1) + b_1 r_{0,1} + \cdots + b_{d-1} r_{0,d-1} = 0 \\ b_0 r_{1,0} + b_1(r_{1,1} - 1) + \cdots + b_{d-1} r_{1,d-1} = 0 \\ \vdots \\ b_0 r_{d-1,0} + b_1 r_{d-1,1} + \cdots + b_{d-1}(r_{d-1,d-1} - 1) = 0 \end{cases}$$

Notiamo che questo si può riscrivere in forma matriciale come $(Q - I)(B) = 0$.

Dove I è la matrice identità, $Q = \begin{pmatrix} r_{0,0} & r_{1,0} & \dots & r_{d-1,0} \\ r_{0,1} & r_{1,1} & \dots & r_{d-1,1} \\ \dots & \dots & \dots & \dots \\ r_{0,d-1} & r_{1,d-1} & \dots & r_{d-1,d-1} \end{pmatrix}$ e $B = (b_0, b_1, \dots, b_{d-1})^\intercal$.

Ci riconduciamo così alla ricerca del nucleo di questa matrice, un vettore $B_0 \in ker(Q-I)$ avrà come entrate i coefficienti di un polinomio che soddisfa le condizioni richieste per l'applicazione del I teorema di Berlekamp.

Osservazione 6.2.1.4 In particolare $ker(Q-I)$ e $G = \{g \in \mathbb{Z}_p[x] \mid deg\, g < d \wedge f|(g^p - g)\}$ sono due $\mathbb{Z}_p-$ spazi vettoriali isomorfi.

Abbiamo così dimostrato il segiente risultato

Teorema 6.2.1.5 (II teorema di Berlekamp) Sia $f \in \mathbb{Z}_p[x]$ un polinomio di grado d. Allora vi è un isomorfismo di gli spazi vettoriali tra i polinomi g dello spazio vettoriale $G = \{g \in \mathbb{Z}_p[x] \mid deg\, g < d \wedge f|(g^p - g)\}$ e $ker(Q-I)$, dove Q è la matrice avente per colonne i coefficienti dei polinomi resto di x^{jp} nella divisione per f.

6.2.2 Algoritmo di fattorizzazione di Berlekamp

Sfruttando il I e II teorema di Berlekamp è possibile fattorizzare agevolmente polinomi in $\mathbb{Z}_p[x]$, riportiamo un esempio di come procedere.

Sia $f = x^3 + x + 2 \in \mathbb{Z}_3$.

i) Anzitutto osserviamo che $d = deg\, f = 3$ e che anche $p = 3$.

ii) Scriviamo un generico polinomio di grado $d-1$: $g = b_0 + b_1 x + b_2 x^2$.

iii) Calcoliamo il resto della divisione di x^{0p}, x^{1p}, x^{2p} per $f = x^3 + x + 2$:

$x^0 = 0f + x^0$

$x^3 = 1f - x - 2$

$x^6 = x^3 x^3 = (f - x - 2)(f - x - 2)$ .....

Troviamo la matrice $Q = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ e dunque ci riconduciamo alla ricerca di un vettore nel nucleo della matrice $Q - I = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$

Troviamo che $ker(Q - I) = \langle (1,0,0), (0,1,2)$. Qui bisogna procedere con cautela: È vero che un qualsiasi vettore g nel nucleo è tale che $f|(g^p - g)$, ma al fine di poter applicare il I teorema di Berlekamp dovremo escludere dalle nostre possibilità i vettori della forma $(\lambda, 0, 0)$, i quali identificano dei polinomi costanti. (Si recuperi l'Osservazione *, che chiarisce perchè si troverà sempre il vettore $(1,0,0)$ come generatore del nucleo).

Usando un po' di furbizia cerchiamo un vettore che abbia il maggior numero di entrate nulle così da dover fare meno conti applicando il I teorema di Berlekamp; ad esempio preferiamo il vettore $g = (0,1,2)$ al vettore $(5,6,12)$ (Seppure anche con questo si trovi una valida fattorizzazione di f).

Si può ora concludere calcolando $MCD(f,g), MCD(f,g-1); MCD(f,g-2)$ e moltiplicando tali polinomi otterremo una fattorizzazione di f:

Preso $g = x + 2x^2$, trovandoci in $\mathbb{Z}_3[x]$ osserviamo che $2 \equiv -1_{mod\,3}$ e quindi

$x + 2x^2 = x - x^2 \in \mathbb{Z}_3[x]$, per l'algoritmo di Euclide abbiamo $MCD(f, g) = MCD(f + xg, g)$ $MCD(x^3 + x + 2, -x^2 + x) = MCD(x^3 + x + 2 + x(-x^2 + x), -x^2+x)$ e quindi $= MCD(x^2+x+2, -x^2+x) = MCD(2(x+1), -x^2+x) = MCD(x + 1, -x^2 + x) = MCD(x + 1, -x^2 + x + x(x + 1)) = MCD(x + 1, 2x) = MCD(x + 1, x) = 1$ **E** Trovare $MCD(f, g - 1) = x^2 + 2x + 2$, $MCD(f, g - 2) = x + 1$. (Trovandoci in $\mathbb{Z}_3[x]$ si potrà ottenere un risultato equivalente con ad esempio $MCD(f, g-1) = -2x^2-x-1$ o simili.) Troviamo così che $f = 1 \cdot (x^2 + 2x + 2)(x + 1)$.

Osservazione 6.2.2.1 Nell'applicazione dell'algoritmo di Berlekamp si ricercano i resti della divisione di x^{jp} per *f*. Ciò è equivalente a ricercare un rappresentante della classe $[x^{jp}] \in \mathbb{Z}_p/(f)$ avente grado minore di quello di *f*.

Ci serviremo dunque della sezione 4.5 sui quozienti di $K[x]$ per velocizzare i conti nel seguente esempio.

Trovare una fattorizzazione del polinomio $f = x^4 + 2 \in \mathbb{Z}_3[x]$.
Anzitutto osserviamo che $d = deg\ f = 4$ e $p = 3$. Dovremo quindi calcolare la divisione per f dei polinomi x^0, x^3, x^6 e x^9.
x^0 ha grado minore di d dunque sarà esso stesso il resto nella divisione per *f*.
Per x^3, grazie all'Osservazione precedente, sarà sufficiente calcolarne la congruenza modulo f: $x^3 \equiv x^3_{mod\ f}$ ed anche esso sarà il suo stesso resto.
$x^6 = x^2 \cdot x^4$; il primo fattore ha grado minore di d e quindi farà parte del resto mentre per x^4 notiamo che $[f] = 0 = [x^4 + 2] = [x^4] + [2]$ e quindi $[x^4] = [-2] = [1]_{mod\ f}$. Dunque il resto di x^6 sarà x^2.
Per $x^9 = x^3 \cdot x^6$ abbiamo già fatto il lavoro necessario, il suo resto nella divisione per f sarà il polinomio $x^3 \cdot x^2 = x^5 = x^4 \cdot x = x$.

La matrice associata a questi resti sarà dunque $Q = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$.

Cioè un polinomio $g = b_0 + b_1x + b_2x^2 + b_3x^3 \in \mathbb{Z}_3[x]$ è tale che $f|(g^p - g)$ se e solo se $(b_0, b_1, b_2, b_3) \in ker(Q-I)$. In particolare il nucleo ha dimensione 3, ed è generato dai vettori $(1,0,0,0), (0,1,0,1), (0,0,1,0)$. Per semplicità prendiamo il semplice monomio x^2 e calcoliamo i polinomi $MCD(f, x^2), MCD(f, x^2-1), MCD(f, x^2-2)$ trovando che $x^4 + 2 = (x^2+1)(x^2+2)$. Possiamo poi continuare tentando di fattorizzare i due fattori ottenendo che il nucleo della matrice $Q_1 - I$ ottenuta considerando il polinomio $x^2 + 1$ è generato dal solo vettore $(1,0)$, dunque il polinomio $x^2 + 1$ è irriducibile.

Il nucleo della matrice $Q_2 - I$ ottenuta a partire dal polinomio $x^2 + 2$ ci permette di trovare ad esempio il polinomio x che ci porta alla fattorizzazione $x^2 + 2 = (x+1)(x+2)$. Dunque una fattorizzazione per mezzo di irriducibili di $x^4 + 2 \in \mathbb{Z}_3[x]$ è data da $x^4 + 2 = (x^2+1)(x+1)(x+2)$.

Fattorizzare il polinomio $f = x^{10} + 4 \in \mathbb{Z}_5[x]$.

Procedendo come fatto fino ad ora dovremmo fare molti conti e lavorare infine con una matrice 10x10, il che non è conveniente. Sarà quindi meglio manipolare questo polinomio sfruttando quanto abbiamo visto fino ad ora. In particolare notiamo che $x^{10} + 4 = (x^5 + 2)^2$ (la caratteristica del campo è un numero primo) e così possiamo ricondurci a dei conti più semplici sul polinomio $x^5 + 2$, ma possiamo fare di meglio.

Infatti $x^{10} + 4 = (x^2)^5 + 4$ ed in $\mathbb{Z}_5[x]$ vale il Piccolo Teorema di Fermat per le costanti come 4, così abbiamo che $4 = 4^5 \in \mathbb{Z}_5$ e dunque $x^{10} + 4 = (x^2+4)^5 =$

$(x+2)^5(x+2)^5 = (x+2)^{10}$.

6.3 III teorema di Berlekamp

Abbiamo fatto notare nell'Osservazione 6.2.1.3 che l'algoritmo di Berlekamp ci dà una fattorizzazione propria ma che i fattori non sono necessariamente irriducibili. Il seguente teorema ci dà informazioni su tale questione.

Teorema 6.3.1 (III teorema di Berlekamp) Sia $f \in \mathbb{Z}_p[x]$ un polinomio di grado d. Allora il numero di fattori irriducibili di f è pari alla dimensione del nucleo della matrice $Q - I$, inoltre f è irriducibile se e solo se la dimensione di $ker(Q-I)$ è 1 e $MCD(f, Df)$ è un polinomio unitario.

Dimostrazione Dalla teoria precedente sappiamo che p è un numero primo $\Rightarrow \mathbb{Z}_p$ è un campo $\Rightarrow \mathbb{Z}_p[x]$ è un campo $\Rightarrow \mathbb{Z}_p[x]$ è un UFD. Possiamo quindi supporre che $f = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_k^{\alpha_k}$, con $q_1, \dots, q_k$ irriducibili e distinti in $\mathbb{Z}_p[x]$. Consideriamo $g \in G$ un polinomio appartenente all'insieme definito nel II teorema di Berlekamp, cioè tale che $f|(g^p - g)$ ed avente grado minore di d. Ricordiamo che per l'Osservazione 6.2.1.1,iii) $g^p - g = g(g-1)..(g-p+1)$. La condizione $f|(g^p-g)$ può essere quindi riscritta come $q_1^{\alpha_1} q_2^{\alpha_2} \dots q_k^{\alpha_k} | g(g-1)..(g-p+1)$ ed in particolare, per ogni $i = 1, \dots, k$, $q_i | g(g-1)\dots(g-p+1)$. Essendo i q_i tutti irriducibili e primi otteniamo che q_i divide uno dei fattori $g, (g-1), \dots, (g-p+1)$, ad esempio $q_i|(g-s_i)$; con $s_i \in \mathbb{Z}_p$ e per l'Osservazione 6.2.1.1 iv) tale $g - s_i$ è l'unico fattore divisibile per q_i.
Inoltre $q_i^{\alpha_i}|f$ ed $f|(g^p-g)$ quindi anche $q_i^{\alpha_i}|(g^p-g)$. Avendo già stabilito che per ogni q_i esisto un unico $g - s_i$ che ne è multiplo otteniamo che $q_i^{\alpha_i}|(g-s_i)$,

questo per ogni $i = 1, \ldots, k$.

Abbiamo così individuato univocamente una k-upla $(s_1, \ldots, s_k)$ di elementi di $\mathbb{Z}_p^k$ e dunque una funzione $\varphi\colon G \to \mathbb{Z}_p^k$ tale che $g = \prod_{i=0}^{p-1}(g - s_i) \in G$ $\varphi(g) = (s_1, \ldots, s_k)$. Tale funzione è suriettiva, infatti fissata una k-upla $(s_1, \ldots, s_k)$ nel codominio vogliamo trovare un polinomio $g \in G$ che soddisfi il sistema di congruenze:

$$\begin{cases} g(x) \equiv s_1 \mod q_1^{\alpha_1} \\ g(x) \equiv s_2 \mod q_2^{\alpha_2} \\ \qquad\qquad\qquad\qquad \vdots \\ g(x) \equiv s_k \mod q_k^{\alpha_k} \end{cases}$$

Siccome $q_i^{\alpha_i}$ sono a due a due coprimi abbiamo, per il Teorema cinese dei resti, che esistono (infiniti) polinomi g che sono soluzione del sistema, per il Teorema 4.5.1 esiste unico g tale che, oltre ad essere soluzione del sistema, ha anche grado minore di quello di f. Preso questo g verifichiamo che esso appartiene a G: per ogni i si ha $q_i^{\alpha_i} | (g - s_i) \Rightarrow q_i^{\alpha_i} | g^p - g \Rightarrow f = \prod_{i=1}^{k} q_i^{\alpha_i} | g^p - g \Rightarrow$ $g \in G$. Si verifica inoltre che tale funzione è anche iniettiva (Siano $g_1, g_2 \in G$ tali che $\varphi(g_1) = \varphi(g_2) = (s_1, \ldots, s_k)$ allora $q_i | g_1 - s_i$ e $q_i | g_2 - s_i$, per lo stesso ragionamento fatto sopra si ottiene poi $q_i^{\alpha_i} | g_1 - s_i$ e $q_i^{\alpha_i} | g_2 - s_i$. Dunque $q_i^{\alpha_i} | g_1 - g_2 \Rightarrow f | g_1 - g_2$ ma essendo $g_1, g_2 \in G$ essi hanno grado minore di *deg* f e la relazione trovata sopra resta coerente se e solo se $g_1 - g_2 = 0$.) Abbiamo quindi una funzione biiettiva $\varphi : G \to \mathbb{Z}_p^k$. Come è ben noto se esiste una biiezione tra due insiemi allora essi hanno lo stesso numero di elementi; siccome $|\mathbb{Z}_p^k| = p^k$ allora anche $|G| = p^k$ e per il II teorema

di Berlekamp anche $|ker(Q-I)| = p^k$. Come abbiamo visto $ker(Q-I)$ è uno spazio vettoriale, esso ha una base finita $v_1, \ldots, v_r$. Per definizione $ker(Q-I) = \{\sum_{i=1}^{r} \lambda_i v_i | \lambda_i \in \mathbb{Z}_p\}$ ed ha quindi cardinalità p^r, ma per quanto visto sopra imponiamo $p^r = p^k \Rightarrow r = k$. Cioè la dimensione del nucleo di $Q-I$ è pari al numero di fattori irriducibili di f. La seconda parte del teorema deriva facilmente dal Teorema 4.4.18.

Osservazione 6.3.2 Se f è un polinomio della forma $f = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ allora esiste un numero $\overline{p}$ tale che $f_{mod\, p} \in \mathbb{Z}_p[x]$ ha la stessa successione di coefficienti di f, per ogni numero primo $p > \overline{p}$. In particolare per p numero primo "sufficientemente grande" possiamo cercare una fattorizzazione di $f \in \mathbb{Z}_p[x]$ applicando i Teoremi di Berlekamp, e tale fattorizzazione sarà (eventualmente) anche una fattorizzazione di f in $\mathbb{Z}[x]$. Questo succederà se tutti i polinomi considerati nell'applicazione dell'algoritmo avranno per coefficienti dei numeri minori di tale p. Per questo motivo, perchè le successioni dei coefficienti hanno solo un numero finito di entrate non nulle, per l'ordinamento negli interi e perchè esistono infiniti numeri primi si ottiene che esisterà sempre un p primo per il quale una fattorizzazione di $f \in \mathbb{Z}_p[x]$ coinciderà con una fattorizzazione di $f \in \mathbb{Z}[x]$.)

Un ragionamento più raffinato prende il nome di Metodo di sollevamento di Hensel.

In sostanza abbiamo visto come si può fattorizzare polinomi in $\mathbb{Z}_p[x]$ per p primo, e osservato che per p_f primo sufficientemente grande (che dipende in prima battuta dai coefficienti del polinomio f, ma non solo) tale fattorizzazione si può sollevare ad una fattorizzazione in $\mathbb{Z}[x]$ (e quindi anche ad una

fattorizzazione in $\mathbb{Q}[x]$). Non si entra in ulteriori dettagli.

La teoria sviluppata fino ad ora permette di apprezzare questo video introduttivo sul sistema dei numeri p-adici.

7 Estensioni di anelli e di campi

7.1 Polinomi in più variabili

Sia A un anello ed $A' = A[x]$ il corrispondente anello dei polinomi nella variabile x. L'anello di polinomi $A'[y]$ ha per elementi polinomi della forma $b_0 + b_1 y + \cdots + b_n y^n$; dove $b_i \in A'$ sono a loro volta dei polinomi della forma
$b_0 = a_{00} + a_{1,0}x + \ldots$
$\vdots$
$b_n = a_{n0} + a_{n1}x + \ldots$
Un polinomio $f \in A'[y]$ è dunque della forma $f = (a_{00} + a_{10}x + ..) + (a_{01} + a_{11}x + \ldots)y + \cdots + (a_{0n} + \ldots)y^n = \sum_{i,j \in I} a_{i,j} x^i y^j$.

Definizione 7.1.1 L'anello A' così costruito si denota con $A[x, y]$ e si dice *anello dei polinomi in due variabili.*

Osservazione 7.1.2 Questa costruzione si generalizza banalmente ripetendo lo stesso processo partendo dall'anello $A'[y] = A''$, costruendo $A''' = A''[z] = A[x, y, z]$ e così via per un numero arbitrario di variabili. Abbiamo cioè definito ricorsivamente l'anello $(A[x_1, \ldots, x_{n-1}])[x_n] = A[x_1, \ldots, x_n]$ dei polinomi nelle n variabili $x_1, \ldots, x_n$, gli elementi di tale anello sono della forma $\sum_{(i_1,\ldots,i_n) \in I} a_{i_1,\ldots,i_n} x_1^{i_1} \ldots x_n^{i_n}$.

Osservazione 7.1.3
L'anello $A[x_1, \ldots, x_n]$ può essere interpretato in vari modi, ad esempio $= (A[x_1, \ldots, x_{n-1}])[x_n] = (A[x_1])[x_2, \ldots, x_n] = (A[x_2])[x_1, x_3, \ldots, x_n]$ e così via.

Definizione 7.1.4

Sia $f = \in A[x_1, \ldots, x_n]$ un polinomio in n variabili. Si definiscono:

i) Il *grado relativo alla variabile* x_i *di* f come il grado di $f \in (A[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n])[x_i]$

ii) Il *grado globale di* f come la somma di tutti i gradi relativi alle variabili $x_1, \ldots, x_n$

Osservazione 7.1.5

i) Se A è un dominio d'integrità allora $A' = A[x_1]$ è un dominio d'integrità, dunque anche $A'[x_2]$ è un dominio e così via. Si prova induttivamente che se A è un dominio allora $A[x_1, \ldots, x_n]$ è un dominio.

ii) Se A è un dominio d'integrità e $f, g \in A[x_1, \ldots, x_n]$ sono due polinomi di grado globale $deg\ f, deg\ g$ rispettivamente allora $deg(fg) = deg\ f + deg\ g$

iii) Se K è un campo allora $K[x_1]$ è un UFD ed in generale $K[x_1, \ldots, x_n]$ è un UFD. (Ciò si vede con un ragionamento simile a quello utilizzato per dimostrare il Lemma di Gauss)

Teorema 7.1.6 (Teorema di estensione) Sia $\varphi\colon A \to B$ un omomorfismo di anelli. Siano $b_1, \ldots, b_n \in B$ elementi fissati. Allora $\exists!\Phi\colon A[x_1, \ldots, x_n] \to B$ omomorfismo di anelli tale che $\Phi|_A = \varphi$ e $\Phi(x_i) = b_i$. Inoltre detto F l'omomorfismo di valutazione definito in 4.2.7 vale $\Phi(F(x_1, \ldots, x_n)) = F(b_1, \ldots, b_n)$

Dimostrazione Per induzione sul numero di variabili dell'anello. Il caso $n = 1$ è il Teorema 4.2.8. Supponiamo vera la tesi fino ad $n - 1$. Allora $\exists!\overline{\Phi}\colon A[x_1, \ldots, x_{n-1} \to B$ tale che $\overline{\Phi}|_A = \varphi$ e $\Phi(x_i) = b_i$ con $i = 1, \ldots, n-1$. Scelta ora una nuova variabile x_n ed un elemento $b_n \in B$ applichiamo il Teore-

ma 4.2.8 trovando che esiste $\Phi : (A[x_1, \ldots, x_{n-1})[x_n] \to B$ tale che $\Phi(x_n) = b_n$ e $\Phi|_{A[x_1,\ldots,x_{n-1}]} = \overline{\Phi}$. Allora $\Phi|_A = \varphi$ e si ha inoltre $\Phi(x_i) = \overline{\Phi}(x_i) = b_i$ per ogni $i = 1, \ldots, n-1$ e $\Phi(x_n) = b_n$.

Osservazione 7.1.7 Vale il principio di identità dei polinomi.

Osservazione 7.1.8 L'ideale $I = (x, y) \subseteq \mathbb{Q}[x, y]$ è massimale.

Dimostrazione Attraverso il teorema precedente definiamo $\Phi\colon \mathbb{Q}[x, y] \to \mathbb{Q}$ imponendo $\Phi|_{\mathbb{Q}} = id$ e $\Phi(x) = \Phi(y) = 0$. Tale funzione è suriettiva in quanto $\mathbb{Q} \subset \mathbb{Q}[x, y]$ e $\Phi(\mathbb{Q}) = id(\mathbb{Q}) = \mathbb{Q}$. Per il II teorema di omomorfismo otteniamo $\mathbb{Q}[x, y]/_{ker\ \Phi} \simeq \mathbb{Q}$.

Vogliamo osservare che $ker\ \Phi = (x, y) = \{ax + by | a, b \in \mathbb{Q}[x, y]\}$. Si verifica facilmente che $(x, y) \subseteq ker\Phi$, ci concentriamo quindi sulla seconda inclusione. Prendiamo un polinomio $F(x, y) \in ker\ \Phi \subseteq \mathbb{Q}[x, y]$. Per sfruttare la teoria sui polinomi in una variabile interpretiamo F come appartenente a $(\mathbb{Q}[x])[y]$; dunque esso sarà della forma $F = b_0 + b_1x + \cdots + b_ny^n$ con $b_0, \ldots, b_n \in \mathbb{Q}[x]$. Effettuiamo quindi la divisione di F per il polinomio y, otteniamo $F(x, y) = q(x, y)y + r(x, y)$. Con $deg_y r(x, y) < deg_y\ y = 1$. Dunque il polinomio $r(x, y)$ ha grado rispetto alla variabile y pari a 0, in sostanza è un polinomio nella sola variabile x oppure è il polinomio nullo. Abbiamo trovato che $F(x, y) = q(x, y)y + r(x)$. Per ipotesi questo elemento appartiene al nucleo di un omomorfismo, dunque abbiamo $\Phi(F(x, y)) = \Phi(q(x, y)y + r(x)) = \Phi(q(x, y)y) + \Phi(r(x)) = 0$. Per come è definito Φ sappiamo inoltre che $\Phi(y) = 0$. Dunque si ottiene $\Phi(r(x)) = r(0) = 0$ e ciò accade se e solo se il polinomio $r(x)$ non ha il termine noto, ovvero $r(x) = a_1x + \ldots a_mx^m = x(a_1 + \cdots + a_mx^{m-1})$. Posti $a = (a_1 + \cdots + a_mx^{m-1})$ si ottiene che $F(x, y) =$

$q(x,y)y + x(a_1 + \cdots + a_m x^{m-1}) = ax + by \in (x,y)$.

Più in generale vale la seguente condizione:

Teorema 7.1.9 Sia $K[x_1, \ldots, x_n]$ un anello di polinomi a coefficienti un un campo K. Allora l'ideale $I = (x_1 - \alpha_1, x_2 - \alpha_2, \ldots, x_n - \alpha_n)$ generato dai polinomi $x_i - \alpha_i$ è massimale.
Dimostrazione (Abbozzo) Vogliamo vedere che $K[x_1, \ldots, x_n]/I$ è un campo. Per fare questo si costruisce un omomorfismo opportuno $K[x_1, \ldots, x_n] \xrightarrow{\varphi} K$ che sia suriettivo e il cui nucleo sia proprio I, così da poter tracciare l'isomorfismo $K[x_1, \ldots, x_n]/I \simeq K$.

Consideriamo l'omomorfismo φ: $K[x_1, \ldots, x_n] \to K$ tale che $\varphi|_K = id$ e $\varphi(x_i) = \alpha_i$. Esso è chiaramente suriettivo. Si verifica facilmente che $I \subseteq ker(\varphi)$. Per vedere che $ker(\varphi) \subseteq I$ prendiamo un polinomio $F(x_1, \ldots, x_n) \in ker(\varphi)$. Interpretando $K[x_1, \ldots, x_n]$ come $(K[x_1, \ldots, x_{n-1}])[x_n]$ possiamo effettuare la divisione di F per il polinomio $g_n(x_n) = x_n - \alpha_n$ ottenendo $F(x_1, \ldots, x_n) = q_n(x_1, \ldots, x_n)g_n(x_n) + r_n(x_1, \ldots, x_n])$.
Naturalmente $deg_{x_n} r_n < deg_{x_n} g_n$ quest'ultimo ha grado 1 e dunque $r_n(x_1, \ldots, x_n)$ sarà un polinomio nelle sole variabili $x_1, \ldots, x_{n-1}$.
Osserviamo che $F(\alpha_1, \ldots, \alpha_n) = q_n(\alpha_1, \ldots, \alpha_n)g_n(\alpha_n) + r_n(\alpha_1, \ldots, \alpha_{n-1}) = q_n(\alpha_1, \ldots, \alpha_n)0 + r_n(\alpha_1, \ldots, \alpha_{n-1}) = 0$ e possiamo riapplicare questo processo al polinomio $r_n \in (K[x_1, \ldots, x_{n-2})[x_{n-1}]$ e dividendolo per il polinomio $g_{n-1} = (x_{n-1} - \alpha_{n-1})$ trovando un resto r_{n-1} e avanti così.
Infine si troverà che $F(x_1, \ldots, x_n) = q_1 g_1 + q_2 g_2 + \cdots + q_n g_n$ dove per g_i si sarà sempre scelto il polinomio $x_i - \alpha_i$. Otteniamo così che F è una combinazione lineare dei polinomi che generano l'ideale I: $\forall F \in ker(\varphi), F \in I \Rightarrow ker(\varphi) \subseteq$

I. Abbiamo così provato che $I = ker(\varphi)$ e per la suriettività e il II teorema di omomorfismo si ha infine $K[x_1, \ldots, x_n]/I = K[x_1, \ldots, x_n]/ker(\varphi) \simeq Im(\varphi) = K$. Quindi il quoziente è isomorfo ad un campo; I è massimale.

Osservazione 7.1.10

i) Non vale il viceversa: NON è vero che se un ideale è massimale allora è della forma $I = (x_1 - \alpha_1, x_2 - \alpha_2, \ldots, x_n - \alpha_n)$. Ad esempio già solo per il caso particolare di una sola variabile abbiamo visto che un ideale è massimale se e solo se è generato da un polinomio irriducibile. Ma in alcuni $K[x]$ esistono polinomi irriducibili di grado maggiore di 1! (Si pensi ad esempio a $x^2 + 1 \in \mathbb{Q}[x]$ il quale è irriducibile e infatti $I = (x^2 + 1)$ è massimale).

ii) Dal controesempio si intuisce che il "problema" che rende in generale falso il viceversa sta nel fatto che ci possono essere polinomi irriducibili di grado maggiore di 1.

iii) In un campo algebricamente chiuso tutti e soli i polinomi irriducibili sono quelli di grado 1

Teorema 7.1.11 (Teorema degli zeri di Hilbert) Se K è un campo algebricamente chiuso allora $\mathcal{M} \subseteq K[(x_1, \ldots, x_n]$ è massimale se e solo se $\exists \alpha_1, \ldots, \alpha_n \in K$ tali che $\mathcal{M} = ((x_1 - \alpha_1, x_2 - \alpha_2, \ldots, x_n - \alpha_n)$.

Dimostrazione omessa

Teorema 7.1.12 Sia $K[x_1, \ldots, x_n]$ un anello di polinomi a coefficienti un un campo K. Allora l'ideale $I = (x_1 - \alpha_1, x_2 - \alpha_2, \ldots, x_i - \alpha_i)$ generato dai polinomi $\{x_i - \alpha_i\}_{0<i\leq n-1}$ è primo per ogni $i \leq n - 1$.

Dimostrazione Analoga a quella del Teorema 7.1.9

Senza perdere di generalità supponiamo $i = n - 1$. Vogliamo vedere che

$K[x_1, \ldots, x_n]/I$ è un dominio d'integrità.

Definiamo $K[x_1, \ldots, x_n] \xrightarrow{\varphi} K[x_n]$ tale che $\varphi|_K = id$; $\varphi(x_1) = \alpha_1 \ldots \varphi(x_{n-1}) = \alpha_{n-1}, \varphi(x_n) = x_n$.

Si procedede esattamente come fatto nel Teorema 7.1.9 trovando infine $K[x_1, \ldots, x_n]/I \simeq K[x_n]$ il quale è un dominio d'integrità, cioè I è ideale primo.

Se avessimo fissato un altro i avremmo trovato $K[x_1, \ldots, x_n]/I \simeq K[x_{n-i}, \ldots, x_n]$ il quale è ancora un dominio.

Osservazione 7.1.13 Gli anelli di polinomi in più variabili non sono necessariamente dei domini ad ideali prncipali; ad esempio l'ideale (x, y) non è principale in $\mathbb{K}[x, y]$.

Infatti se per assurdo esistesse $f \in \mathbb{K}[x, y]$ tale che $(x, y) = (f)$ allora avremmo che $x = \alpha f$ e $y = \beta f$ e ragionando sui gradi otteniamo $deg_y\ x = deg_y\ (\alpha f) = deg_y(\alpha) + deg_y(f) = 0$ e quindi $deg_y\ f \leq 0$; analogamente si vede che $deg_x\, y = 0 \Rightarrow deg_y\, f \leq 0$. Cioè il polinomio f avrebbe grado globale minore o uguale di 0. f non può essere il polinomio nullo per ovvi motivi, se invece avesse grado 0 sarebbe una costante in $\mathbb{K}$ e quindi invertibile e dunque il corrispondente ideale sarebbe $(f) = (1) = \mathbb{K}[x, y]$, il che è assurdo in quanto $\mathbb{K} \not\subset (x, y)$

7.2 Estensioni, elementi algebrici e trascendenti

Definizione 7.2.1 Sia B un anello ed $A \subseteq B$ un suo sottoanello. Siano $b_1, \ldots, b_n \in B$. Allora il più piccolo anello $\overline{A}$ tale che $A \cup \{b_1, \ldots, b_n\} \subseteq \overline{A}$ è della forma $\overline{A} = \{ \sum_{i_1 \ldots i_n \in I} a_{i_1 \ldots i_n} b_1^{i_1} \ldots b_n^{i_n} | a_{i_1 \ldots i_n} \in A\}$ e si denota con $A[b_1, \ldots, b_n]$.

Osservazione 7.2.2 Sfruttando il teorema di estensione possiamo definire una funzione $\varphi \colon A[x_1, \ldots, x_n] \to B$ tale che $\varphi(a) = a; \ \forall a \in A$ (cioè $\varphi|_A = id$) e tale che $\varphi(x_i) = b_i$. Osserviamo che preso un polinomio $F(x_1, \ldots, x_n) = \sum_{(i_1, \ldots, i_n) \in I} a_{i_1, \ldots, i_n} x_1^{i_1} \ldots x_n^{i_n} \in A[x_1, \ldots, x_n]$ la sua immagine attraverso φ è $\varphi(F(x_1, \ldots, x_n)) = F(b_1, \ldots, b_n) = \sum_{i_1 \ldots i_n \in I} a_{i_1 \ldots i_n} b_1^{i_1} \ldots b_n^{i_n}$. Cioè l'immagine $Im(\varphi) = A[b_1, \ldots, b_n]$ e ciò spiega la notazione utilizzata.

Definizione 7.2.3 Sia L un campo e $K \subseteq L$ un suo sottocampo. Allora L si dice anche *estensione di* K e per esprimere tale relazione si scrive $L : K$.

Osservazione 7.2.4 Se L, K sono due campi tali che $L : K$ allora l'anello $K[a] \subseteq L$ eredita da L il fatto di essere dominio d'integrità.

Osservazione 7.2.5 Siano L, K due campi tali che $L : K$. Sia $a \in L$ fissato. Allora il più piccolo campo che contiene K ed a è $Q(K[a])$ il campo dei quozienti del dominio $K[a]$ e si denota con $K(a)$.

Definizione 7.2.6 Siano L, K due campi tali che $L : K$. Un elemento $a \in L$ si dice:

i) *algebrico su* K se esiste un polinomio non nullo $f(x) \in K[x]$ (a coefficienti

in K) tale che $f(a) = 0$

ii) *trascendente su* K se non esiste un polinomio non nullo $f(x) \in K[x]$ (a coefficienti in K) tale che $f(a) = 0$.

Ad esempio su $\mathbb{Q}$ i numeri $\sqrt{2}, \sqrt[3]{7}$ sono algebrici mentre i numeri $0, 101001\underbrace{000000}_{3!}1\underbrace{0\ldots0}_{4!}1\ldots,$ il numero di Nepero e ed anche π sono trascendenti.

Definizione 7.2.7 Sia K un campo e sia a un elemento algebrico su K. Allora un polinomio (non nullo) di grado minimo che si annulla in a si dice *polinomio minimo di a su K.*

Osservazione 7.2.8

i) Se a è algebrico su K allora esistono dei polinomi in $K[x]$ che si annullano quando valutati in a. Essendo il grado di un polinomio un numero naturale ci si convince facilmente che esiste sempre un polinomio minimo di a su K.

ii) Se $m(x) \in K[x]$ è un polinomio minimo di a allora anche $\alpha m(x)$ (con $\alpha \in K \setminus 0$) è un polinomio minimo di a; infatti questi hanno lo stesso grado e si annullano in a.

iii) Per ogni $\alpha \neq 0 \in K$ $\exists \alpha^{-1}$. Il punto precedente si può quindi riformulare come: Se $m(x)$ è un polinomio minimo di a su K allora ogni polinomio $\overline{m}(x)$ associato ad m è anche un polinomio minimo.

iv) Per quanto detto nei punti precedenti e per l'Osservazione 4.2.3 ii) si ha che $\exists m(x)$ polinomio minimo di a su K monico.

v) Tale polinomio minimo monico è unico. Infatti se esistessero $m_1(x) = a_0 + a_1x + ... + x^n; m_2(x) = b_0 + b_1x + ... + x^m$ minimi e monici allora $m{=}n$ e il polinomio $m_1(x) - m_2(x) = (a_0 - b_0) + (a_1 - b_1)x + \cdots + (a_{n-1} - b_{n-1})x^{n-1} + 0x^n$

si annullerebbe in a, ma esso è di grado minore di $n = deg\, m_1 = deg\, m_2$ e dunque dovrà essere il polinomio nullo, si ha cioè $m_1 = m_2$.

Motivati da questa osservazione potremo sviluppare la teoria supponendo che i polinomi minimi di un elemento siano monici e dalla loro unicità potremo usare l'articolo determinativo.

Teorema 7.2.9 Sia $a \in L$ un elemento algebrico su K. Sia $m(x)$ il polinomio minimo. Allora $m(x)$ è irriducibile.
Dimostrazione Supponiamo per assurdo che la fattorizzazione $m = fg$ con $f, g \in K[x]$ sia propria. Essendo L un campo esso è in particolare un dominio. Per ipotesi si ha l'uguaglianza $m(a) = f(a)g(a) = 0$, ciò implica $f(a) = 0 \vee g(a) = 0$, siccome $f, g \neq 0$ sono non costanti e i loro gradi sono minori di quello di m si contraddice l'ipotesi di m polinomio minimo.

Osservazione 7.2.10 Siano K, L due campi tali che $L : K$. Allora L è un K-spazio vettoriale con la somma di L e il prodotto di L ristretto all'insieme $K \times L$ (cioè definito come $\cdot : K \times L \to L$ tale che $(a, b) \mapsto ab$ dove ab è il prodotto degli elementi $a, b \in L$).

Definizione 7.2.11 La dimensione di L come K-spazio vettoriale si dice *grado dell'estensione* e si denota come $[L : K]$.

Ad esempio sia $L = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$. Esso è un campo (Per verificare la chiusura rispetto agli inversi si fa uso della razzionalizzazione) ed un'estensione di $\mathbb{Q}$ (fissando $b = 0$ al variare di a si ottiene $\mathbb{Q}$). Il grado dell'estensione è $[L : \mathbb{Q}] = 2$; una base dello spazio vettoriale è data dai vettori 1 e $\sqrt{2}$ (per

verificare la lineare indipendenza si usa il fatto che $\sqrt{2}$ è irrazionale.)
Sia $L = \{a+b\sqrt[3]{2}+c\sqrt[3]{4}|a,b,c \in \mathbb{Q}\}$. Anche in questo caso esso è un campo ed un'estensione di $\mathbb{Q}$. Si ha che $[L:\mathbb{Q}] = 3$ ed una base dello spazio vettoriale è data dai vettori $1, \sqrt[3]{2}, \sqrt[3]{4}$.

$[\mathbb{R}:\mathbb{Q}]$ ha per grado un'infinità non numerabile.

Teorema 7.2.12 Siano L, K due campi tali che $L:K$, sia $a \in L$.
i) Se $a \in L$ è algebrico su K ed m è il corrispondente polinomio minimo allora $K[a] \simeq K[x]/(m)$ ed esso è un campo.
ii) Se $a \in L$ è trascendente su K allora $K[x] \simeq K[a]$. Dimostrazione Si consideri l'omomorfismo φ: $K[x] \to L$ definito da $\varphi(\alpha) = \alpha$; $\forall \alpha \in K$ e $\varphi(x) = a$. Nel caso i) il suo nucleo è $ker\,\varphi = \{f \in K[x]|\varphi(f(x)) = f(a) = 0\}$. Come tutti gli ideali in $K[x]$ anch'esso è principale e si nota facilmente che coincide con l'ideale (m) generato dal polinomio minimo di a su K. Dal II teorema di omomorfismo si ha $K[x]/(ker\,\varphi) \simeq Im(\varphi)$ e dall'Osservazione 8.2 concludiamo che $K[x]/(m) \simeq Im(\varphi) \simeq K[a]$. Inoltre per il Teorema * m è irriducibile e per il Teorema 4.5.4 $K[x]/(m)$ è un campo e dunque pure $K[a]$ è un campo. Nel caso ii) il suo nucleo è $ker\,\varphi = \{0\}$ e per il II teorema di omomorfismo si ha $K[x]/(ker\,\varphi) = K[x]/(0) \simeq K[x] \simeq Im(\varphi) \simeq K[a]$ ed in particolare esso è un dominio.

Teorema 7.2.13 (Teorema della torre) Siano K, L, M tre campi tali che $L:K$ e $M:L$. Allora $M:K$ e $[M:K] = [M:L]\cdot[L:K]$.
Dimostrazione Il primo punto è banale essendo $K \subseteq L \subseteq M$.
Riportiamo la dimostrazine per $[M:K], [M:L], [L:K]$ numeri finiti, il Teorema continua a valere per gradi infiniti considerando le cardinalità. Sia

$n = [M : L]$; quindi $\exists b_1, \ldots, b_n \in M$ base del L-spazio vettoriale M. Inoltre posto $m = [L : K]$ si ottiene analogamente che $\exists a_1, \ldots, a_m \in L$ base del K-spazio vettoriale L.

Consideriamo un elemento $u \in M$, esso può essere espresso come combinazione lineare della base di M: $u = \lambda_1 b_1 + \cdots + \lambda_n b_n$ con $\lambda_j \in L$.

Tutti i λ_j si possono a loro volta esprimere come combinazioni lineari della base di L: $\lambda_j = \mu_{1,j} a_1 + \cdots + \mu_{m,j} a_m$ con $\mu_{ij} \in K$.

Mettendo assieme quanto trovato si ha l'espressione $u = (\mu_{11} a_1 + \cdots + \mu_{m1} a_m) b_1 + \cdots + (\mu_{1n} a_1 + \cdots + \mu_{mn} a_m) b_n$. Sviluppando i conti e ricompattando si trova $u = \sum_{\substack{i=1,\ldots,m \\ j=1,\ldots,n}} \mu_{ij} a_i b_j$ cioè $u \in M$ è combinazione lineare degli elementi $a_i b_j$ con coefficienti in K e quindi M è generato dagli elementi $(a_i b_j)_{\substack{i=1,\ldots,m \\ j=1,\ldots,n}}$ che sono in numero mn. Se tali elementi fossero linearmente indipendenti su K avremmo concluso; consideriamo allora una loro combinazione lineare nulla:

$\sum_{i,j} \mu_{ij} a_i b_j = (\mu_{11} a_1 + \cdots + \mu_{m1} a_m) b_1 + \cdots + (\mu_{1n} a_1 + \cdots + \mu_{mn} a_m) b_n = 0.$

Dalla lineare indipendenza dei b_j si ha che per ogni j il corrispondente $\sum_{i=(1,\ldots,m)} \mu_{ij} a_i = 0$ e dalla lineare indipendenza degli a_i si ha che tutti i μ_{ij} sono nulli; si è così provato che una combinazione lineare nulla ha necessariamente coefficienti nulli e quindi i vettori sono linearmente indipendenti.

Definizione 7.2.14 Siano K, L due campi tali che $L : K$. L'estensione L si dice *estensione algebrica su* K se per ogni $a \in L$ si ha che a è algebrico su K.

Teorema 7.2.15 Siano K, L due campi tali che $L : K$. Se $[L : K] = n$ è un numero finito allora L è un'estensione algebrica su K.

Dimostrazione Sia $\alpha \in L$. Essendo L uno spazio vetoriale su K di dimensione n abbiamo che gli $n+1$ elementi gli elementi $\alpha^0 = 1; \alpha^1 = \alpha, \ldots, \alpha^n \in L$ sono linearmente dipendenti; cioè esiste una loro combinazione lineare nulla in cui non tutti i coefficienti sono nulli: $\Lambda = \lambda_0\alpha^0 + \lambda_1\alpha + \cdots + \lambda_n\alpha^n = 0$. Un elemento nella controimmagine di Λ attraverso l'omomorfismo di valutazione v_α è il polinomio $\lambda_0 + \lambda_1 x + \cdots + \lambda_n x^n \in K[x]$. Questo è un polinomio non nullo a coefficienti in K che si annulla quando valutato in α; cioè α è algebrico.

7.3 Campi di spezzamento

Osservazione 7.3.1 Se $f \in K[x]$ è irriducibile allora $L = K[x]/(f)$ è tale che $L : K$. Infatti L così definito è un campo ed i suoi elementi sono combinazioni lineari di $[1], [x], \ldots, [x^{deg\, f-1}]$, ed in particolare prendendo gli elementi della forma $\lambda[1]$ otteniamo K.

Teorema 7.3.2 Sia $f \in K[x]$ un polinomio irriducibile. Allora f ha una radice in $L = K[x]/(f)$.
Dimostrazione Se $f = a_0 + a_1 x + \cdots + a_n x^n$ e $deg\, f = n$ allora gli elementi di L sono delle combinazioni lineari degli elementi $[1], [x], \ldots, [x^{n-1}]$. Posto $\xi = [x]$ si vede che $f(\xi) = a_0 + a_1[x] + \cdots + a_n[x^n] = [a_0 + a_1 x + \cdots + a_n x^n] = [f(x)] = 0 \in K[x]/(f)$. Quindi ξ è una radice di f in L.

Teorema 7.3.3 Sia $f \in K[x]$ un polinomio di grado maggiore o uguale di uno. Allora esiste L estensione di K tale che f ha tutte le radici in L; cioè $f = (x - \alpha_1)^{r_1} \ldots (x - \alpha_m)^{r_m}$.

Dimostrazione Per induzione completa sul grado di f. Se $n = deg\, f = 1$ allora $f = a_0 + a_1 x$ ha per radice l'elemento $-\frac{a_0}{a_1} \in K$; preso $L = K$ abbiamo la tesi.

Sia $n > 1$: Sappiamo che se K è un campo allora $K[x]$ è un UFD. Poniamo dunque $f = qf_1$ con $q \in K[x]$ irriducibile, dal Teorema precedente esiste un campo K_1 dove q ha almeno una radice α_1, possiamo quindi fattorizzare q come $q = (x - \alpha_1)^{r_1} q'$. Quindi $f = (x - \alpha_1)^{r_1} q' f_1 \in K_1[x]$. Denotato $q' f_1 = g$ osserviamo che esso ha grado minore di $deg\, f$. Possiamo così applicare l'ipotesi induttiva trovando che esiste un'estensione L di K_1 nella quale $g = c(x - \alpha_2)^{r_2}(x - \alpha_3)^{r_3} \dots (x - \alpha_m)^{r_m}$.

In particolare $L : K$ ed in L si ha $f = c(x - \alpha_1)^{r_1}(x - \alpha_2)^{r_2}(x - \alpha_3)^{r_3} \dots (x - \alpha_m)^{r_m}$.

Definizione 7.3.4 Sia K un campo ed $f \in K[x]$ un polinomio. L'estensione $L : K$ tale che $f \in L$ si spezza in fattori lineari si dice *campo di spezzamento per* f o *campo di riducibilità completa*.

Osservazione 7.3.5 Il polinomio $x^2 + 1 \in \mathbb{R}[x]$ è irriducibile. Consideriamo l'estensione $L = \mathbb{R}[x]/(x^2 + 1)$. L'elemento $\xi = [x] \in L$ è tale che $\xi^2 = [x^2] = [-1] \in L$ ed è radice del polinomio $x^2 + 1 \in L$. Inoltre gli elementi di L sono combinazioni lineari degli elementi $[1], [x] = \xi$; cioè $L = \mathbb{R}[x]/(x^2+1) = \{a[1] + b\xi | a, b \in \mathbb{R}\}$. Verificando le operazioni ci convinciamo di aver appena costruito il campo dei numeri complessi $\mathbb{C}$, dove $\xi = [x]_{x^2+1} = i = \sqrt{-1}$ è l'unità immaginaria.

8 Campi finiti

Si ricorda che se K è un campo finito allora esso ha per caratteristica un numero primo.

Osservazione 8.1 Gli anelli $\mathbb{Z}_p$, con p primo, sono campi finiti.

Teorema 8.2 Sia K un campo finito di caratteristica un numero primo p. Allora $\exists n \in \mathbb{N}$ tale che K ha p^n elementi.
Dimostrazione Per l'Osservazione 4.4.3 sappiamo che K contiene una copia isomorfa al campo $\mathbb{Z}_p$, in altre parole $K : \mathbb{Z}_p$. In particolare per l'Osservazione * K è un $\mathbb{Z}_p$-spazio vettoriale; quindi ha una base finita. Posto $n = dim_{\mathbb{Z}_p} K$ prendiamo una base $(b_1, \ldots, b_n)$ di K. Un elemento di K è quindi della forma $\sum_{i=1}^{n} \lambda_i b_i$ con $\lambda_i \in \mathbb{Z}_p$. Osserviamo che per ogni $i = 1, \ldots, n$ il corrispondente λ_i può essere scelto in p modi. Dunque per un semplice calcolo combinatorio si ottiene che K ha p^n elementi. Bisogna però verificare che questi elementi sono tutti distinti; lo sono in quanto i vettori b_i sono una base.

Osservazione 8.3
i) Un campo finito $(K, +, \cdot)$ è in particolare un gruppo finito con la somma e, escluso l'elemento 0, con il prodotto.
ii) K ha necessariamente per caratteristica un numero primo p, cioè l'unità del gruppo $(K, +)$ ha ordine p.

Si riportano quindi ulteriori risultati sui gruppi finiti:

Osservazione 8.4 Sia $(G, \cdot)$ un gruppo finito di k elementi e sia $g \in G$.

Allora

i) L'ordine di g divide k. Infatti essendo G un gruppo finito ogni suo elemento ha un ordine finito. Inoltre l'ordine di g coincide con l'ordine del sottogruppo $\langle g \rangle \subseteq G$; si conclude applicando il Teorema di Lagrange.

ii) $g^k = 1$. Infatti dal punto precedente per ogni $g \in G$ si ha che $k = l \cdot ord(g)$ e quindi $g^k = g^{l \cdot ord(g)} = (g^{ord(g)})^l = 1^l = 1$.

Teorema 8.5 Sia ancora G un gruppo finito di k elementi. Siano $g_1, g_2 \in G$ tali che $ord(g_1), ord(g_2) \in \mathbb{N}$ siano coprimi. Allora $ord(g_1 g_2) = ord(g_1) ord(g_2)$.

Dimostrazione Per compattezza poniamo $ord(g_1) = a$ e $ord(g_2) = b$. Osserviamo che $(g_1 g_2)^{ab} = g_1^{ab} g_2^{ab} = g_1^{a^b} g_2^{b^a} = 1$. Ciò significa che ab è un multiplo dell'ordine di $g_1 g_2$; in particolare l'ordine di $g_1 g_2$ va cercato tra divisori di ab. Essendo a,b coprimi l'insieme dei divisori di ab è costituito solo dagli elementi a, b, ab. Possiamo escludere facilmente le prime due possibilità ottenendo così la tesi.

Teorema 8.6 Sia G un gruppo finito e $g \in G$ un elemento avente ordine $ord(g) = a = bc$. Allora l'elemento $g^c \in G$ ha ordine b. Infatti $(g^c)^b = g^{bc} = g^a = 1$ e dunque otteniamo che $ord(g^c)|b$. Viceversa considerato l'elemento $g^{c \cdot ord(g^c)} = (g^c)^{ord(g^c)} = 1 = g^a$ otteniamo che $a|(c \cdot ord(g^c))$ e quindi esiste un u per cui $c \cdot ord(g^c) = bcu$ e moltiplicando per c^{-1} si ha $ord(g^c) = bu$; cioè $b|ord(g^c)$. Naturalmente $b|ord(g^c) \ \wedge ord(g^c)|b \Rightarrow b = ord(g^c)$.

Teorema 8.7 Sia G un gruppo finito e $g_1, g_2 \in G$ elementi di ordini a,b rispettivamente. Allora esiste un elemento $\overline{g} \in G$ avente ordine $mcm(a, b)$.

Dimostrazione Sia $d = MCD(a, b)$, allora $mcm(a, b) = \frac{ab}{d}$. I numeri $a, \frac{b}{d}$ sono coprimi; inoltre posto $u = \frac{b}{d}$ (e quindi $b = du$) per il Teorema precedente

l'elemento $g_2^d = h$ ha ordine u.

g_1 ha ordine a ed h ha ordine u e tali ordini sono coprimi; quindi l'elemento $g_1 h$ ha ordine au per il Teorema**. Cioè $g_1(g_2^{\frac{b}{d}})$ ha ordine $au = \frac{ab}{d} = mcm(a, b)$.

Teorema 8.8 (Teorema dell'elemento primitivo) Sia K un campo finito. Allora la struttura $K^* = (K \setminus \{0\}, \cdot)$ è un gruppo ciclico. Ovvero $\exists \alpha \in K^*$ tale che $K^* = \{\alpha^n | n \in \mathbb{N}\}$.

Dimostrazione Sia K un campo con n elementi; allora il gruppo $G = (K \setminus \{0\}, \cdot)$ ha n-1 elementi. Consideriamo $S = \{a \in \mathbb{N} | a = ord(g); g \in G\}$ l'insieme i cui elementi sono gli ordini degli elementi di G. Ovviamente $a \leq n-1$ per l'Osservazione * ii). Se riuscissimo a dimostrare che $\exists \alpha \in G | ord(\alpha) = n - 1$ ciò sarebbe sufficiente a dimostrare la tesi.

Sia $e = max(S)$ ed $a \in S$ qualsiasi. Allora il numero $mcm(a, e)$ appartiene ad S per il Teorema precedente e dunque non può essere altro che e; ciò significa che $a|e$ per ogni possibile ordine a di un elemento di G. Allora $\forall \beta \in G$ si ha $ord(\beta)|e$ e quindi $\beta^e = 1$. Quindi il polinomio $x^e - 1$ ha per zero ogni elemento $\beta \in G$. Cioè ha almeno $n - 1$ radici; per il Teorema di D'Alambert $e \geq n - 1$. Dunque si ha $n - 1 \leq e \leq n - 1 \Rightarrow e = n - 1$.

Definizione 8.9 Tale elemento α generatore del gruppo K^* si dice *elemento primitivo*.

Teorema 8.10 Sia K un campo finito di caratteristica p. Allora esiste $q \in \mathbb{Z}_p[x]$ polinomio irriducibile tale che $K \simeq \mathbb{Z}_p[x]/(q)$.

Dimostrazione Sappiamo che $K : \mathbb{Z}_p$. Consideriamo l'omomorfismo $\varphi : \mathbb{Z}_p[x] \to K$ tale che $\varphi|_{\mathbb{Z}_p} = id$ e $\varphi(x) = \alpha$; dove α è l'elemento primitivo

di K.

Osserviamo che $x^n \overset{\varphi}{\mapsto} \alpha^n$, essendo α il generatore di $(K \setminus \{0\}, \cdot)$ al variare di n si ottiene tutto $K \setminus \{0\}$ e $\varphi(0) = 0$; cioè φ è suriettiva. Applicando il II teorema di omomorfismo si ottiene che $\mathbb{Z}_p[x]/ker\ \varphi \simeq K$. Naturalmente $ker\ \varphi$ è un ideale di $\mathbb{Z}_p[x]$; in particolare è principale e quindi esiste un polinomio $q \in K[x]$ per cui $ker\ \varphi = (q)$. Inoltre essendo K un campo isomorfo a $\mathbb{Z}_p[x]/(q)$ anche questo dovrà essere un campo; ma ciò avviene (per il Teorema 4.5.4) se e solo se il polinomio $q \in \mathbb{Z}_p[x]$ è irriducibile.

Osservazione 8.11

i) Per il Teorema dell'elemento primitivo il gruppo $(K^*, \cdot)$ è ciclico; per il Teorema ** esso ha di ordine $p^n - 1$. Dunque per ogni $a \in K \setminus \{0\}$ l'elemento $a^{p^n-1} = 1$. Moltiplicando ambo i membri per a si ricava $a^{p^n} = a$; inoltre tale uguaglianza sussiste anche per l'elemento 0. Si è così ottenuto che $\forall a \in K; a^{p^n} = a$ o ancora $a^{p^n} - a = 0$.

ii) Interpretando $a^{p^n} - a = 0$ come un polinomio di $\mathbb{Z}_p[x]$ valutato in a otteniamo che a è algebrico su $\mathbb{Z}_p$; in quanto per il punto i) il polinomio $x^{p^n} - x$ si annulla per ogni elemento $a \in \mathbb{Z}_p$.

Teorema 8.12 Sia p un numero primo, sia $n \in \mathbb{N}$ fissato. Allora esiste un campo finito di p^n elementi.

Dimostrazione Dati p primo ed $n \in \mathbb{N}$ consideriamo il polinomio $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$. Sia F un campo di riducibilità completa per f, ovvero F contiene tutte le radici di questo polinomio. Sia $K = \{a \in F | f(a) = 0\}$. L'insieme K contiene al più p^n elementi per costruzione. Ne avrà di meno se la molteplicità di (almeno) una radice è maggiore di 1; e ciò accadrebbe

se e solo se nella fattorizzazione di f comparissero fattori multipli. Possiamo utilizzare il criterio esposto nel Teorema 4.4.18: f ha fattori multipli se e solo se $MCD(f, Df)$ non è unitario. Si trova facilmente che $Df = p^n x^{p^n-1} - 1$; trovandoci in $\mathbb{Z}_p[x]$ si ha che $p^n = 0$ e quindi $Df = -1$ e naturalmente $MCD(f, Df) = u$ con u unitario, quindi f non ha fattori multipli e $|K| = p^n$. Si verifica infine che K è un campo; cioè $\forall a, b \in K$ si ha $(a+b)^{p^n} = a + b$ e $(ab)^{p^n} = ab$:
$ab^{p^n} = a^{p^n} b^{p^n} = ab$.
$(a+b)^{p^n} = (a+b)^{p^{p^{p^{\cdots^p}}}}$ che applicando consecutivamente un risultato analogo al Teorema 4.4.7 fa $a^{p^n} + b^{p^n} = a + b$. Per provare che in K ci sono inversi basta osservare che esso è un insieme finito chiuso per le operazioni; quindi in particolare per ogni elemento $c \in K$ esistono $r, s \in \mathbb{N}$ tali che $rc = 0$ e $c^s = 1$; gli inversi addittivi e moltiplicativi di c saranno quindi $(r-1)c$ e c^{s-1} rispettivamente.

Corollario 8.13 Dato $n \in \mathbb{N}$ e p numero primo esiste sempre un polinomio irriducibile di grado n in $\mathbb{Z}_p[x]$

Osservazione 8.14 Se $q \in \mathbb{Z}_p[x]$ è un polinomio irriducibile di grado n allora $q|(x^{p^n} - x)$.
Infatti considerando la proiezione canonica $\pi \colon \mathbb{Z}_p[x] \to \mathbb{Z}_p[x]/(q)$. $\mathbb{Z}_p[x]/(q)$ è un campo e π è un epimorfismo, inoltre $[\pi(x)] = [\pi(x)^{p^n}]$ quindi $\pi((x^{p^n} - x)) = [0] \in \mathbb{Z}_p[x]/(q) \iff x^{p^n} - x \in ker\, \pi = (q)$.

Teorema 8.15 Se K_1, K_2 sono due campi finiti con lo stesso numero di elementi. Allora $K_1 \simeq K_2$.
Dimostrazione Sia K un campo di riducibilità completa per il polinomio

$(x^{p^n} - x) \in \mathbb{Z}_p[x]$. Sia $F = \{a \in K | a^{p^n} = a\}$ il campo che per il Teorema *** ha p^n elementi.

Inoltre esistono $q_1, q_2 \in \mathbb{Z}_p[x]$ polinomi irriducibili di grado n tali che $K_1 \simeq \mathbb{Z}_p[x]/(q_1)$ e $K_2 \simeq \mathbb{Z}_p[x]/(q_2)$. Vogliamo usare K come ponte tra K_1 e K_2, sia quindi $q \in \mathbb{Z}_p[x]$ un polinomio irriducibile di grado n. Per l'Osservazione precedente $q|(x^{p^n} - x)$ cioè esiste un polinomio h per il quale $(x^{p^n} - x) = qh$. Il polinomio $(x^{p^n} - x)$ ha tutte le radici in F,anche q avrà radici in F, sia $\beta \in F$ una radice di q. Consideriamo una funzione $\mathbb{Z}_p[x] \xrightarrow{f} F$ tale che
$a \mapsto a$ per $a \in \mathbb{Z}_p$ e $x \mapsto \beta$. q è irriducibile ed è il polinomio minimo di β su $\mathbb{Z}_p$. $ker\ f = (q) \simeq Im(f) \subseteq F$. Ma $\mathbb{Z}_p/(q)$ ha p^n elementi così come F quindi f è suriettiva. Allora si ha proprio $Im(f) \simeq \mathbb{Z}_p/(q) \simeq F$; $\forall q \in \mathbb{Z}_p[x]$ irriducibile di grado fissato n.

Definizione 8.16 L'unico (a meno di isomorfismi) campo finito di p^n elementi si dice *campo di Galois di p^n elementi* e si denota con $GF(p, n)$.

9 Appendice

Si raccolgono qui alcune nozioni utili che non si potevano inserire coerentemente nella trattazione precedente.

Induzione

Logica

Calcolo combinatorio **Funzuioni biiettive** $f\colon A \to B$ biiettiva $\Rightarrow |A| = |B|$

Insiemi numerabili (Per le estensioni)

Combinazioni e permutazioni

Bionomio di Newton

$(a+b)^p = a^p + b^b$ in $\mathbb{Z}_p$
Se p è primo allora il coefficiente binomiale $\binom{p}{k}$ è divisibile per p. Infatti per definizione $\binom{p}{k} = \frac{p(p-1)\ldots(p-k+1)}{k(k-1)\ldots 2\cdot 1} \in \mathbb{N}$. Ciò significa che il denominatore verrà semplificato effettuando i conti, ma essendo p primo e $k < p$ avremo che p sopravviverà come fattore al numeratore e dividerà quindi il risultato.

Gruppi di permutazioni (Servirà per fare un esempio di applicazione dei teoremi di Sylow)
Definizione Dato un insieme finito $A = \{a_1, a_2, \ldots, a_n\}$ di n elementi si dice *permutazione di A* una funzione biiettiva $\sigma : A \to A$.
L'insieme S_n di tutte le permutazioni su n elementi risulta un gruppo (non commutativo) con l'operazione di composizione tra funzioni e si dice *Gruppo simmetrico di ordine n* o *gruppo di permutazioni su n elementi.* Tale gruppo ha ordine $n!$.

Siccome ogni insieme di n oggetti è in biiezione con l'insieme {1,. . . ,n} gli elementi di A si denotano per semplicità con il numero del loro indice:
$a_1 \equiv 1, \ldots, a_n \equiv n$.

Un elemento σ di S_n si scrive esplicitamente con la notazione $\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$

Definizione Preso un elemento i in {1,. . . ,n} la successione $(i, \sigma(i), \sigma^2(i), \dots, \sigma^{n_i}(i))$ si dice *ciclo di lunghezza* n_i. Qui n_i è il minimo numero di iterazioni per il quale vale l'uguaglianza $\sigma^{n_i}(i) = i$. (E) Perchè esiste tale numero?
Un ciclo τ di lunghezza 2 si dice *scambio* o *trasposizione* e per definizione $\tau^2 = id$

Una permutazione si può sempre scrivere come composizione di cicli; ad esempio la permutazione $\varsigma \in S_4$ definita come $\varsigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$ si può riscrivere come: i) (1, 3, 2) (4) oppure come ii) (1, 3, 2, 4) (1, 4).

Da questo esempio deduciamo che la fattorizzazione in cicli di una permutazione non è unica.

Un ciclo di un solo elemento si dice *singoletto*. Se è specificato l'ambiente in cui si lavora si omette dalla scrittura, così che i) diventa (1, 3, 2).
Si osservi che $\varsigma \in S_4$ scritta così è indistinguibile dalla permutazione (scritta propriamente) in S_3 o dalla permutazione (1, 3, 2) (4) (5), (6), (7) $\in S_7$.
In i) compaiono dei cicli che si dicono *disgiunti*.
Se i cicli sono disgiunti la loro composizione è commutativa, altrimenti no.

Matrici e Linear Algebra (Servirà per i teoremi di Berlekamp)