Dimostrazioni per l'esame di Algebruh

Filippo Troncana, dalle note del professor W. A. De Graaf

A.A. 2022/2023

Indice

1 MCD in $\mathbb{Z}$

DEF. Siano $a, b, d \in \mathbb{Z}$. Allora $d = MCD(a, b) \Leftrightarrow (d|a \wedge d|b) \wedge (c|a \wedge c|b \Rightarrow c|d)$

1.1 Esistenza

Teorema. *Siano $a, b \in \mathbb{Z}$. Allora esiste $d \in \mathbb{Z} : d = MCD(a, b)$ ed esistono $s, t \in \mathbb{Z} : d = sa + tb$*

Dimostrazione. Se $a = b = 0$ prendiamo banalmente $d = 0$ e $s = t = 0$. Altrimenti definiamo l'insieme:

$$I = \{xa + yb : x, y \in \mathbb{Z}\}$$

e indichiamo con I^+ il sottoinsieme degli elementi strettamente positivi di I. Per il principio del buon ordinamento, essendo un sottoinsieme di $\mathbb{N}$ ha un minimo che chiamiamo $d = (sa + tb)$.
Dimostriamo che $d|a$ e in modo assolutamente analogo avremo $d|b$. Facciamo una divisione con resto e otteniamo $q, r \in \mathbb{Z}$ tali che $r = a - qb$ e $0 \leq r < d$. Se avessimo $r \neq 0$ allora apparterrebbe a I^+, ma contraddirrebbe l'ipotesi di minimalità di d, quindi abbiamo $r = 0$ e $qd = a \Leftrightarrow d|a$.
Ora prendiamo $c \in \mathbb{Z}$ tale che $c|a$ e $c|b$. Allora abbiamo che $a = a_0c$ e $b = b_0c$ per qualche $a_0, b_0 \in \mathbb{Z}$ e che $d = (sa_0 + tb_0)c$, quindi automaticamente abbiamo $c|d$. QED

1.2 Gli MCD sono associati

Teorema. *Siano $a, b, d, d' \in \mathbb{Z}$ tali che $d = MCD(a, b)$ e $d' = MCD(a, b)$. Allora d e d' sono associati, ovvero $d = \pm d'$*

Dimostrazione. Prendiamo $a, b, d, d' \in \mathbb{Z}$ tali che $d = MCD(a, b)$, $d' = MCD(a, b)$. Segue automaticamente che d|d' e d'|d, quindi $d = \pm d'$. QED

Per convenzione e semplicità prendiamo il valore positivo tra i due MCD di due numeri, permettendo di definirlo come funzione $\mathbb{Z}^2 \to \mathbb{Z}$

2 Fattorizzazione di polinomi

DEF. Dato un insieme $(\mathbb{F}, +, \times)$ dotato di due leggi di composizione interna tali che esso sia un anello e $(\mathbb{F}\backslash\{0\}, \times)$ sia un gruppo abeliano. allora $(\mathbb{F}, +, \times)$ si dice **campo**.

Teorema. *Sia $(\mathbb{F}, +, \times)$ un campo e $\mathbb{F}[x]$ l'anello dei suoi polinomi. Sia $f \in \mathbb{F}[x]$ un polinomio tale che esista $a \in \mathbb{F}$ tale che $f(a) = 0$. Allora si ha che $(x - a)|f$.*

Dimostrazione. Prendiamo $f \in \mathbb{F}[x]$ e $a \in \mathbb{F}$ tale che $f(a) = 0$. Eseguiamo una divisione con resto e otteniamo $q, r \in \mathbb{F}[x]$ tali che $f = q \times (x - a) + r$ e $0 \leq \deg r < \deg(x-a) = 1 \Rightarrow r \in \mathbb{F}$. Allora si ha che $f(a) = q(a) \times (a-a) + r = 0 + r = 0 \Rightarrow r = 0 \Rightarrow (x - a)|f$ QED

3 Fattorizzazione in un dominio con norma

DEF. Sia $(\mathbb{D}, +, \times)$ un dominio. $a \in \mathbb{D}$ si dice **irriducibile** in $\mathbb{D}$ se non è 0, non è invertibile e se $a = bc$ implica che b o c sia invertibile

Osservazione. Essendo a non invertibile per ipotesi, solo uno dei due può essere invertibile.

Teorema. Sia $(\mathbb{D}, +, \times)$ un dominio dotato di una funzione $\nu : \mathbb{D}\backslash\{0\} \to \mathbb{N}$ (che chiameremo norma nel corso della nostra trattazione) tale che $\nu(ab) > \nu(b)$ per ogni a non invertibile. Ogni elemento non zero e non invertibile di $\mathbb{D}$ può essere scritto come prodotto di irriducibili

Dimostrazione. Sia $S \subset \mathbb{D}$ l'insieme degli $a \in \mathbb{D}$ diversi da zero e non invertibili che non possono essere scritti come prodotto di irriducibili, e supponiamolo non vuoto. Chiaramente gli elementi di S non possono essere essi stessi irriducibili. Con un abuso di notazione paragonabile al mio abuso di sostanze stupefacenti, sia $\nu(S) \subseteq \mathbb{N}$ l'insieme dei valori della norma di elementi di S, chiaramente non vuoto.

In quanto sottoinsieme non vuoto di $\mathbb{N}$, deve avere un minimo che chiamiamo n_0, al quale deve corrispondere $a_0 \in S$ tale che $\nu(a_0) = n_0$. Visto che a_0 non può essere irriducibile nè prodotto di irriducibili, può essere scritto come $a_0 = b_0 c_0$ per qualche b_0 e c_0 in $\mathbb{D}$.

Sia b_0 che c_0 però devono appartenere a S, perchè nessuno dei due può essere invertibile e se fossero irriducibili o prodotto di irriducibili allora a_0 stesso lo sarebbe. Ma allora avremmo $n_0 = \nu(a_0) = \nu(b_0c_0)$ quindi per ipotesi maggiore sia di $\nu(b_0)$ che di $\nu(c_0)$, entrambi elementi di $\nu(S)$, che allora deve essere vuoto (in quanto sottoinsieme di $\mathbb{N}$ che abbiamo dimostrato non avere minimo) e implica evidentemente che anche S sia vuoto. QED

4 Fattorizzazione essenzialmente unica se e solo se primalità di ogni irriducibile

DEF. Sia $(\mathbb{D}, +, \times)$ un dominio. $a \in \mathbb{D}$ si dice **primo** se è diverso da zero, non è invertibile e $a|bc$ implica che $a|b$ o $a|c$.

Osservazione. Una definizione un po' meno intuitiva rispetto alla solita, ma permette un'estensione più semplice oltre ai numeri primi in $\mathbb{Z}$.

DEF. Sia $(\mathbb{D}, +, \times)$ un dominio in cui ogni elemento a non zero e non invertibile si può scrivere come prodotto di irriducibili, ovvero $a = p_1...p_s$, con p_i irriducibile per ogni i. Una scrittura di questo tipo si dice **fattorizzazione** di a. Questa fattorizzazione si dice **essenzialmente unica** se data una qualsiasi altra fattorizzazione $a = q_1...q_t$, si ha $s = t$ ed esiste un ordine in cui p_i e q_i sono associati per ogni i. (Un dominio a fattorizzazione unica si indica per brevità con UFD, *Unique Factorization Domain.*

Teorema. Sia $(\mathbb{D}, +, \times)$ un dominio in cui ogni elemento diverso da zero e non invertibile può essere scritto come prodotto di irriducibili. Ogni fattorizzazione in $\mathbb{D}$ è essenzialmente unica se e solo se ogni irriducibile in $\mathbb{D}$ è anche primo.

Dimostrazione. Come di consueto, dividiamo in due parti la dimostrazione per dimostrare l'implicazione in entrambe le direzioni.
"UFD $\Rightarrow$ primalità degli irriducibili"
Supponiamo che $(\mathbb{D}, +, \times)$ sia un dominio a fattorizzazione unica e prendiamo un irriducibile qualsiasi $a \in \mathbb{D}$ per dimostrare che è primo. Supponiamo $a|bc$ per qualche $b, c \in \mathbb{D}$, dunque esiste $d \in \mathbb{D}$ tale che $bc = ad$.
Scriviamo le fattorizzazioni di bc e ad:

$$b_1...b_rc_1...c_s = ad_1...d_t$$

Per definizione di UFD, esistono i e j tali che a sia associato a b_i oc_j, supponiamo dunque $b_i = ua$ con $u \in \mathbb{D}$ invertibile, dunque si ha $a|b$, analogamente si ha che nel caso di c_j abbiamo $a|c$, perciò abbiamo che a è primo.
"Primalità degli irriducibili $\Rightarrow$ UFD"
Supponiamo che ogni irriducibile in $\mathbb{D}$ sia primo e prendiamo $a \in \mathbb{D}$ e due sue fattorizzazioni, ovvero $a = p_1...p_m = q_1...q_n$.
Possiamo assumere senza perdita di generalità che $n \geq m$. Dato che p_1 è primo, deve dividere almeno un q_i, quindi dopo aver riordinato in modo che si

abbia $i = 1$ possiamo scrivere $q_1 = u_1 p_1$. Ma essendo q_1 irriducibile, si ha che u_1 deve essere invertibile. Otteniamo l'equazione $p_2 ... p_m = u_1 q_2 ... q_n$, dove p_2 non può dividere u_1 perchè altrimenti sarebbe invertibile. Continuiamo per m passi finchè non otteniamo l'uguaglianza $1 = u_1 ... u_m q_{m+1} ... q_n$. $n > m$ implicherebbe $q_n | 1$, dunque sarebbe invertibile quando per definizione è irriducibile, dunque abbiamo necessariamente $n = m$, e $p_i = u_i q_i$ per ogni i, dunque ogni fattorizzazione è unica. QED

5 Fattorizzazione in dominio euclideo

DEF. Sia $(\mathbb{D}, +, \times)$ un dominio nel quale è possibile definire una norma $\nu : \mathbb{D} \setminus \{0\} \to \mathbb{N}$ tale che $\forall a, b \in \mathbb{D}, \nu(ab) \geq \nu(a)$ e tale che è possibile eseguire la divisione con resto, ovvero $\forall a, b \in \mathbb{D}, \exists q, r \in \mathbb{D} : \nu(r) < \nu(b)$ e $a = qb + r$. Allora $(\mathbb{D}, +, \times)$ si dice **dominio euclideo**.

Teorema. Sia $(\mathbb{D}, +, \times)$ un dominio euclideo. Allora ogni $a \in \mathbb{D}$ non zero e non invertibile si può scrivere come prodotto di irriducibili.

Suggerimento. Si può usare il teorema 3 senza fornirne la dimostrazione.

Dimostrazione. Sia $(\mathbb{D}, +, \times)$ un dominio euclideo, e $a, b \in \mathbb{D}$ diversi da zero e a non invertibile. Allora esistono $q, r \in \mathbb{D}$ tali che $b = qab + r$ con $r = 0$ oppure $\nu(r) < \nu(ab)$. Se avessimo $r = 0$, allora avremmo $1 = qa$ e dunque a sarebbe invertibile, in contraddizione con l'ipotesi, dunque r deve essere diverso da zero. Dunque abbiamo $\nu(ab) > \nu(r) = \nu(b(1 - qa) \geq \nu(b)$, ovvero $\nu(ab) > \nu(b)$ e quindi otteniamo le ipotesi del teorema 3 che garantisce la fattorizzazione in irriducibili. QED

6 Primalità degli irriducibili in un dominio euclideo

Teorema. Sia $(\mathbb{D}, +, \times)$ un dominio euclideo. Ogni irriducibile in $\mathbb{D}$ è primo.

Dimostrazione. Sia $(\mathbb{D}, +, \times)$ e $a, b, c, d \in \mathbb{D}$ tali che a sia irriducibile e $a | bc$ e $d = MCD(a, b)$, allora si ha che $d | a$ e dunque $a = ud$, ma essendo a irriducibile almeno uno tra u e d deve essere invertibile.
Assumendo u invertibile abbiamo $a | d$ e dunque $a | b$.
Assumendo d invertibile, scriviamo $d = sa + tb$ con opportuni $s, t \in \mathbb{D}$. Dunque abbiamo $1 = d^{-1} sa + d^{-1} tb$ e quindi $c = d^{-1} sac + d^{-1} tbc$. Dato che $a | bc$, abbiamo che esiste $v \in \mathbb{D}$ tale che $bc = va$, dunque abbiamo $c = d^{-1} sac + d^{-1} tva$, ovvero $c = (d^{-1} sc + d^{-1} tv) a$ e quindi $a | c$. QED

7 Struttura di campo di $\mathbb{Z}/p\mathbb{Z}$

DEF. Dato $n \in \mathbb{Z}$ definiamo come **conguenza modulo n** la relazione di equivalenza in $\mathbb{Z}$ data da $a \equiv b \mod n \Leftrightarrow n|(a-b)$

DEF. Dato $n \in \mathbb{Z}$ indichiamo con $\mathbb{Z}/n\mathbb{Z}$ **l'insieme delle classi di congruenza modulo n**.

Lemma. Dato $n \in \mathbb{Z}$ e l'insieme $\mathbb{Z}/n\mathbb{Z}$ delle classi di congruenza modulo n, esso ha esattamente n elementi, e può essere scritto come $\{[0], ..., [n-1]\}$.

Lemma. Dato $n \in \mathbb{Z}$ e l'insieme $\mathbb{Z}/n\mathbb{Z}$ delle classi di congruenza modulo n, possiamo definire una somma e un prodotto in esso:

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

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

Date queste operazioni, $\mathbb{Z}/n\mathbb{Z}$ è un anello commutativo con unità $[1]$.

Teorema. Sia $p \in \mathbb{Z}$ un numero primo. $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ *è un campo.*

Dimostrazione. Sia $p \in \mathbb{Z}$ un numero primo e $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ l'insieme delle classi di congruenza modulo p. Data la struttura di anello commutativo con unità $[1]$, basta dimostrare che ogni elemento diverso da $[0]$ possiede un inverso moltiplicativo.
Prendiamo $a \in \mathbb{Z}$ tale che $[a] \neq [0]$, allora si ha che $MCD(a,p) = 1$ e perciò esistono $s, t \in \mathbb{Z}$ tali che $sa + tp = 1$, dunque $[s][a] + [t][0] = [1]$ e perciò $[s][a] = [1]$. QED

DEF. Sia $p \in \mathbb{Z}$ un numero primo. Indichiamo il campo $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ con $\mathbb{F}_p$

8 Criterio di Eisenstein

Lemma (Lemma di Gauss). *Sia $f \in \mathbb{Z}[x]$ e supponiamo che esistano $g, h \in \mathbb{Q}[x]$ tali che* $\deg(g), \deg(h) > 0$ *e $f = gh$. Allora esistono $\alpha, \beta \in \mathbb{Q}$ tali che $\alpha g, \beta h \in \mathbb{Z}[x]$ e $f = (\alpha g)(\beta h)$*

Teorema. Sia $f = a_0, ..., a_n x^n \in \mathbb{Z}[x]$, e supponiamo che esista $p \in \mathbb{Z}$ primo tale che p divida tutti i coefficienti tranne a_n e p^2 non divida a_0. Allora f è irriducibile in $\mathbb{Q}[x]$

Dimostrazione. Consideriamo la mappa $\psi_p : \mathbb{Z}[x] \to \mathbb{F}_p[x]$ data da $\psi_p(b_0 + ... + b_n x^n) = [b_0]_p + ... + [b_n]_p x^n$. Essa è ben definita ed omomorfismo di anelli per la definizione delle operazioni nei vari anelli considerati.
Supponiamo che $f = a_0 + ... + a_n x^n \in \mathbb{Z}[x]$ sia riducibile e che esista il primo p

di cui sopra, dunque per il lemma di Gauss esistono $g, h \in \mathbb{Z}[x]$ tali che $f = gh$ con $\deg(g), \deg(h) \geq 1$. Per le ipotesi su p, abbiamo che $\psi_p(f) = [a_n]_p x^n$ ma anche che $\psi_p(gh) = \psi_p(g)\psi_p(h)$. per la fattorizzazione unica, abbiamo che $\psi_p(g) = [b_r]_p x^r$ e $\psi_p(h) = [c_s]_p x^s$, dunque abbiamo che $p|b_0$ e $p|c_0$, ma quindi avremmo che $p^2|a_0$, escluso per ipotesi, dunque f è irriducibile. QED

9 Teorema del resto cinese

DEF. Siano R, S due anelli. definiamo il **prodotto diretto** $R \times S$ come l'insieme $\{(r, s)|r \in R, s \in S\}$ con le seguenti operazioni:

$$(a, b) + (c, d) = (a + c, b + d)$$

$$(a, b) \times (c, d) = (a \times c, b \times d)$$

Chiaramente con queste operazioni, $R \times S$ è un anello a sua volta.

DEF. Siano R, S due anelli e $f : R \to S$ un omomorfismo tra loro. Il **nucleo** di f è l'insieme degli elementi $a \in R$ tali che $f(a) = 0$. Lo indichiamo con $\ker(f)$.

Lemma. Siano R, S due anelli e $f : R \to S$ un omomorfismo tra loro. Allora f è iniettivo se e solo se $\ker(f) = \{0\}$.

Teorema. Siano $m, n \in \mathbb{Z}^+$ tali che $MCD(m, n) = 1$. Allora esiste un isomorfismo σ di anelli definito come:

$$\sigma : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

$$[a]_{mn} \to ([a]_m, [a]_n)$$

Dimostrazione. Supponiamo la situazione dell'ipotesi. Immediatamente abbiamo che σ è un omomorfismo, per la definizione delle operazioni nei vari anelli (è lunga da scrivere come cosa quindi io la ometto ma è davvero banale).
Dimostriamo che $\ker(\sigma) = \{0\}$. Sia $[a]_{mn} \in \mathbb{Z}/mn\mathbb{Z}$ tale che $\sigma([a]_{mn}) = ([0]_m, [0]_n)$, allora per definizione si ha che $m|a$ e $n|a$, ed essendo m e n coprimi, $mn|a$ e dunque $[a]_{mn} = [0]_{mn}$.
Dimostrata l'iniettività di σ, notiamo che in quanto mappa iniettiva tra insiemi finiti, è suriettiva se e solo se dominio e codominio hanno la stessa cardinalità, cosa abbastanza evidente:

$$|\mathbb{Z}/mn\mathbb{Z}| = mn = |\mathbb{Z}/m\mathbb{Z}||\mathbb{Z}/n\mathbb{Z}| = |\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}|$$

QED

10 Sistema RSA

10.1 Piccolo teorema di Fermat e corollario

Teorema. Sia $p \in \mathbb{Z}$ un numero primo e $a \in \mathbb{Z}$ tale che p non divide a. Allora si ha che $a^p \equiv a \mod p$.

Corollario 1. *Sia $p \in \mathbb{Z}$ un numero primo e $a \in \mathbb{Z}$ tale che p non divide a. Allora si ha che $a^{p-1} \equiv 1 \mod p$.*

Dimostrazione. Dimostriamo il teorema per induzione su $a \in \mathbb{N}$, perchè se avessimo $a < 0$ potremmo scrivere $a = -b$ con $b \in \mathbb{N}$ e con p dispari avremmo $a^p \equiv -b^p \equiv -b \mod p \equiv a \mod p$, mentre con $p = 2$ avremmo $a^2 = b^2 = b \mod 2 = a \mod 2$.
. Il caso $a = 0$ è banale, quindi supponiamo $a \in \mathbb{N}$ e $a^p \equiv a \mod p$. Allora dimostriamo $(a+1)^p \equiv a+1 \mod p$:

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + ... + \binom{p}{p-1} a + 1$$

Per $1 \leq i \leq p-1$ abbiamo che $p! = \binom{p}{i}(p-i)!i!$, ma dato che p ovviamente non divide nè $(p-i)!$ nè $i!$, necessariamente $p|\binom{p}{i}$, dunque abbiamo $(a+1) \equiv a+1 \mod p$, dimostrando il teorema per ogni $a \in \mathbb{N}$. QED

Dimostrazione. Dimostriamo il corollario: per il teorema precedente, p divide $a^p - a = a(a^{p-1} - 1)$, ma dato che non divide a per ipotesi abbiamo automaticamente la tesi.

10.2 $a^{x\varphi(pq)+1} = a \mod pq$

Teorema. Siano $p, q \in \mathbb{Z}$ due primi distinti e definiamo la funzione $\varphi(pq) = (p-1)(q-1)$. Sia $x \in \mathbb{N}\backslash\{0\}$. Allora per ogni $a \in \mathbb{Z}$, si ha che $a^{x\varphi(pq)+1} = a \mod pq$.

Dimostrazione. Dimostriamo in primo luogo che p divide $a^{x\varphi(pq)+1} - a$.
Se $p|a$ allora è evidente, altrimenti dimostriamo che p divide $a^{x(p-1)(q-1)} - 1$. Chiamiamo $A = a^{x(q-1)}$, chiaramente non un multiplo di p indipendentemente dal valore di x, quindi per il piccolo teorema di Fermat si ha che $A^{(p-1)} - 1 \equiv 0 \mod p$.
Analogamente per q. QED

10.3 Conseguenze per il sistema RSA

Ma questa cosa perchè è utile per il sistema RSA? Beh, innanzitutto, come si cripta un messaggio in RSA?

Algoritmo. Per criptare un messaggio in RSA è necessario:

1. *Assegnare un valore numerico a ognuno dei simboli possibili presenti nel messaggio, da* 0 *a* $k-1$*, dove* k *è il numero di simboli possibili.*
2. *Riscrivere il proprio messaggio come sequenza di numeri.*
3. *Scegliere due numeri primi distinti* p *e* q*, più grandi sono meglio è, e calcolare* $n = pq$ *e* $\varphi(n) = (p-1)(q-1)$*.*
4. *Scegliere un* r *tale che* $1 < r < \varphi(n)$ *e che sia coprimo a* $\varphi(n)$
5. *Con l'algoritmo di Euclide esteso, calcoliamo* s *e* t *tali che* $0 < s < \varphi(n)$ *e* $st + t\varphi(n) = 1$*.*
6. *Definiamo la coppia* (r, n) ***chiave pubblica*** *e la coppia* (s, n) ***chiave privata****.*
7. *Dunque criptiamo l'intero* $0 \leq a < n$ *come l'intero* $0 \leq b < n$ *calcolando* $b \equiv a^r \mod n$ *e lo decriptiamo successivamente calcolando* $a \equiv b^s \mod n$

Dimostrazione informale. Adesso supponiamo $p, q, r, s, n, \varphi(n)$ come sopra. Visto che assumiamo r e s positivi, t deve essere necessariamente negativo, dunque abbiamo:

$$(a^r)^s = a^{rs} = a^{-t\varphi(n)+1} \equiv a \mod n$$

Da ciò segue la correttezza dell'algoritmo, ovvero che criptazione e decriptazione sono inverse. QED

11 Omomorfismi

DEF. Sia $(R, +, \times)$ un anello. Un insieme $I \subseteq R$ si dice **ideale** se contiene lo zero, per ogni $a, b \in I$ si ha che $a - b \in I$ e per ogni $a \in R$ e $b \in I$ si ha che $ab, ba \in I$.

DEF. Sia $(R, +, \times)$ un anello e I un suo ideale. Definiamo la relazione di equivalenza $a \equiv b \Leftrightarrow a - b \in I$. Indichiamo la classe di equivalenza di un generico elemento $a \in R$ come $a + I$. L'insieme di queste classi di equivalenza è detto **quoziente** di R e I e si indica come R/I.

Lemma. Sia $(R, +, \times)$ *un anello e* I *un suo ideale. Allora* R/I *eredita da* R *le definizioni di somma e prodotto e la struttura di anello:*

$$(a + I) + (b + I) = (a + b) + I$$

$$(a + I)(b + I) = ab + I$$

11.1 Idealità del nucleo

Teorema. Siano R, S due anelli, e sia $f : R \to S$ un omomorfismo tra loro. Il nucleo di f è un ideale di R.

Dimostrazione. Prendiamo $a, b \in \ker(f)$, segue automaticamente che in quanto omomorfismo tra anelli si ha $f(a-b) = f(a) - f(b) = 0$, dunque $a - b \in \ker(f)$.
Allo stesso modo, $f(0) = f(a-a) = f(a) - f(a) = 0$, perciò $0 \in \ker(f)$
Infine, prendiamo un qualsiasi $k \in R$, abbiamo $f(ka) = f(k)f(a) = 0f(k) = 0$, perciò $ka \in \ker(f)$ (analogamente per ak). QED

11.2 Iniettività in $S/\ker(f)$

Teorema. Siano R, S due anelli, e sia $f : R \to S$ un omomorfismo tra loro. Allora f induce un omomorfismo iniettivo $\hat{f} : R/\ker(f) \to S$ definito come $\hat{f}(a + \ker(f)) = f(a)$

Dimostrazione. Dimostriamo innanzitutto che $\hat{f}$ è ben definito: prendiamo $a, b \in R$ tali che $a \equiv b$ e tentiamo di dimostrare $\hat{f}(a+\ker(f)) = \hat{f}(b+\ker(f)$. Abbiamo che $a - b \in \ker(f)$, dunque $\hat{f}(a + \ker(f)) - \hat{f}(b + \ker(f)) = \hat{f}(a + \ker(f) - b + \ker(f)) = f(a - b) = 0$, perciò $\hat{f}(a + \ker(f)) = \hat{f}(b + \ker(f))$.
Il fatto che $\hat{f}$ sia un omomorfismo segue immediatamente dalla struttura di anello di $R/\ker(f)$ ereditata da R.
Ora dimostriamo che è iniettiva, ovvero che il suo nucleo è $\{0 + \ker(f)\}$. Prendiamo $a + \ker(f) \in \ker(\hat{f})$, allora abbiamo $a \in \ker(f)$, quindi $a \equiv 0$. QED

12 Dominio euclideo $\Rightarrow$ PID

DEF. Sia $(\mathbb{D}, +, \times)$ un dominio. Un ideale I di $\mathbb{D}$ si dice **principale** se è della forma $I = \{ba : b \in \mathbb{D}\}$ con $a \in \mathbb{D}$ fissato, e si indica con $\langle a \rangle$.

DEF. Sia $(\mathbb{D}, +, \times)$ un dominio. Si dice **a ideali principali** (per brevità PID, *Principal Ideals Domain*) se tutti i suoi ideali sono principali.

Teorema. Sia $(\mathbb{D}, +, \times)$ un dominio euclideo. Allora $\mathbb{D}$ è un dominio a ideali principali.

Dimostrazione. Siano $(\mathbb{D}, +, \times)$ un dominio euclideo e $\nu : \mathbb{D}\backslash\{0\} \to \mathbb{N}$ come da definizione. Prendiamo un ideale $I \subseteq \mathbb{D}$.
Se $I = \{0\}$, automaticamente $I = \langle 0 \rangle$. Altrimenti contiene elementi non zero.
Sia $S = \nu(I\backslash\{0\})$. In quanto sottoinsieme di $\mathbb{N}$, possiede un minimo che chiamiamo m_0, quindi prendiamo $b \in I\backslash\{0\}$ tale che $\nu(b) = m_0$. Sia $a \in I\backslash\{0\}$ ed eseguiamo la divisione con resto, quindi troviamo $s, r \in \mathbb{D}$ con $\nu(r) < \nu(b)$ oppure $r = 0$ tali che $a = qb + r$. Allora avremmo $r = a - qb$ con $a, qb \in I$,

da cui segue $r \in I$, ma per la scelta di minimalità di $\nu(b)$ necessariamente si ha $r = 0$, perciò per ogni $a \in I$ si ha che $a = qb$ e perciò $I = \langle b \rangle$. QED

13 Primalità di un ideale se e solo se quoziente è dominio

DEF. Sia $(\mathbb{A}, +, \times)$ un anello commutativo unitario e $I \subseteq \mathbb{A}$ un suo ideale. Allora I si dice **primo** se è un sottoinsieme proprio di $\mathbb{A}$ e per ogni $ab \in I$ si ha $a \in I$ oppure $b \in I$.

> *Teorema. Sia $(\mathbb{A}, +, \times)$ un anello commutativo unitario e $I \subseteq \mathbb{A}$ un suo ideale. Allora I è primo se e solo se $\mathbb{A}/I$ è un dominio.*

Dimostrazione. Supponiamo che I sia primo. Abbiamo che R/I è già un anello commutativo e unitario, quindi ci basta dimostrare $1 \not\equiv 0$ e che non ci sono divisori dello zero. Innanzitutto, $1 \equiv 0$ implicherebbe direttamente $1 \in I$, dunque avremmo $I = \langle 1 \rangle = \mathbb{A}$, assurdo, quindi $1 \not\equiv 0$. Supponiamo $a, b \in \mathbb{A}$ tali che $ab \equiv 0$, ma quindi avremmo $ab \in I$, dunque avremmo $a \equiv 0$ o $b \equiv 0$.
Ora supponiamo che $\mathbb{A}/I$ sia un dominio. Abbiamo automaticamente $1 \not\equiv 0$, dunque $I \subset \mathbb{A}$. Siano $a, b \in \mathbb{A}$ tali che $ab \equiv 0$, ma non essendoci divisori dello zero abbiamo $a \equiv 0$ o $b \equiv 0$. QED

14 Massimalità di un ideale se e solo se quoziente è campo

DEF. Sia $(\mathbb{A}, +, \times)$ un anello commutativo unitario e $I \subseteq \mathbb{A}$ un suo ideale. Allora I si dice **massimale** se è un sottoinsieme proprio di $\mathbb{A}$ e gli unici ideali di $\mathbb{A}$ in cui è contenuto sono sè stesso ed $\mathbb{A}$.

> *Teorema. Sia $(\mathbb{A}, +, \times)$ un anello commutativo unitario e $I \subseteq \mathbb{A}$ un suo ideale. Allora I è massimale se e solo se $\mathbb{A}/I$ è un campo.*

Dimostrazione. Supponiamo I massimale. Abbiamo gratis che $\mathbb{A}/I$ è un anello commutativo e unitario, dunque basta dimostrare che $1 \not\equiv 0$, che ogni elemento non zero ha un inverso moltiplicativo. Come sopra, $1 \equiv 0$ implicherebbe $I = \mathbb{A}$, già escluso, dunque $I \not\equiv 0$. Prendiamo $a \in \mathbb{A}$ tale che $a \not\equiv 0$ e $J = I + \langle a \rangle$. Automaticamente $I \subset J$ e $I \neq J$, dunque $J = \mathbb{A}$, quindi abbiamo $c \in I$ e $b \in R$ tali che $c + ab = 1$, dunque $ab \equiv 1 - c \equiv 1$.
Adesso supponiamo che $\mathbb{A}/I$ sia un campo. Abbiamo subito $1 \not\equiv 0$ e quindi $I \not\equiv \mathbb{A}$. Sia $J \subseteq \mathbb{A}$ un ideale tale che $I \subseteq J \subseteq \mathbb{A}$ e supponiamo $I \neq J$. Prendiamo $a \in J \backslash I$ e dato che $\mathbb{A}/I$ è un campo, esiste $b \in \mathbb{A}$ tale che $ab \equiv 1 \equiv 1 + c$ per ogni $c \in I$, dunque abbiamo $ab \in J$, dunque $ab - c \in J$ e quindi $1 \in J$, perciò abbiamo $J = \mathbb{A}$. QED