ALGEBRA I: ARITMETICA MODULARE E QUOZIENTI DI ANELLI

1. Classi di resto e divisibilità

In questa parte sarò asciuttissimo, e scriverò solo le cose essenziali. I commenti avete potuto ascoltarli a lezione.

Definizione 1.1. Se a, b sono elementi di un anello A, si dice che a *divide* b — e si indica con la notazione $a|b$ — se esiste $x \in A$ tale che $b = ax$.

Osservazione 1.2. La relazione di divisibilità è transitiva: se $a|b$ e $b|c$, allora esistono x, y tali che $b = ax, c = by$ e quindi $c = (ax)y = a(xy)$.

Inoltre, in un dominio d'integrità, se $c \neq 0$, si ha $a|b \Leftrightarrow ac|bc$: se $b = ax$, allora moltiplicando per c si ottiene $bc = (ax)c = (ac)x$; viceversa, se $bc = (ac)x$, allora $c(b - ax) = 0$ e poiché $c \neq 0$ si ottiene $b = ax$. Quando $a|b$ si dice anche che b è un *multiplo* di a.

Lemma 1.3. *Siano a, b, c elementi di un anello A. Se $a|b, a|c$, allora $a|bh \pm ck$ per ogni $h, k \in A$.*

Dimostrazione. Se $a|b, a|c$, allora esistono $x, y \in A$ tali che $b = ax, c = ay$. Ma allora $bh \pm ck = (ax)h \pm (ay)k = a(xh \pm yk)$ è un multiplo di a. □

Noi saremo interessati principalmente all'anello dei numeri interi, che è un dominio d'integrità.

Definizione 1.4. Sia $n \in \mathbb{N}, n > 1$. Due elementi $a, b \in \mathbb{Z}$ si dicono *congrui* o *congruenti modulo* n se $n|b - a$. Questo fatto si indica con la notazione $a \equiv b \mod n$.

Proposizione 1.5. *La relazione di congruenza modulo n è di equivalenza.*

Dimostrazione. Riflessività: $a \equiv a \mod n$, in quanto $n \mid 0 = a - a$.
Simmetria: se n divide $b - a$, allora divide anche $a - b = -(b - a)$; quindi $a \equiv b \mod n \Rightarrow b \equiv a \mod n$.
Transitività: se n divide $b - a$ e $c - b$ divide anche la loro somma $c - a = (c - b) + (b - a)$. Questo mostra che da $a \equiv b \mod n$ e $b \equiv c \mod n$ segue anche $a \equiv c \mod n$. □

L'insieme quoziente di $\mathbb{Z}$ per la relazione di congruenza modulo n si indica con $\mathbb{Z}/(n)$.

Lemma 1.6. *$\mathbb{Z}/(n)$ contiene esattamente n elementi.*

Dimostrazione. Gli elementi $0, 1, \ldots, n - 1$ appartengono a classi di equivalenza distinte, in quanto da $0 \leq a, b < n$, $a \neq b$, si ricava $0 \neq |a - b| < n$, quindi $a - b$ non può essere multiplo di n.

Per vedere che ogni elemento $a \in \mathbb{Z}$ giace in una delle classi di equivalenza $[0], [1], \ldots, [n - 1]$, basta utilizzare la divisione euclidea:

$$a = nq + r, \quad 0 \leq r < n,$$

per concludere che $a \equiv r \mod n$. □

Proposizione 1.7. *Se $a \equiv a' \mod n$ e $b \equiv b' \mod n$, allora $a + b \equiv a' + b' \mod n$ e $ab \equiv a'b' \mod n$. Di conseguenza, le operazioni $[a] + [b] = [a + b], [a] \cdot [b] = [ab]$ sono ben definite in $\mathbb{Z}/(n)$.*

Dimostrazione. Le ipotesi sono equivalenti a dire che $n|a' - a, n|b' - b$. Ma allora $n|(a' - a) + (b' - b) = (a' + b') - (a + b)$, cioè $a + b \equiv a' + b' \mod n$. Inoltre $n|(a' - a)b' + a(b' - b) = a'b' - ab$, cioè $ab \equiv a'b' \mod n$. □

Teorema 1.8. *Se $n > 1$, $\mathbb{Z}/(n)$, dotato delle operazioni di somma e prodotto ereditate da $\mathbb{Z}$, è un anello commutativo con unità.*

Dimostrazione. Le proprietà di commutatività, associatività e distributività delle operazioni discendono da quelle di $\mathbb{Z}$. L'elemento neutro rispetto alla somma è $[0]$, mentre l'unità è $[1]$. L'inverso additivo di $[a]$ è chiaramente $[-a]$. □

Osservazione 1.9. Se $n = 1$, $\mathbb{Z}/(n)$ contiene un solo elemento. Una delle richieste che facciamo ad un anello con unità è che l'elemento neutro 0 rispetto all'addizione e l'elemento neutro 1 rispetto alla moltiplicazione siano diversi tra loro. Questo è l'unico motivo per il quale $\mathbb{Z}/(1)$, che è un anello, non può essere un anello commutativo con unità.
L'anello $\mathbb{Z}/(0)$ è isomorfo a $\mathbb{Z}$, in quanto due interi sono congrui modulo 0 se e solo se coincidono. L'anello $\mathbb{Z}/(n)$ non è quindi un oggetto algebrico nuovo quando $n = 0$.
Infine, la congruenza modulo n e quella modulo $-n$ sono concetti equivalenti, quindi non c'è alcuna necessità di considerare congruenze modulo interi negativi.

2. Identità di Bézout e numeri primi

Qui richiamo alcune proprietà della divisibilità dei numeri interi che sono dimostrate in appunti precedentemente scritti:

Definizione 2.1. $0 \neq d \in \mathbb{Z}$ è un *massimo comun divisore* di $a, b \in \mathbb{Z}$ — e si indica con la notazione $d = (a, b)$ — se

- $d|a, d|b$;
- se $d'|a, d'|b$, allora $d'|d$.

In altri termini, d è un divisore comune di a e b che è diviso da ogni altro divisore comune.

Osservazione 2.2. Si noti che se d è un massimo comun divisore di a, b, allora anche $-d$ è un massimo comun divisore. Per la definizione data, il massimo comun divisore di due elementi non è unico, ed in realtà non è neanche chiara la sua esistenza, che va dimostrata.

Lemma 2.3. *Siano $a, b \in \mathbb{Z}$ elementi non nulli, e sia d il minimo elemento positivo della forma $ha \pm kb$, dove $h, k \in \mathbb{Z}$. Allora d divide sia a che b.*

Proposizione 2.4. *Siano a, b elementi non nulli di $\mathbb{Z}$. Allora un massimo comun divisore tra a e b esiste, ed è della forma $ha + kb$ per un'opportuna scelta di $h, k \in \mathbb{Z}$.*

Corollario 2.5. *Se $a, b, c \in \mathbb{Z}$ sono interi non nulli, e $c = ha + kb$ per qualche $h, k \in \mathbb{Z}$, allora il massimo comun divisore di a e b divide c. In particolare a e b sono primi tra loro se e solo se è possibile esprimere 1 nella forma $ha + kb$ per una scelta opportuna di $h, k \in \mathbb{Z}$.*

Due numeri si dicono primi tra loro se 1 è un loro massimo comun divisore.

Proposizione 2.6. *Siano $a, b \in \mathbb{Z}$ non entrambi nulli, $d = (a, b)$. Allora $d \neq 0$ e $a/d, b/d$ sono primi tra loro.*

Definizione 2.7. Un numero intero $p \neq 0$ si dice *primo* se non è invertibile in $\mathbb{Z}$, e vale una (e quindi entrambe) delle due proprietà equivalenti:

- in ogni fattorizzazione $p = ab$, almeno uno tra i fattori a, b è invertibile;
- ogni volta che p divide un prodotto ab, allora divide almeno uno dei fattori a, b.

Osservazione 2.8. E' utile ricordare come gli unici elementi invertibili in $\mathbb{Z}$ siano 1 e -1. Segue quindi immediatamente che gli unici divisori di un elemento primo $p \in \mathbb{Z}$ sono $\pm 1, \pm p$, e sono tutti distinti.
E' bene anche notare che se $p \in \mathbb{Z}$ è primo e $a \in \mathbb{Z}$, allora p non divide a se e solo se $(a, p) = 1$.

Proposizione 2.9. *Sia $n \in \mathbb{Z}$. Se $n \mid ab$ e $(a, n) = 1$, allora n divide b.*

Teorema 2.10. *Sia $n > 1$ un numero intero. Allora $\mathbb{Z}/(n)$ è un dominio d'integrità se e solo se n è primo.*

Dimostrazione. Se n non è primo, allora possiamo esprimere n come prodotto ab di numeri a e b entrambi positivi e diversi da 1. Allora $[a][b] = [n] = [0]$, ma $[a] \neq [0], [b] \neq [0]$, e quindi $\mathbb{Z}/(n)$ è un dominio d'integrità.

Viceversa, se n è primo, e $[a][b] = [0]$, allora n divide ab, e per il lemma precedente, n deve dividere almeno uno dei fattori, cioè $[a] = [0]$ oppure $[b] = [0]$. □

Il seguente fatto ci sarà utile fra qualche tempo.

Corollario 2.11. *Se $p \in \mathbb{Z}$ è primo, allora le uniche soluzioni di $x^2 \equiv 1 \mod p$ sono $x \equiv \pm 1 \mod p$.*

Dimostrazione. Risolvere l'equazione $[x]^2 = [1]$ in $\mathbb{Z}/(p)$ è equivalente a risolvere $[x - 1][x + 1] = [0]$. Poiché $\mathbb{Z}/(p)$ è un dominio d'integrità, si ottiene $[x - 1] = [0]$ oppure $[x + 1] = [0]$. □

3. Classi di resto invertibili

In questa sezione dimostriamo un enunciato più preciso di quello contenuto nel Teorema 2.10.

Lemma 3.1. *Siano $a, n \in \mathbb{N}$ interi maggiori di 1. Allora $[a]$ è invertibile in $\mathbb{Z}/(n)$ se e solo se $(a, n) = 1$.*

Dimostrazione. Se $(a, n) = 1$, per l'identità di Bezout è possibile trovare $h, k \in \mathbb{Z}$ tali che $ha + kn = 1$. Ma allora $[h][a] = [ha] = [1 - kn] = [1]$ in $\mathbb{Z}/(n)$, e quindi $[h]$ è l'inverso di $[a]$ in $\mathbb{Z}/(n)$.

Viceversa, se $[a]$ possiede un inverso $[h]$ in $\mathbb{Z}/(n)$, allora $[ah] = [1]$, cioè $ha \equiv 1 \mod n$. Ma allora $ha - 1 = kn$, cioè $1 = ha + kn$ per qualche $k \in \mathbb{Z}$, e $(a, n) = 1$ per il Corollario 2.5. □

Corollario 3.2. *Se $(a, n) = 1$ e $[h]$ è l'inverso di $[a]$ in $\mathbb{Z}/(n)$, allora $(h, n) = 1$.*

Dimostrazione. Anche $[h]$ è invertibile in $\mathbb{Z}/(n)$, poiché $[a]$ è il suo inverso. □

Teorema 3.3. *Se $p \in \mathbb{Z}$ è un numero primo, allora $Z/(p)$ è un campo.*

Dimostrazione. Se $[a]$ è una classe di resto diversa da $[0]$, allora p non divide a. In tal caso $(a, p) = 1$ e quindi $[a]$ possiede un inverso moltiplicativo. □

Il numero degli elementi invertibili in $\mathbb{Z}/(n)$ si indica con $\phi(n)$. Chiaramente $\phi(p) = p - 1$ se p è un numero primo.

Lemma 3.4. $(ab, n) = 1$ *se e solo se* $(a, n) = (b, n) = 1$.

Dimostrazione. Sia $n \neq 0$. Allora, per il Teorema fondamentale dell'aritmetica, $(c, n) = 1$ equivale a dire che i primi che compaiono nella fattorizzazione di n non compaiono nella fattorizzazione di c. Ma un primo compare nella fattorizzazione di ab se e soltanto se compare nella fattorizzazione di almeno uno tra a e b.
Il caso $n = 0$ è ovvio. □

Corollario 3.5. *Se $a, p \in \mathbb{Z}$ e p è primo, allora $(a, p) = 1$ se e solo se $(a, p^n) = 1$.*

Di conseguenza, se $p \in \mathbb{Z}$ è primo e $n > 0$, ogni $[a] \in \mathbb{Z}/(p^n)$ è invertibile, tranne quando $p \mid a$. Pertanto gli elementi non invertibili di $\mathbb{Z}/(p^n)$ sono p^{n-1} e quindi $\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$.

Osservazione 3.6. Siano $a, b, n \in \mathbb{Z}$. Condizione necessaria affinché la congruenza $ax \equiv b \mod n$ abbia soluzioni in $\mathbb{Z}$ è che il massimo comun divisore $d = (a, n)$ divida b. In effetti $ax \equiv b \mod n$ è equivalente a dire che n divide $ax - b$, cioè che $b = ax + kn$ per qualche $k \in \mathbb{Z}$. Dal momento che d divide sia a che n, divide anche i loro multipli, e quindi anche b.

Quando tale condizione necessaria è soddisfatta, possiamo scrivere $a = a'd, b = b'd, n = n'd$ per un'opportuna scelta di $a', b', n' \in \mathbb{Z}$. Allora la congruenza diventa $d(a'x - b') \equiv 0 \mod n'd$, che, per l'Osservazione 1.2, è equivalente a $a'x \equiv b' \mod n'$. In quest'ultima congruenza, si ha $(a', n') = 1$ per la Proposizione 2.6. In tale situazione, il Lemma 3.1 ci assicura che a' possiede un inverso modulo n. Moltiplicando entrambi i membri per a'^{-1} si ottengono tutte le soluzioni della congruenza iniziale.

Questo mostra che $(a, n) \mid b$ è una condizione necessaria e sufficiente affinché la congruenza $ax \equiv b \mod n$ abbia soluzione.

Teorema 3.7. *L'insieme $\mathbb{Z}/(n)^*$ degli elementi invertibili di $\mathbb{Z}/(n)$ è un gruppo (abeliano) rispetto all'operazione di moltiplicazione.*

Dimostrazione. L'insieme $\mathbb{Z}/(n)^*$ è non vuoto perché contiene $[1]$ e per il Lemma 3.1 contiene $[a], a \in \mathbb{Z}$ se e solo se $(a, n) = 1$. Il Lemma 3.4 ci assicura che se $[a], [b] \in \mathbb{Z}/(n)^*$, allora $[a][b] = [ab] \in \mathbb{Z}/(n)^*$: la moltiplicazione definisce quindi un'operazione su $\mathbb{Z}/(n)^*$, che è chiaramente associativa e commutativa, poiché gode di queste proprietà nell'anello $\mathbb{Z}/(n)$.
Inoltre possiede un elemento neutro $[1] \in \mathbb{Z}/(n)^*$, ed ogni elemento di $\mathbb{Z}/(n)^*$ possiede un inverso in $\mathbb{Z}/(n)$ – e quindi anche in $\mathbb{Z}/(n)^*$ – per definizione. □

4. Gruppi ed omomorfismi di gruppi (facoltativo)

Nel prossimo paragrafo introdurrò il concetto di omomorfismo di anelli. Dal momento che il concetto di omomorfismo di gruppi è più semplice. Di gruppi abbiamo già parlato in altri appunti, quindi non richiamo neanche la definizione.

Definizione 4.1. Siano G, H gruppi. Un'applicazione $f : G \to H$ si dice *omomorfismo di gruppi*, o più semplicemente *omomorfismo* se soddisfa $f(ab) = f(a)f(b)$ per ogni $a, b \in G$.

Proposizione 4.2. *Siano $1_G, 1_H$ le identità di G, H rispettivamente. Ogni omomorfismo $f : G \to H$ soddisfa*

- $f(1_G) = 1_H$;
- $f(g^{-1}) = f(g)^{-1}$.

Dimostrazione. Dalla proprietà di omomorfismo si ricava

$$f(g) = f(1_G \cdot g) = f(1_G)f(g),$$

da cui, moltiplicando a destra per l'inverso di $f(g) \in H$, si ottiene $1_H = f(g)f(g)^{-1} = f(1_G)f(g)f(g)^{-1} = f(1_G)$.
Allo stesso modo, si ha

$$f(g^{-1})f(g) = f(g^{-1}g) = f(1_G) = 1_H = f(1_G) = f(gg^{-1}) = f(g)f(g^{-1}),$$

quindi $f(g)$ e $f(g^{-1})$ sono uno l'inverso dell'altro. Per l'unicità dell'inverso in un gruppo, segue che $f(g^{-1}) = f(g)^{-1}$. Si noti che g^{-1} è l'inverso di g in G, mentre $f(g)^{-1}$ è l'inverso di $f(g)$ in H. □

Definizione 4.3. Sia G un gruppo. Un sottoinsieme $H \subset G$ si dice *sottogruppo* di G se è un gruppo rispetto alle stessa operazione di G.

Proposizione 4.4. *Se G è un gruppo, $H \subset G$ è un sottogruppo se e solo se*

- $1_G \in H$;
- $ab \in H$ *per ogni* $a, b \in H$;
- $a^{-1} \in H$ *per ogni* $a \in H$.

Dimostrazione. Intanto mostriamo che se H soddisfa le tre condizioni è allora un gruppo rispetto alla stessa operazione di G. Intanto, H è non vuoto, in quanto $1_G \in H$.
L'operazione di G, quando effettuata su elementi di H, fornisce un risultato in H per la seconda delle proprietà elencate, e quindi definisce un'operazione su H. Questa operazione è associativa in quanto lo è già su G. Inoltre 1_G è un elemento neutro di questa operazione in H poiché lo è già rispetto a tutti gli elementi di G.
L'ultima cosa da mostrare è che ogni elemento in H possiede un inverso in H rispetto al prodotto, ma questo è garantito dalla terza delle proprietà elencate.

Il viceversa è anche facile. Supponiamo che H sia un gruppo rispetto all'operazione indotta da G. Se $a, b \in H$, il prodotto ab deve appartenere ad H, poiché la restrizione di $\cdot$ deve essere un'operazione su H, e quindi fornire un

risultato in H.
Sia ora 1_H l'identità di H rispetto all'operazione indotta da quella di G. Allora $1_H h = h = 1_G h$ per ogni $h \in H$. Moltiplicando a destra per l'inverso di h in G, si ottiene

$$1_H = 1_H h h^{-1} = 1_G h h^{-1} = 1_G,$$

e quindi l'identità di H è 1_G, che in particolare appartiene ad H. Allo stesso modo, se x è l'inverso di h in H rispetto all'operazione indotta da G, allora $hx = 1_H = 1_G$. Moltiplicando a sinistra per l'inverso h^{-1} di h in G, si ottiene $x = h^{-1}hx = h^{-1}1_G = h^{-1}$. Pertanto l'inverso di $h \in H$ in H coincide con il suo inverso in G. Questo mostra che $h^{-1} \in H$ per ogni $h \in H$. □

Osservazione 4.5. La prima delle tre proprietà può essere sostituita da $H \neq \emptyset$. In effetti, se H contiene qualche elemento non vuoto a, deve possedere per la terza proprietà anche a^{-1} e per la seconda il prodotto $aa^{-1} = 1_G$.

Teorema 4.6. *Sia $f : G \to H$ un omomorfismo di gruppi. Allora il* nucleo $\ker f = \{g \in G \mid f(g) = 1_H\}$ *di f è un sottogruppo di G, e l'*immagine *Im $f = \{h \in H \mid h = f(g)$ per qualche $g \in G\}$ di f è un sottogruppo di H.*

Dimostrazione. Mostriamo innanzitutto che $\ker f$ è un sottogruppo di G. Abbiamo già visto che ogni omomorfismo soddisfa $f(1_G) = 1_H$, e quindi $1_G \in \ker f$. Inoltre, se $a, b \in \ker f$, allora $f(a) = f(b) = 1_H$ e quindi $f(ab) = f(a)f(b) = 1_H 1_H = 1_H$, cioè $ab \in \ker f$. Infine, se $a \in \ker f$, allora $f(a) = 1_H$ e di conseguenza $f(a^{-1}) = f(a)^{-1} = 1_H^{-1} = 1_H$: in altre parole $a^{-1} \in \ker f$.

Mostriamo ora che Im f è un sottogruppo di H. Intanto, $1_H = f(1_G)$, e quindi $1_H \in$ Im f. Inoltre, se $a, a' \in$ Im f, allora esistono $g, g' \in G$ tali che $a = f(g), a' = f(g')$. Ma allora $aa' = f(g)f(g') = f(gg')$ e quindi $aa' \in$ Im f. Infine, se $a = f(g)$, allora $a^{-1} = f(g)^{-1} = f(g^{-1})$, e quindi $a \in$ Im $f \Rightarrow a^{-1} \in$ Im f. □

Osservazione 4.7. Si può in realtà dimostrare che il nucleo di un omomorfismo $f : G \to H$ è un *sottogruppo normale* di G: se $x \in \ker f$ e $g \in G$ allora $gxg^{-1} \in \ker f$. In effetti, se $x \in \ker f$ e $g \in G$, allora

$$f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(g)1_H f(g)^{-1}) = 1_H.$$

Si può mostrare che un sottogruppo N di G è normale se e solo se è il nucleo di qualche omomorfismo $f : G \to H$.

Proposizione 4.8. *Un omomorfismo di gruppi $f : G \to H$ è iniettivo se e solo se* $\ker f = \{1_G\}$ *e suriettivo se e solo se Im $f = H$.*

Dimostrazione. La seconda affermazione segue dalla definizione di immagine di un'applicazione. Per quanto riguarda la prima, notiamo innanzitutto che se f è iniettiva, $\ker f$ contiene al più un elemento. Dal momento che $f(1_G) = 1_H$, si ha allora $\ker f = \{1_G\}$.

Viceversa, supponiamo che $\ker f = \{1_G\}$. Supponendo che $f(a) = f(b)$, si ottiene $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = f(a)f(a)^{-1} = 1_H$. Ma allora $ab^{-1} \in \ker f = \{1_G\}$, e quindi $ab^{-1} = 1_G$; moltiplicando entrambi i membri a destra per b si ottiene $a = b$, e quindi l'iniettività di f. □

5. Anelli ed omomorfismi di anelli

5.1. **Omomorfismi di anelli e prime proprietà.** Del Teorema cinese del resto abbiamo dato più dimostrazioni, anche se l'ultima era più evoluta, e più adatta ad un corso di algebra. Per presentarla abbiamo però bisogno di poche nozioni di teoria degli anelli, che raccolgo qui.

Definizione 5.1. Siano A, B anelli. Un'applicazione $f : A \to B$ è un *omomorfismo di anelli* se soddisfa

- $f(a + a') = f(a) + f(a')$;
- $f(aa') = f(a)f(a')$,

per ogni scelta di $a, a' \in A$. Se A, B sono anelli con unità, ed indichiamo con $1_A, 1_B$ le loro unità, un omomorfismo di anelli $f : A \to B$ è detto *omomorfismo di anelli con unità* se $f(1_A) = 1_B$.

Esempi 5.2.

(1) L'applicazione $f : A \to B$ tale che $f(a) = 0_B$ per ogni $a \in A$ è un omomorfismo di anelli. Se A e B sono anelli con unità, f è un omomorfismo di anelli, ma non un omomorfismo di anelli con unità.
(2) L'applicazione identità $\mathrm{id} : A \to A$ è un omomorfismo di anelli, ed è un omomorfismo di anelli con unità se A è un anello con unità.
(3) Se A è un anello con unità, definiamo un'applicazione $f : \mathbb{Z} \to A$ ricorsivamente come segue: $f(0) = 0_A, f(n + 1) = f(n) + 1_A$ se $n \geq 0$, $f(n) = -f(-n)$ se $n < 0$. Ad esempio $f(-2) = -(1_A + 1_A)$. Verificate che f è un omomorfismo di anelli con unità – è in realtà l'unico omomorfismo di anelli con unità da $\mathbb{Z}$ in A.

Proposizione 5.3. *Sia $f : A \to B$ un omomorfismo di anelli. Allora f soddisfa*

- $f(0_A) = 0_B$
- $f(-a) = -f(a)$
- $f(a - b) = f(a) - f(b)$.

Inoltre, se f è suriettivo, A è un anello con unità, e $B \neq (0)$, allora B è un anello con unità e $f(1_A) = 1_B$.

Dimostrazione. Per mostrare che $f(0_A) = 0_B$ basta osservare che

$$f(0_A) = f(0_A + 0_A) = f(0_A) + f(0_A).$$

Sommando $-f(0_A)$ ad entrambi i membri, si ottiene $0_B = f(0_A)$.
Allo stesso modo si ha

$$0_B = f(0_A) = f(a + (-a)) = f(a) + f(-a).$$

sommando ad entrambi i membri l'inverso additivo $-f(a)$ di $f(a)$ si ottiene $-f(a) = f(-a)$. Immediatamente si ha anche

$$f(a - b) = f(a + (-b)) = f(a) + f(-b) = f(a) + (-f(b)) = f(a) - f(b).$$

L'ultima affermazione è più delicata: abbiamo

$$f(a)f(1_A) = f(a1_A) = f(a) = f(1_A a) = f(1_A)f(a),$$

per ogni $a \in A$. Se f è suriettiva, ogni elemento di B è della forma $f(a)$, e quindi $f(1_A)b = b = bf(1_A)$ per ogni $b \in B$. Questo basta ad affermare che $f(1_A)$ è (l'unico) elemento neutro per la moltiplicazione in B, ma non che B sia un anello con unità!

In effetti un anello B si dice anello con unità se esiste un elemento neutro 1_B per la moltiplicazione, e questo elemento è **diverso da** 0_B. Tuttavia, se B possiede più di un elemento, e quindi qualche elemento $b \neq 0$, allora $b \cdot 0_B = 0_B \neq b$ mostra che 0_B non può essere l'elemento neutro della moltiplicazione. Quindi nel nostro caso B è un anello con unità, e $1_B = f(1_A)$. □

Teorema 5.4. *Se $n > 1$, l'applicazione $\pi : \mathbb{Z} \to \mathbb{Z}/(n)$ di proiezione al quoziente è un omomorfismo di anelli con unità.*

Dimostrazione. L'applicazione di proiezione al quoziente è quella che associa ad ogni elemento $a \in \mathbb{Z}$ la sua classe di equivalenza $[a] \in \mathbb{Z}/(n)$, quindi $\pi(a) = [a]$ per ogni $a \in \mathbb{Z}$.

Per verificare che π sia un omomorfismo di anelli dobbiamo mostrare che $\pi(a+b) = \pi(a)+\pi(b), \pi(ab) = \pi(a)\pi(b)$, cioè che $[a + b] = [a] + [b], [ab] = [a][b]$. Ma questo segue dalla definizione della struttura di anello su $\mathbb{Z}/(n)$. Inoltre, π è un omomorfismo di anelli con unità poiché è suriettivo. □

Concludo questo paragrafo con la costruzione della somma diretta di anelli.

Proposizione 5.5. *Siano A, B anelli. Le operazioni $(a, b) + (a', b') = (a + a', b + b')$, $(a, b) \cdot (a', b') = (aa', bb')$ definiscono sul prodotto cartesiano $A \times B$ una struttura di anello, detto* somma diretta *di A e B, che si indica con $A \oplus B$.*

Dimostrazione. Tutte le proprietà di associatività, commutatività e distributività delle operazioni si dimostrano facilmente a partire dalle analoghe proprietà per le operazioni di A e B. L'elemento neutro rispetto alla somma è $0_{A\oplus B} = (0_A, 0_B)$ e l'inverso additivo di (a, b) è $(-a, -b)$. □

Osservazione 5.6. Se A e B sono entrambi commutativi, allora anche $A \oplus B$ è commutativo. Analogamente, se A, B sono anelli con unità, allora $A \oplus B$ è un anello con unità, la cui unità è $1_{A\oplus B} = (1_A, 1_B)$. Tuttavia, se A, B sono domini d'integrità, $A \oplus B$ non lo è mai, come si osserva notando che $(1_A, 0_B) \cdot (0_A, 1_B) = (0_A, 0_B)$.

5.2. **Sottoanelli. Iniettività e suriettività di omomorfismi.**

Definizione 5.7. Sia A un anello. Un sottoinsieme $B \subset A$ si dice *sottoanello* di A se è un anello rispetto alle stesse operazioni di A.

Proposizione 5.8. *Se A è un anello, $B \subset A$ è un sottoanello se e solo se*

- $0_A \in B$;
- $b + b', bb' \in B$ *per ogni scelta di* $b, b' \in B$;
- $-b \in B$ *per ogni* $b \in B$.

Dimostrazione. Intanto mostriamo che se B soddisfa le tre condizioni è allora un anello rispetto alla stessa operazione di A. Intanto, B è non vuoto, in quanto $0_A \in B$.
Le operazioni di A, quando effettuate su elementi di B, forniscono risultati in B per la seconda delle proprietà elencate, e quindi definiscono operazioni su B. Queste operazioni soddisfanno le condizioni di associatività, commutatività e distributività richieste alle operazioni di un anello in quanto lo fanno già su A. Inoltre 0_A è un elemento neutro della somma in B poiché lo è già rispetto a tutti gli elementi di A.
L'ultima cosa da mostrare è che ogni elemento di B possiede un inverso additivo in B, ma questo è garantito dall'ultima delle proprietà elencate.

Il viceversa è anche facile. Supponiamo che B sia un anello rispetto all'operazione indotta da A. Se $b, b' \in B$, la somma $b + b'$ ed il prodotto bb' devono appartenere a B, poiché le restrizioni di $+$ e $\cdot$ devono essere operazioni su B, e quindi forniscono risultati in B.

Sia ora 0_B l'identità di B rispetto all'operazione di somma indotta da A. Allora $0_B + b = b = 0_A + b$ per ogni $b \in B$. Sommando l'inverso additivo di b in A ad entrambi i membri, si ottiene

$$0_B = 0_B + b - b = b - b = 0_A,$$

e quindi lo zero di B coincide con quello di A, che in particolare appartiene a B. Allo stesso modo, se x è l'inverso additivo di b in B rispetto all'operazione indotta da A, allora $b + x = 0_B = 0_A$. Sommando ad entrambi i membri l'inverso $-b$ di b in A, si ottiene $x = -b + b + x = -b + 0_A = -b$. Pertanto l'inverso additivo di $b \in B$ in B coincide con il suo inverso additivo in A. Questo mostra che $-b \in B$ per ogni $b \in B$. □

Osservazione 5.9. Come nell'Osservazione 4.5, la prima delle condizioni può essere sostituita da $B \neq \emptyset$.

Proposizione 5.10. *Se $f : A \to B$ è un omomorfismo di anelli, allora il suo nucleo $\ker f = \{a \in A \mid f(a) = 0_B\}$ è un sottoanello di A e la sua immagine Im $f = \{b \in B \mid b = f(a)$ per qualche $a \in A\}$ è un sottoanello di B.*

Dimostrazione. Le dimostrazioni sono più o meno immediate. $\ker f \subset A$ è un sottoanello poiché contiene 0_A dal momento che $f(0_A) = 0_B$ e somma e prodotto di elementi che stanno in $\ker f$ appartengono ancora a $\ker f$. Inoltre $f(a) = 0_B \Rightarrow f(-a) = -f(a) = 0_B$.

Per quanto riguarda l'immagine, $0_B \in$ Im f poiché $0_B = f(0_A)$, ed Im f è chiuso rispetto a somma e prodotto poiché f è un omomorfismo. Inoltre $-f(a) = f(-a)$ e quindi se $b = f(a) \in$ Im f, allora $-b \in$ Im f. □

Osservazione 5.11. Vedremo più tardi che il nucleo di un omomorfismo tra anelli non è solo un sottoanello, ma anche un ideale dell'anello di partenza.

Proposizione 5.12. *Un omomorfismo di anelli $f : A \to B$ è iniettivo se e solo se $\ker f = \{0_A\}$ ed è suriettivo se e solo se Im $f = B$.*

Dimostrazione. La seconda parte dell'enunciato segue dalla definizione di immagine di un'applicazione. Per quanto riguarda la prima, la dimostrazione è analoga a quella che avete visto anche in algebra lineare con le applicazioni lineari.

Se f è iniettiva, allora $\ker f = f^{-1}(0_B)$ contiene al più un elemento. Dal momento che $f(0_A) = 0_B$, allora $\ker f = \{0_A\}$. Viceversa, se $\ker f = \{0_A\}$, allora da $f(a) = f(a')$ segue $f(a - a') = f(a) - f(a') = 0_B$ e quindi $a - a' \in \ker f$. Ma allora $a - a' = 0_A \Rightarrow a = a'$, da cui l'iniettività di f. □

5.3. **Ideali.** Gli anelli $\mathbb{Z}/(n)$ sono esempi di anelli quoziente. Per definire questa nozione è necessario introdurre il concetto di ideale.

Definizione 5.13. Un sottoanello $I \subset A$ è un *ideale* di A se $ai, ia \in I$ per ogni scelta di $a \in A, i \in I$.

In altre parole, un ideale di A è un sottoinsieme non vuoto di A, chiuso rispetto alla somma e all'inverso additivo, che assorbe il prodotto per elementi di A.

Esempi 5.14.

(1) $\{0\}$ e A sono sempre ideali di A.
(2) Se A è un anello commutativo, il sottoinsieme $(a) = \{ax \mid x \in A\}$ è un ideale di A. In particolare, $\{0\} = (0)$, e $A = (1)$ se A possiede un'unità 1. Ad esempio, $(d) \subset \mathbb{Z}$ è l'ideale i cui elementi sono tutti e soli i multipli di $d \in \mathbb{Z}$.
(3) Se A è un anello con unità, e I è un ideale di A che contiene 1, allora $I = A$. In effetti, se $1 \in I$, allora $a \cdot 1 \in I$ per ogni $a \in A$.
(4) Gli unici ideali di un campo $\mathbb{K}$ sono quelli banali. In effetti se $I \subset \mathbb{K} \neq (0)$, allora possiede almeno un elemento non nullo $0 \neq x \in I$. Ma allora da $x^{-1} \in \mathbb{K}, x \in I$ segue $1 = x^{-1} \cdot x \in I$ e quindi $I = \mathbb{K}$.
(5) Se A è un anello commutativo con unità nel quale gli unici ideali sono banali, allora A è un campo. In effetti, sia $0 \neq x \in A$. Allora $(0) \neq (x)$ è un ideale di A, e quindi $(x) = A$. Ma allora $1 \in (x)$, e quindi $1 = xy$ per qualche $y \in A$. In altre parole, x possiede un inverso moltiplicativo.
(6) Se $f : A \to B$ è un omomorfismo di anelli, allora $\ker f$ è un ideale A. In effetti, sappiamo già che $\ker f$ è un sottoanello di A, e l'unica cosa da controllare è che da $x \in \ker f$ segua $ax, xa \in \ker f$ per ogni scelta di $a \in A$. Questo è evidente: $f(ax) = f(a)f(x) = f(a)0 = 0 = 0f(a) = f(x)f(a) = f(xa)$.

Teorema 5.15. *Gli unici ideali di $\mathbb{Z}$ sono quelli della forma $(d), d \in \mathbb{Z}$.*

Dimostrazione. Abbiamo già visto che $\{0\} = (0)$. Sia $\{0\} \neq I \subset \mathbb{Z}$ un ideale. Sappiamo che I contiene almeno un elemento $x \neq 0$: a meno di cambiarlo con $-x \in I$ possiamo supporre che sia positivo.

Sia d il minimo elemento positivo di I – esiste per il buon ordinamento di $\mathbb{N}$, poiché $I \cap \mathbb{N} \neq \emptyset$ – e $a \in I$. Se effettuiamo la divisione euclidea $a = qd + r, 0 \leq r < d$, osserviamo che $r = a - qd = a + (-q)d$ appartiene ancora ad I. Poiché d è il minimo elemento positivo, r deve essere uguale a 0, e quindi $a = qd$. Questo mostra che ogni elemento di I è multiplo di d, e quindi che $I \subset (d)$. L'inclusione opposta $(d) \subset I$ segue da $d \in I$. □

La proprietà appena dimostrata si esprime affermando che $\mathbb{Z}$ è un anello ad ideali principali.

Osservazione 5.16. La notazione (d) indica solitamente l'ideale di A *generato* dall'elemento $d \in A$. Questo è l'intersezione di tutti gli ideali di A che contengono d, e può essere diverso dall'insieme dei multipli di d.

Tuttavia, se A è un anello commutativo con unità, l'ideale generato da $d \in A$ coincide con l'insieme dei suoi multipli. Dal momento che ci occuperemo principalmente di questo tipo di anelli, ignoreremo il problema notazionale.

5.4. **Congruenza modulo un ideale e quoziente di un anello per un ideale.** Sia A un anello, I un suo ideale. Dati due elementi $a, b \in A$, diremo che a è congruo a b modulo I, e scriveremo $a \equiv b \mod I$, se $b - a \in I$.

Proposizione 5.17. *Sia A un anello ed I un suo ideale. La congruenza modulo I è una relazione di equivalenza su A.*

Dimostrazione. La dimostrazione è totalmente analoga a quella per le classi di resto modulo n in $\mathbb{Z}$. Riflessività: $a \equiv a \mod I$ poiché $a - a = 0 \in I$. Simmetria: se $b - a \in I$, allora $a - b = -(b - a) \in I$. Transitività: se $b - a, c - b \in I$, allora $c - a = (c - b) + (b - a) \in I$. □

Indicando con $[x]$ la classe di congruenza di $x \in A$ modulo l'ideale I, si ha $[x] = [y]$ se e solo se $y - x \in I$, cioè esattamente quando $y = x + i$, con $i \in I$. Per questo motivo, la classe $[x]$ è indicata anche con $x + I$.

Proposizione 5.18. *Sia A un anello e I un suo ideale. Allora, le operazioni $[a] + [b] = [a + b], [a] \cdot [b] = [ab]$ sono ben definite sulle classi di congruenza modulo I.*

Dimostrazione. Dobbiamo far vedere che se $a \equiv a' \mod I$ e $b \equiv b' \mod I$, allora $a + b \equiv a' + b' \mod I$, $ab \equiv a'b' \mod I$.

Le ipotesi si traducono nel fatto che $a' = a + i, b' = b + j$, con $i, j \in I$. Ma allora $a' + b' = a + b + (i + j)$, e $i + j$ appartiene ad I in quanto somma di elementi di I. Allora stesso modo, $a'b' = (a + i)(b + j) = ab + (aj + ib + ij)$, e $aj + ib + ij$ appartiene ad I in quanto somma dei tre elementi aj, ib, ij appartenenti ad I. □

Teorema 5.19. *Sia A un anello, $I \subset A$ un suo ideale, e indichiamo con $\sim$ la relazione in A di congruenza modulo I. Allora esiste un'unica struttura di anello sull'insieme quoziente $A/\sim$ che renda la proiezione al quoziente $\pi : A \to A/\sim$ un omomorfismo di anelli. Tale struttura è detta* quoziente dell'anello A per l'ideale I *e si indica con A/I.*

Dimostrazione. Se indichiamo con $[a]$ la classe di $\sim$-equivalenza di $a \in A$, la proiezione $\pi : A \to A/\sim$ è un omomorfismo di anelli se e soltanto se $[a] + [b] = [a + b], [a][b] = [ab]$. L'unica cosa da verificare è quindi che queste operazioni definiscano su $A/\sim$ una struttura di anello.

Abbiamo già verificato che tali operazioni sono ben definite sulle classi di equivalenza; l'unica cosa ancora da verificare è che soddisfino le proprietà commutative, associative e distributive contenute negli assiomi di anello. E' facile, e lo lascio come esercizio, controllare che tutte le proprietà seguono dalle analoghe proprietà delle operazioni di A. L'elemento neutro rispetto alla somma è $[0]$ e l'inverso additivo di $[a]$ è $[-a]$. □

Osservazione 5.20. Si mostra anche facilmente che se A è commutativo anche A/I è commutativo, e che se A è un anello con unità 1, allora $[1]$ è l'elemento neutro della moltiplicazione in A/I.

Corollario 5.21. *Sia A un anello. Un sottoinsieme $I \subset A$ è un ideale se e solo se esiste un anello B e un omomorfismo di anelli $f : A \to B$ tale che $I = \ker f$.*

Dimostrazione. Abbiamo già visto che i nuclei di omomorfismi sono ideali. Rimane da mostrare che ogni ideale è nucleo di qualche omomorfismo. Questo è semplice: se I è un ideale di A, allora il nucleo della proiezione al quoziente $\pi : A \to A/I$ è esattamente I, in quanto $[a] = [0]$ se e solo se $a = a - 0 \in I$. □

Esempi 5.22.

(1) Gli unici ideali di $\mathbb{Z}$ sono della forma $(d), d \in \mathbb{Z}$. Il quoziente di $\mathbb{Z}$ per il suo ideale (d) è esattamente l'anello $\mathbb{Z}/(d)$ delle classi di resto modulo d, il che giustifica la notazione precedentemente introdotta.
(2) Il quoziente A/A è un anello con un solo elemento, e tutte le operazioni banali.
(3) Il quoziente $A/(0)$ è un anello isomorfo ad A, tramite l'isomorfismo $\pi : A \to A/(0)$ definito da $\pi(a) = [a] = \{a\}$.

5.5. **La corrispondenza tra gli ideali di un anello e gli ideali di un suo quoziente.** Quozientare un anello A per un suo ideale I equivale a *buttare a zero* tutti gli elementi che appartengono all'ideale. Come conseguenza, i sottoanelli e gli ideali di A/I dovrebbero rappresentare una buona testimonianza dei sottoanelli e degli ideali di A che contengono I.

Dei fatti che seguono, abbiamo fatto a lezione soltanto la parte che riguarda gli ideali – e la dimostrazione è stata anche abbastanza fumosa...

Lemma 5.23. *Sia A un anello, I un suo ideale, $\pi : A \to A/I$ la proiezione canonica. Allora, se S è un sottoanello di A, $\pi(S)$ è un sottoanello di A/I, e se J è un ideale di A, $\pi(J)$ è un ideale di A/I. Inoltre, se $\overline{S}$ è un sottoanello di A/I, allora $\pi^{-1}(\overline{S})$ è un sottoanello di A che contiene I, e se $\overline{J}$ è un ideale di A/I, allora $\pi^{-1}(\overline{J})$ è un ideale di A che contiene I.*

Dimostrazione. Se S è un sottoanello di A, allora la restrizione $\pi|_S$ di $\pi : A \to A/I$ ad S è ancora un omomorfismo di anelli e la sua immagine è esattamente $\pi(S)$, che è quindi un sottoanello di A/I.

Viceversa, se $\overline{S}$ è un sottoanello di A/I, sia $S = \pi^{-1}(\overline{S})$: allora $a \in S$ se e solo se $\pi(a) \in \overline{S}$. In particolare, se $a, b \in S$, allora $\pi(a), \pi(b) \in \overline{S}$ e $\pi(a + b) = \pi(a) + \pi(b), \pi(ab) = \pi(a)\pi(b)$ appartengono entrambi ad $\overline{S}$. Inoltre $-\pi(a) = \pi(-a)$ e quindi $-a \in S$ se $a \in S$. Infine, $I \subset S$ poiché $0 \in \overline{S}$ e $S \supset \pi^{-1}(0) = I$, il che mostra anche che S è non vuoto. In conclusione S è un sottoanello di A che contiene S.

Per quanto riguarda gli ideali, se $\overline{J}$ è un ideale di A/I, consideriamo la proiezione al quoziente $\overline{\pi} : A/I \to (A/I)/\overline{J}$, il cui nucleo è esattamente $\overline{J}$. Allora $\pi^{-1}(\overline{J}) = \ker \overline{\pi} \circ \pi$ ed è quindi un ideale di A che contiene I.

Viceversa, se J è un ideale di A, è in particolare un suo sottoanello, e quindi $\pi(J)$ è un sottoanello di A/I. Per verificare che è anche un ideale, basta controllare che $[a][j], [j][a] \in \pi(J)$ per ogni scelta di $[a] \in A/I$, $[j] \in \pi(J)$. Ma questo è ovvio, in quanto $[a][j] = [aj], [j][a] = [ja]$, e $aj, ja \in J$ se $j \in J$. □

Teorema 5.24. *$S \mapsto \pi(S)$ è una corrispondenza biunivoca tra sottoanelli di A che contengono I e sottoanelli di A/I. In tale corrispondenza, S è un ideale di A se e solo se $\pi(S)$ è un ideale di A/I.*

Dimostrazione. Per mostrare la prima parte dell'enunciato, è sufficiente costruire un'inversa all'applicazione $S \mapsto \pi(S)$. In effetti, $\overline{S} \mapsto \pi^{-1}(\overline{S})$ è l'inversa desiderata.

Per verificarlo, notiamo innanzitutto che per il lemma precedente $S \mapsto \pi(S)$ associa a sottoanelli di A (che contengono I) sottoanelli di A/I, e che $\overline{S} \mapsto \pi^{-1}(\overline{S})$ associa a sottoanelli di A/I sottoanelli di A che contengono I. Dobbiamo quindi mostrare le due composizioni di tali applicazioni sono uguali all'identità.

Intanto, se $f : X \to Y$ è un'applicazione suriettiva, si vede facilmente che $f(f^{-1}(Z)) = Z$ per ogni sottoinsieme $Z \subset Y$, quindi $\pi(\pi^{-1}(\overline{S})) = \overline{S}$ è chiaramente vera, poiché la proiezione π è suriettiva. Rimane da far vedere che $\pi^{-1}(\pi(S)) = S$ se S è un sottoanello di A che contiene I.

Di nuovo, se $f : X \to Y$ è un'applicazione qualsiasi, allora $Z \subset f^{-1}(f(Z))$ è vera per ogni $Z \subset X$, quindi $S \subset \pi^{-1}(\pi(S))$. Per mostrare l'inclusione opposta, basta osservare che se $a \in \pi^{-1}(\pi(S))$ se e solo se $\pi(a) \in \pi(S)$, cioè $\pi(a) = \pi(s)$ per qualche $s \in S$. Ma allora $[a] = [s]$ e quindi $a = s + i$ con $i \in I$. Dal momento che $I \subset S$, si ha che $a \in S$, da cui $\pi^{-1}(\pi(S)) \subset S$. L'ultima affermazione è stata già dimostrata nel lemma precedente. □

Osservazione 5.25. Per restrizione, $J \mapsto \pi(J)$ costituisce una corrispondenza biunivoca tra ideali di A che contengono I ed ideali di A/I.

Diamo una facile applicazione della corrispondenza appena dimostrata.

Proposizione 5.26. *Sia A un anello commutativo con unità, I un suo ideale. Allora A/I è un campo se e solo se I è un ideale massimale di A cioè $I \subset J \Rightarrow J = I$ oppure $J = A$.*

Dimostrazione. Innanzitutto, se A è un anello commutativo con unità e $I \neq A$ è un suo ideale, anche A/I è un anello commutativo con unità.

Abbiamo già visto che un anello commutativo con unità è un campo se e solo se i suoi unici ideali sono banali, quindi A/I è un campo se e solo se i suoi unici ideali sono (0) e A/I. La corrispondenza biunivoca tra ideali di A/I e ideali di A che contengono I ci assicura che questo succede se e solo se gli unici ideali di A che contengono I sono $\pi^{-1}(0) = I$ e $\pi^{-1}(A/I) = A$. □

5.6. **Il teorema di omomorfismo per anelli.** Il teorema di omomorfismo per anelli e la traduzione del teorema di fattorizzazione per applicazioni al contesto della teoria degli anelli.

Teorema 5.27. *Siano A, B anelli, $I \subset A$ un ideale, $\pi : A \to A/I$ la proiezione canonica, $f : A \to B$ un omomorfismo di anelli tale che $I \subset \ker f$. Allora esiste un unico omomorfismo $F : A/I \to B$ tale che $f = F \circ \pi$.*

F è suriettiva se e solo se f è suriettiva, poiché Im f = Im F. Inoltre F è iniettiva se e solo se $\ker f = I$, poiché $\ker F = \pi(\ker f)$.

Dimostrazione. Se $a \equiv a' \mod I$, allora $a' - a \in I \subset \ker f$ e quindi $f(a) - f(a') = f(a - a') = 0 \Rightarrow f(a) = f(a')$. Per il teorema di omomorfismo per applicazioni, questo mostra l'esistenza di un'unica applicazione $F : A/I \to B$ tale che $f = F \circ \pi$. Rimane da mostrare che F è un omomorfismo di anelli.

Ma questo è evidente: sappiamo che $F([a]) = f(a)$ per ogni $a \in A$. Per verificare che F è un omomorfismo di anelli, basta controllare che $F([a] + [b]) = F([a]) + F([b])$ e che $F([a] \cdot [b]) = F([a])F([b])$. Ma questo è equivalente a far vedere che $f(a + b) = f(a) + f(b)$, $f(ab) = f(a)f(b)$, che segue dal fatto che f è un omomorfismo di anelli.

Im F = Im f segue da $F([a]) = f(a)$. Per quanto riguarda l'iniettività di F, $\ker F = \{[a] \in A/I \mid f(a) = 0\}$ e quindi $\ker F = \pi(\ker f)$. Ma allora $\ker F = (0)$ se e solo se $\ker f \subset I$. Poiché sappiamo già che $I \subset \ker f$, questo accade esattamente quando $\ker f = I$. □

Corollario 5.28 (Primo teorema di isomorfismo)**.** *Sia $f : A \to B$ un omomorfismo di anelli. Allora l'applicazione $A/I \ni [a] \mapsto f(a)$ è un isomorfismo tra $A/ker f$ e l'immagine di f.*

Dimostrazione. Basta applicare il teorema di omomorfismo all'omomorfismo suriettivo $f : A \to$ Im f ottenuto restringendo B all'immagine di f, utilizzando l'ideale $I = \ker f$. □

Il corollario che segue mostra che le uniche relazioni di equivalenza che sono compatibili con la struttura di anello sono le congruenze modulo un ideale.

Corollario 5.29. *Sia A un anello, e $\sim$ una relazione di equivalenza su A tale che le operazioni $[a] + [b] = [a + b]$, $[a][b] = [ab]$ siano ben definite, e forniscano una struttura di anello sull'insieme quoziente $A/\sim$. Allora $\sim$ è la congruenza modulo un ideale di I.*

Dimostrazione. Sia B la struttura di anello definita su $A/\sim$, ed indichiamo con $f : A \to B, f(a) = [a]_\sim$ la proiezione canonica al quoziente. Per le ipotesi fatte, f è un omomorfismo suriettivo di anelli.

Se $I = \ker f$, allora il corollario precedente mostra che l'applicazione $A/I \ni [a]_I \mapsto [a]_\sim \in B$ è un ben definito isomorfismo di anelli. In altre parole, $[a]_I = [b]_I$ se e solo se $[a]_\sim = [b]_\sim$ e quindi le classi di equivalenza di A/I coincidono con quelle di B. In conclusione, $\sim$ coincide con la congruenza modulo I. □

Il Teorema 5.27 fornisce una corrispondenza biunivoca tra l'insieme di tutti gli omomorfismi di anelli $f : A \to B$ tali che $I \ker f$ e l'insieme di tutti gli omomorfismi $F : A/I \to B$. In effetti, una volta che sia data f il teorema produce un'unica F tale che $f = F \circ \pi$; viceversa, se abbiamo un omomorfismo $F : A/I \to B$, la composizione $f = F \circ \pi$ è un omomorfismo di anelli che contiene I nel suo nucleo. A seconda delle circostanze può essere più comodo costruire un omomorfismo $A/I \to B$ o un omomorfismo $A \to B$ che abbia I nel suo nucleo.

Nella dimostrazione del Teorema cinese del resto, utilizzeremo il seguente fatto

Proposizione 5.30. *Siano $m, n \in \mathbb{Z}$ tali che $n|m$. Allora l'applicazione $\mathbb{Z}/(m) \ni [a] \to [a] \in \mathbb{Z}/(n)$ è ben definita, ed è un omomorfismo di anelli.*

Dimostrazione. Sia $A = \mathbb{Z}$, $B = \mathbb{Z}/(n)$, $I = (m)$, $f : A \to B$ la proiezione al quoziente. Allora $I \subset \ker f$ poiché se $a \in I = (m)$, allora $a = hm$ e quindi $[hm] = [0]$ in B in quanto m è un multiplo di n.

Possiamo allora applicare il Teorema 5.27 per ottenere un omomorfismo di anelli $F : \mathbb{Z}/(m) \to \mathbb{Z}/(n)$ che manda la classe di $a \in \mathbb{Z}$ modulo m nella classi di a modulo n. □

Quella appena vista è una conseguenza del

Teorema 5.31 (Secondo teorema di isomorfismo)**.** *Sia A un anello ed $I \subset J \subset A$ ideali. Se $\pi : A \to A/I$ è la proiezione canonica, indichiamo con J/I l'ideale $\pi(J)$ di A/I. Allora A/J è isomorfo al quoziente $(A/I)/(J/I)$.*

Dimostrazione. Sia $f : A \to A/J$ la proiezione al quoziente. Allora $\ker f = J$ e quindi $I \subset \ker f$. Applicando il Teorema 5.27, si ottiene un omomorfismo suriettivo $F : A/I \to A/J$ il cui nucleo è dato da $\pi(\ker f) = \pi(J) = J/I$. Ma allora, per il primo teorema di isomorfismo, A/J è isomorfo al quoziente $(A/I)/(J/I)$. □

Per completezza, enunciamo anche il

Teorema 5.32 (Terzo teorema di isomorfismo)**.** *Sia A un anello, $B \subset A$ un sottoanello, $I \subset A$ un ideale. Allora $B + I$ è un sottoanello di A, $B \cap I$ è un ideale di B e i quozienti $(B + I)/I$, $B/(B \cap I)$ sono isomorfi.*

Dimostrazione. Sia $\pi : A \to A/I$ la proiezione al quoziente. Si vede facilmente che $B + I = \pi^{-1}(\pi(B))$ ed è quindi una sottoalgebra di A. Essendo I un ideale di A, lo è a maggior ragione anche di $B + I$.

La composizione dell'inclusione $B \to B+I$ e della proiezione al quoziente $B+I \to (B+I)/I$ è un omomorfismo di anelli, che è suriettivo, poiché ogni elemento di $(B + I)/I$ è della forma $[b + i] = [b]$ per qualche $b \in B$.

Il nucleo di $B \to (B+I)/I$ è dato dagli elementi di B che giacciono in I e coincide quindi con $B \cap I$, che è pertanto un ideale di B. Per il primo teorema di omomorfismo, B/I è allora isomorfo a $(B + I)/I$. □

6. Il teorema cinese del resto

Siamo finalmente in grado di dare la dimostrazione evoluta del

Teorema 6.1 (cinese del resto)**.** *Se $m, n \in \mathbb{Z}$ soddisfano $(m, n) = 1$, il sistema di congruenze*

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n \end{cases}$$

ammette soluzione per ogni scelta di $a, b \in \mathbb{Z}$, che è unica modulo mn.

Dimostrazione. L'applicazione $\mathbb{Z} \to \mathbb{Z}/(m) \oplus \mathbb{Z}/(n)$ definita da $x \mapsto ([x]_m, [x]_n)$ è un omomorfismo di anelli, il cui nucleo è dato da $(m) \cap (n)$. Dal momento che $(m, n) = 1$, tale intersezione è uguale a (mn).

Per il Teorema 5.27, abbiamo un omomorfismo iniettivo $\mathbb{Z}/(mn) \ni [x]_{mn} \mapsto ([x]_m, [x]_n) \in \mathbb{Z}/(m) \oplus \mathbb{Z}/(n)$; poiché entrambi gli anelli possiedono mn elementi, tale omomorfismo è anche suriettivo, e quindi ogni elemento $([a]_m, [b]_n) \in \mathbb{Z}/(m) \oplus \mathbb{Z}/(n)$ appartiene all'immagine, e possiede un'unica controimmagine in $\mathbb{Z}/(mn)$. □

Questo teorema è vero in maggiore generalità

Teorema 6.2. *Sia A un anello, $I, J \subset A$ ideali tali che $I + J = A$. Allora l'applicazione $A/(I \cap J) \to A/I \oplus A/J$ definita da $[a]_{I\cap J} \mapsto ([a]_I, [a]_J)$ è un isomorfismo di anelli.*

Dimostrazione. Si verifica facilmente che l'applicazione $f : A \to A/I \oplus A/J$ definita da $f(x) = ([x]_I, [x]_J)$ è un omomorfismo di anelli, il cui nucleo è $I \cap J$. L'enunciato si dimostra dal Teorema 5.28 non appena abbiamo controllato che f sia suriettiva.

Per mostrare come $([a]_I, [b]_J)$ appartenga all'immagine di f per ogni scelta di $a, b \in A$, scriviamo $a = i + j, b = i' + j'$ con $i, i' \in I$ e $j, j' \in J$. Allora $[a]_I = [j]_I$ e $[b]_J = [i']_J$, mentre $[j]_J = [0]_J$ e $[i']_I = [0]_I$. Quindi $f(j + i') = f(j) + f(i') = ([a]_I, [0]_J) + ([0]_I, [b]_J) = ([a]_I, [b]_J)$. □

7. Il piccolo teorema di Fermat ed il teorema di Eulero

Dipartimento di Matematica, Università degli studi di Roma – "La Sapienza"
E-mail address: dandrea@mat.uniroma1.it