Dim. Sia $n = \deg(a)$ e $m = \deg(b)$. Se $n < m$ basta porre $q = 0$ e $r = a$. Sia quindi $n \geq m$. Siano $a_n = \mathrm{LC}(a)$ e $b_m = \mathrm{LC}(b)$ i coefficienti direttivi di a e b. Sia $\widetilde{a} := a - a_n b_m^{-1} x^{n-m} b$, allora $\deg(\widetilde{a}) < n$. Per induzione su n esistono $\widetilde{q}$ e $\widetilde{r}$ tali che $\widetilde{a} = b\widetilde{q} + \widetilde{r}$ e $\deg(\widetilde{r}) < m$. Basta porre $q = a_n b_m^{-1} x^{n-m} + \widetilde{q}$ e $r = \widetilde{r}$.

Proviamo ora l'unicità. Supponiamo che $a = bq + r = bq_1 + r_1$ con r e r_1 di grado inferiore a m. Segue quindi che $b(q - q_1) = r_1 - r$. Se per assurdo $q \neq q_1$ allora $b(q - q_1)$ avrebbe grado almeno m. Allora $\deg(r_1 - r) \geq \deg(b)$ il che è assurdo in quanto sia r che r_1 hanno grado minore di m. Allora deve essere necessariamente $q = q_1$ e $r = r_1$. □

L'unicità di quoziente e resto caratterizza univocamente gli anelli di polinomi a coefficienti su un campo (si veda [Jod67]).

Osservazione 3.11 *Nella dimostrazione precedente l'ipotesi che K sia un campo entra in gioco solo quando si afferma l'esistenza dell'inverso del coefficiente direttivo del polinomio divisore.*

Esercizio 3.12 *Imitare l'algoritmo di divisione lunga per spiegare la tecnica che avete appreso da piccoli per dividere due interi.*

Osservazione 3.13 *La procedura usata nella dimostrazione precedente fornisce il cosiddetto algoritmo di divisione lunga tra polinomi.*

Esempio 3.14 *Si vuole calcolare in $\mathbb{Q}[x]$ quoziente e resto tra i polinomi*

$$a(x) = 2x^3 + x^2 - 3x + 5 \qquad b(x) = 3x^2 - 2$$

Procedendo come descritto sopra si ottiene:

$+2x^3$	$+x^2$	$-3x$	$+5$	$3x^2 - 2$
$-2x^3$		$+(4/3)x$		$(2/3)x + 1/3$
	x^2	$-(5/3)x$	$+5$	
	x^2		$+2/3$	
		$-(5/3)x$	$+17/3$	

Quindi si ha $q(x) = (2/3)x + 1/3$ e $r(x) = (-5/3)x + 17/3$.

Esercizio 3.15 *Implementare un codice in* Magma *per il calcolo della divisione lunga tra polinomi.*

3.3 Congruenze tout court

Tra le varie relazioni di equivalenza che si possono definire su una struttura algebrica quelle che rivestono maggior interesse sono quelle compatibili con le operazioni, nel senso che verrà precisato fra breve. Tali relazioni vengono anche dette congruenze.

Definizione 3.16 *Sia X un insieme su cui è definita un'operazione binaria $*$ e una relazione d'equivalenza R. Si dice che R è compatibile con l'operazione $*$, o che R è una* ***congruenza*** *rispetto all'operazione $*$, se $\forall a, a', b, b' \in X$*

$$aRa',\ bRb' \implies (a * b)R(a' * b')$$

Lemma 3.17 *Mostriamo che R è una congruenza rispetto $a *$ sse $\forall a, b, c \in X$ aRb implica $(a * c)R(b * c)$ e $(c * a)R(c * b)$.*

Dim. Sia R una congruenza e aRb. Siccome cRc, si ha sia $a * cRb * c$ che $c * aRc * b$. Viceversa siano aRb e $a'Rb'$, allora $(a * a')R(b * a')$ e $(b * a')R(b * b')$, da cui per transitività $(a * a')R(b * b')$. □

Definizione 3.18 *Indichiamo per $a \in X$ con $[a]_R$ la classe di equivalenza $\{b \in X : bRa\}$ di a rispetto ad R e con $X/R = \{[a]_R : a \in X\}$ l'insieme quoziente.*

Proposizione 3.19 *Sia R una congruenza su un insieme X dotato dell'operazione $*$, allora è definita su X/R l'operazione $*_R : X/R \times X/R \to X/R$ ponendo $\forall\ [a]_R, [b]_R \in X/R$:*

$$[a]_R *_R [b]_R := [a * b]_R$$

Dim. Dimostriamo che tale operazione è ben definita modificando i rappresentanti delle classi coinvolte. Sia aRa', allora $(a * b)R(a' * b)$. Si procede analogamente se $b'Rb$. □

L'importanza di questa proposizione è che fornisce una ricetta per costruire nuove strutture algebriche a partire da congruenze su strutture note.

3.4 Congruenze sugli interi

Sia $\mathbb{N} = \{0, 1, 2, \ldots\}$ l'insieme dei numeri naturali (in questo corso $0 \in \mathbb{N}$). Nel corso di Fondamenti avete incontrato la nozione di relazione di equivalenza. Il concetto di congruenza ottenuta da una relazione rispetto ad un'operazione è originato dalle congruenze su $\mathbb{Z}$. Queste sono state introdotte da Gauss agli inizi dell'Ottocento per risolvere varie questioni di Teoria dei Numeri.

Definizione 3.20 *Siano $a,\ b \in \mathbb{Z}$. Si dice che b* ***divide*** *a (o a è un* ***multiplo*** *di b) e si scrive $b \mid a$ se esiste $c \in \mathbb{Z}$ tale che $a = bc$. Dato $m \in \mathbb{N}$, si dice b^m è la massima potenza di b che divide a se $b^m \mid a$ ma $b^{m+1} \nmid a$. Si scriverà anche $b^m \mid\mid a$.*

Osservazione 3.21 *Si osservi che la relazione aRb sse $a \mid b$ è riflessiva e transitiva, ma non simmetrica. Se $a \mid b$ e $b \mid a$, allora $b = \pm a$.*

Definizione 3.22 *Sia $n \in \mathbb{Z},\ n > 1$. Se $a,\ b \in \mathbb{Z}$ diciamo che a è* ***congruo*** *b modulo n e scriviamo*

$$a \equiv b \pmod{n} \qquad \text{o} \qquad a \equiv_n b$$

se $n \mid (a - b)$. Cioè se $\exists\, h \in \mathbb{Z}$ tale che $a - b = hn$.

Un esempio di risultato che coinvolge le congruenze è il seguente:

Teorema 3.23 (Piccolo Teorema di Fermat) *Sia p primo e $a \in \mathbb{Z}$ con $p \nmid a$. Allora $a^{p-1} \equiv 1 \pmod{p}$.*

Si noti che $a \equiv b \pmod{n}$ sse $a \equiv b \pmod{-n}$. Inoltre per $n = 0$, $a \equiv b \pmod{n}$ sse $a = b$. Quindi possiamo d'ora in poi assumere $n > 0$.

Proposizione 3.24 *La relazione di congruenza modulo n è di equivalenza. Se $n > 0$, le partizioni determinate dalle classi di equivalenza sono esattamente n. Indicata con $[\,a\,]_n$ la classe di equivalenza contenente a, l'insieme delle classi di equivalenza fissato n sono $[\,0\,]_n$, $[\,1\,]_n$, $\ldots, [\,n-1\,]_n$; sono cioè rappresentate da tutti i possibili resti nella divisione intera per n.*

Dim. Proviamo che è una relazione di equivalenza.

1. Riflessiva: Infatti $a - a = 0n$.
2. Simmetrica: $a - b = hn$ implica $b - a = (-h)n$.
3. Transitiva: $a - b = hn$ e $b - c = kn$ implica $a - c = (h + k)n$.

Sia $a = nq + r$, con $0 \leq r < n$, allora $a \equiv r \pmod{n}$. Infine se $0 \leq r \leq s < n$, allora $s \equiv r \pmod{n}$ sse $r = s$. Quindi ho esattamente n classi di equivalenza rappresentate da $0 \leq r < n$. □

Definizione 3.25 *Sia $\mathbb{Z}$ con la relazione $\equiv_n$ di congruenza modulo n. Allora le classi $[\,a\,]_n$ vengono dette classi di resto e l'insieme quoziente viene indicato con*

$$\mathbb{Z}/n = \{[\,0\,]_n, \ldots, [\,n-1\,]_n\}.$$

Facciamo notare che gli interi tra 0 e $n-1$ non sono gli unici rappresentanti per le classi di resto. Per vari motivi sono importanti anche rappresentanti s piccoli in valore assoluto, ossia tali che $|2s| \leq n$.

Definizione 3.26 *Dato $0 < n \in \mathbb{N}$ e la relazione di congruenza modulo n, si dicono **rappresentanti canonici** gli interi r tali che $0 \leq r < n$, ossia i resti della divisione mediante n. Si dicono **rappresentanti ridotti** gli interi s tali che $2|s| \leq n$ e se $n = 2m$ è pari, essendo m e $-m$ equivalenti, si pone m come rappresentante ridotto della classe $[m]_n$.*

Esercizio 3.27 *Mostrare che i rappresentanti ridotti modulo $0 < n \in \mathbb{N}$ si possono definire come gli interi tali che*

$$-\frac{n-1}{2} \leq s \leq \frac{n}{2}$$

(distinguete i casi n pari, dispari).

Mostriamo ora che la **congruenza modulo** n è una **congruenza** rispetto alle operazioni di somma e prodotto.

Proposizione 3.28 *La congruenza modulo n è compatibile con $+$ e $\cdot$ definiti in $\mathbb{Z}$.*

Dim. Bisogna provare la compatibilità con somma e prodotto, ossia dobbiamo provare che

$$a \equiv a',\ b \equiv b' \pmod{n} \implies (a+b) \equiv (a'+b'),\ ab \equiv a'b' \pmod{n}.$$

Le prime due condizioni implicano che esistono $h, k \in \mathbb{Z}$ tali che:

$$a - a' = hn, b - b' = kn.$$

Da queste ricaviamo $a = a' + hn$ e $b = b' + kn$. Quindi

$$a + b = a' + b' + (h+k)n.$$

e

$$ab = a'b' + (hb' + ka' + hkn)n,$$

da cui $a' + b' \equiv a + b,\ a'b' \equiv ab \pmod{n}$. □

Quindi per quanto visto è possibile definire sull'insieme $\mathbb{Z}/n$ delle operazioni indotte dalla somma e dal prodotto di numeri relativi. Useremo per comodità ancora i simboli $+$ e $\cdot$ per denotare tali operazioni. La somma sarà definita da:

$$[\,a\,]_n + [\,b\,]_n := [\,a+b\,]_n.$$

Tale operazione avrà come unità bilatera $[\,0\,]_n$ in quanto:

$$[\,a\,]_n + [\,0\,]_n = [\,a+0\,]_n = [\,a\,]_n = [\,0+a\,]_n = [\,0\,]_n + [\,a\,]_n.$$

Inoltre la somma delle classi per come è stata definita eredita tutte le proprietà equazionali della somma sui numeri interi ed è quindi associativa e commutativa. È possibile inoltre definire un prodotto in $\mathbb{Z}/n$ ponendo:

$$[\,a\,]_n \cdot [\,b\,]_n = [\,ab\,]_n.$$

Per il prodotto l'unità bilatera sarà $[\,1\,]_n$. Infatti:

$$[\,a\,]_n \cdot [\,1\,]_n = [\,a \cdot 1\,]_n = [\,a\,]_n = [\,1 \cdot a\,]_n = [\,1\,]_n \cdot [\,a\,]_n$$

Esempio 3.29 *Poniamo $n = 6$ e scriviamo le tavole di composizione della somma e del prodotto in $\mathbb{Z}/6$. Per comodità di scrittura si scriverà $\boldsymbol{k}$ invece di $[\,k\,]_6$, il lettore presti attenzione a questo particolare in modo da non confondere $[\,k\,]_6$ con il valore k.*

Dalla tavola di composizione della somma si può trovare l'inverso di un elemento di $\mathbb{Z}/6$ semplicemente scorrendo la riga e cercando l'unità (cioè lo $\mathbf{0}$). Ad esempio si ha che $\mathbf{4}+\mathbf{2} = \mathbf{0}$ ($[\,4\,]_6 + [\,2\,]_6 = [\,0\,]_6$) e quindi $\mathbf{4}$ è inverso sinistro (e bilatero, per la commutatività) di $\mathbf{2}$. Osservando la tavola di composizione del prodotto si nota facilmente che non tutti gli elementi hanno inverso! Infatti