CLASSI DI EQUIVALENZA

Sia A un insieme e ρ una relazione di equivalenza (→ riflessiva, simmetrica e transitiva.) definita in A. Dato un elemento $a \in A$, si definisce "classe di equivalenza" di a l'insieme : $[a]_\rho = \{x \in A \setminus x \rho a\} = \{x \in A \setminus a \rho x\}$

↳ rappresentante della classe

Proprietà delle classi

Siano A un insieme e ρ una relazione di equivalenza definita su A. E siano $a, b \in A$. Allora:

1) $[a]_\rho \neq \emptyset$
2) $[a] = [b] \iff a \rho b$
3) $[a] \neq [b] \iff [a] \cap [b] = \emptyset$

Dim:

(1) ρ é di equivalenza $\Rightarrow$ ρ é riflessiva $\Rightarrow \forall a \in A\ (a \rho a) \Rightarrow \forall a \in A\ ([a]_\rho \neq \emptyset)$
Questo perché ogni classe ha almeno il suo rappresentante.

(2) ($\Rightarrow$)
Dato il punto 1, $\forall a \in A, a \in [a]_\rho$. Per ipotesi $[a] = [b] \Rightarrow a \in [b] = \{x \in A / x \rho b\} \Rightarrow a \rho b$

($\Leftarrow$)
Per la teoria degli insiemi, $[a] = [b] \iff [a] \subseteq [b] \wedge [b] \subseteq [a]$.

- $[a] \subseteq [b] \iff \forall x \in [a], x \in [b]$

$x \in [a] \Rightarrow x \rho a$, ma per ipotesi, $a \rho b$. Essendo ρ di equivalenza (quindi transitiva) allora $x \rho a \wedge a \rho b \Rightarrow x \rho b$.
Abbiamo così ottenuto che $\forall x \in [a], x \in [b] \Rightarrow [a] \subseteq [b]$.

- $[b] \subseteq [a] \iff \forall x \in [b], x \in [a]$.

$x \in [b] \Rightarrow x \rho b$, ma per ipotesi, $a \rho b$. Sfruttiamo la simmetria: $a \rho b \Rightarrow b \rho a$ e sfruttiamo la transitività: $x \rho b \wedge b \rho a \Rightarrow x \rho a$. Otteniamo così quello che volevamo dimostrare.

(3) ($\Rightarrow$)
Supponiamo per assurdo che $[a] \cap [b] \neq \emptyset$.
Questo implica che $\exists c \in [a] \cap [b]$:

$$\left.\begin{array}{l} \bullet\ c \in [a] \Rightarrow c \rho a \Rightarrow [c] = [a] \\ \bullet\ c \in [b] \Rightarrow c \rho b \Rightarrow [c] = [b] \end{array}\right\} \text{assurdo perché avevamo supposto che } [a] \neq [b].$$

($\Leftarrow$)
Sia per assurdo $[a] = [b]$.
$[a] \cap [b] = [a] \cap [a] = [a] \neq \emptyset$ il che è un assurdo perché avevamo supposto che $[a] \cap [b] = \emptyset$.

Teorema fondamentale dell'aritmetica

Sia $n \in \mathbb{Z} \setminus \{-1,0,1\}$. Tale elemento o è esprimibile come prodotto di primi o è esso stesso primo. Inoltre se $n = p_1 \cdot p_2 \cdot ... \cdot p_r = q_1 \cdot q_2 \cdot ... \cdot q_s$ con $r, s \in \mathbb{N}^*$ e poi $p_1, p_2, ..., p_r, q_1, q_2, ..., q_s$ primi, allora $r = s$ ed esiste una permutazione σ di $\{1, ..., s\}$ tale che $p_i = \pm q_{\sigma(i)}$ per ogni $i = 1, ..., s$.

Dim (esistenza)

Sia $n \in \mathbb{Z}$, $n \geq 2$. Dimostriamo la tesi per induzione su n.

- Passo base: sia $n = 2$. Poichè 2 è primo* => l'enunciato è vero.
- Passo induttivo: supponiamo la tesi vera per ogni numero compreso tra 2 ed n. Dimostriamolo per $n+1$.
  Se $n+1$ è primo, abbiamo dimostrato la tesi.
  Se $n+1$ non è primo, allora esiste p che divide $n+1$ => $\exists a \in \mathbb{Z} \,(n+1 = p \cdot a)$ con $2 \leq a \leq n$. Poichè $2 \leq a \leq n$, per ipotesi induttiva o a è primo, oppure si può scrivere come prodotto tra numeri primi.
  A ogni modo siamo riusciti a scrivere $n+1$ come prodotto di numeri primi, e da ciò segue la tesi.

(unicità)

Procediamo per assurdo e supponiamo che:

$n = p_1 \cdot p_2 \cdot ... \cdot p_r$

$n = q_1 \cdot q_2 \cdot ... \cdot q_s$

primo

$p / ab \Rightarrow p/a \vee p/b$

Allora $p_1 / n = q_1 \cdot q_2 \cdot ... \cdot q_s$ => p_1 divide almeno uno dei q_i. A meno di riordinare $q_1, q_2, ..., q_s$ possiamo supporre che p_1 / q_1, ma allora, essendo primi, $p_1 = q_1$ oppure $p_1 = -q_1$. Dividendo ora n per p_1 si ottiene dunque:

$$p_2 \cdot ... \cdot p_r = n = \pm q_2 \cdot ... \cdot q_s$$

Procedendo in questo modo alla fine si ricava $n = s$, ed anche l'unicità dei primi nelle due fattorizzazioni, a meno dell'ordine e dei segni.

Perchè 2 è primo? Per essere primo (irriducibile), un intero a:

1) Non è invertibile
2) Ha solo divisori banali
   - se consideriamo il monoide commutativo $(M, \cdot)$, sono gli elementi associati ad a e invertibili in M.
   - Sono propri i divisori NON associati ad a.

In aiuto abbiamo il lemma di Gauss che afferma che: $\forall p \in \mathbb{Z}$ vale la seguente implicazione:

$$p \in \mathbb{P} \Rightarrow \forall a, b \in \mathbb{Z}\,(p/ab \Rightarrow p/a \vee p/b)$$

2 non è nullo e non è invertibile (in quanto in $\mathbb{Z}$ gli unici invertibili sono 1 e -1). Dobbiamo dimostrare l'implicazione sopra. Siano $a, b \in \mathbb{Z}$ t.c. $2/ab$.

- Se a è pari => $2/a$ e abbiamo finito.
- Se a è dispari => $2 \nmid a$. In particolare $a \equiv_2 1$. Per ipotesi $2/ab$ => $ab \equiv_2 0$. Sostituendo otteniamo $1b \equiv_2 0$ => $b \equiv_2 0$ che significa che b è pari => $2/b$. Che è quello che volevamo dimostrare.

TEOREMA DI BÉZOUT

Siano a e b interi positivi non nulli. Sia $d = MCD(a,b)$. Allora $\exists u,v \in \mathbb{Z}(d = au + bv)$

Dim

resto della divisione Euclidea.

Sia t il minimo numero di passi tale che $r_t = 0$.

- Se il primo resto è 0 (quindi $t = 1$), allora $a = bq_1 \Rightarrow b = MCD(a,b)$ e si può scrivere come $b = a \cdot 0 + b \cdot 1 \Rightarrow (u,v) = (0,1)$.
- Se il secondo resto è 0 ($t = 2$), allora $r_1 \neq 0$ e $r_2 = 0$. Quindi $r_1 = a - bq_1 = a \cdot 1 + b \cdot (-q_1)$. Dunque $r_1 = MCD(a,b)$ e $(u,v) = (1,-q_1)$

Assumiamo l'asserto vero $\forall r_i : 1 \leq i < t$. Vogliamo dimostrare che $r_t = 0 \Rightarrow r_{t-1} = MCD(a,b)$. Assumiamo che i due resti precedenti, cioè r_{t-2} e r_{t-3} sono già esprimibili come combinazione lineare, ovvero $r_{t-2} = au + bv$ e $r_{t-3} = aw + bx$. Sostituiamo queste espressioni in:

$$\left.\begin{aligned} r_{t-1} &= r_{t-3} - q_{t-1} \cdot r_{t-2} = \\ &= (aw + bx) - q_{t-1}(au + bv) = \\ &= aw + bx - q_{t-1} \cdot au - q_{t-1} bv = \\ &= a(w - uq_{t-1}) + b(x - vq_{t-1}) \end{aligned}\right\} \Rightarrow r_{t-1} = au' + bv'$$

PRODOTTO TRA POLINOMI

La definizione formale del prodotto tra polinomi come successioni è:

- $\cdot : ((a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}}) \in A[x] \times A[x] \mapsto \left(\sum_{i+j=n} a_i + b_j\right)_{n\in\mathbb{N}}$

Facciamo un esempio pratico per capire meglio: sia $f(x) = 2 + 3x\ (2,3,0,0,\dots)$ e $g(x) = 1 + x = (1,1,0,0,\dots)$

Allora:

$$\left.\begin{aligned} c_0 &= a_0 b_0 \ (\text{perché}: 0 = 0 + 0) = 2 \cdot 1 = 2 \\ c_1 &= a_0 b_1 + a_1 + b_0 = 2 \cdot 1 + 3 \cdot 1 = 5 \\ c_2 &= a_0 b_2 + a_2 b_0 + a_1 b_1 = 2 \cdot 0 + 3 \cdot 1 + 0 \cdot 1 = 3 \end{aligned}\right\} f(x) + g(x) = (2,5,3,0,0,\dots) = 2 + 5x + 3x^2$$

coefficienti in posizione k

QUALCHE AGGIUNTA SUI POLINOMI

Sia A un anello. $f \in A[x]$ è invertibile $\Leftrightarrow$ è un polinomio costante con coefficienti invertibili in A

La legge di addizione dei gradi vale se i coefficienti dei polinomi appartengono a un dominio di integrità (come un campo)

↳ La legge NON vale in generale se l'anello dei coefficienti ha divisori dello zero.

ESEMPIO DI ANELLO BOOLEANO A 3 E 8 ELEMENTI

$(P(S), \subseteq)$ un reticolo booleano (reticolo distributivo e complementato), possiamo prendere il suo corrispettivo anello booleano (anello in cui ogni elemento è idempotente, e $(A,+,\cdot)$ anello commutativo unitario) $(P(S), \Delta, \cap)$.

- $|P(S)| = 3$ è impossibile perché non esiste alcun n tale che $2^n = 3$.
- $|P(S)| = 8 \Leftrightarrow |S| = 3$.

PASSARE DA ORDINE LARGO A STRETTO E VICEVERSA

Sia $\rho \in OL(A)$. Definiamo $\bar\rho \in OS(A)$ tale che $\forall x,y \in A\ (x \bar\rho y \Leftrightarrow x \rho y \wedge x \neq y)$

Sia $\rho \in OS(A)$. Definiamo $\bar\rho \in OL(A)$ tale che $\forall x,y \in A\ (x \bar\rho y \Leftrightarrow x \rho y \wedge x = y)$.

QUANDO $\mathbb{Z}_m$ È UN CAMPO?

$\mathbb{Z}_m$ è un campo $\Leftrightarrow$ m è primo.

Dim.

Se m è primo, tutti gli interi $1, \dots, m-1$ sono coprimi con m e quindi tutte le classi $[1]_m, [2]_m, \dots, [m-1]_m$ sono invertibili (per il primo corollario del criterio di esistenza delle soluzioni congruenziali).

Viceversa, supposto che $\mathbb{Z}_m$ sia un campo, se m non fosse primo, esisterebbe un divisore m_1 di m tale che $1 < m_1 < m$. Allora risulterebbe $[m_1]_m \neq [0]_m$ ed $[m_1]_m$ non invertibile dato che $MCD(m, m_1) = m_1 > 1$.
Dall'assurdo segue che m è necessariamente primo.

COME SI DIMOSTRA CHE p È PRIMO?

Lemma sui divisori dei primi:
Se $p \in \mathbb{Z}$ è primo $\Rightarrow$ $Div(p) = \{1, -1, p, -1\}$ (ha solo divisori banali).

Dim.

Sia $n \in \mathbb{Z}$ t.c. n / p $\Leftrightarrow$ $\exists k \in \mathbb{Z} (p = nk)$ $\Rightarrow$ $p / n \vee p / k$ (per definizione di primo).

- Nel caso in cui $p / n \Leftrightarrow \exists h \in \mathbb{Z} (n = ph) \Rightarrow p = phk \Rightarrow hk = 1 \Rightarrow h = k = \pm 1 \Rightarrow n = \pm p$.

- Nel caso in cui $p / k \Leftrightarrow \exists h \in \mathbb{Z} (k = ph) \Rightarrow p = nph \Rightarrow nh = 1 \Rightarrow n = h = \pm 1 \Rightarrow n = \pm 1$ $\square$

SE $\mathbb{Z}_m$ È UN DOMINIO DI INTEGRITÀ $\Rightarrow$ m È PRIMO

Dim

Sia $(\mathbb{Z}_m, +, \cdot)$ un dominio di integrità. Quindi vale la legge di annullamento del prodotto. Sia $m = ab$, allora $[m]_m = [0]_m = [ab]_m = [a]_m \cdot [b]_m \Rightarrow a \equiv_m 0 \vee b \equiv_m 0$. Supponiamo che $a \equiv_m b$, quindi $\exists k \in \mathbb{Z} (a = km) \Rightarrow m = ab = kmb \Rightarrow kb = 1 \Rightarrow b = \pm 1$ e $a = \pm m$.
Dunque m è primo perché ha solo divisori banali.