Soluzioni degli esercizi della settimana del 16 dicembre.

Esercizio 1

Sia R un anello senza nilpotenti, ossia tale che se $x^n = 0$ per qualche n allora necessariamente $x = 0$. Sappiamo inoltre che, per ogni $a, b \in R$ vale $(ab)^2 = a^2 \cdot b^2$. Dimostrare che R è commutativo.

Soluzione

Notiamo che la relazione del testo (valida per ogni scelta di a, b) si riscrive come $a(ba - ab)b = 0$ o $a(ab - ba)b = 0$ (semplicemente moltiplicando per -1).
Usando la coppia $a, a + b$ al posto di a, b otteniamo $a(ab - ba)(a + b) = 0$ e se sottraiamo $a(ab - ba)b = 0$ ricaviamo $a(ab - ba)a = 0$. Per un semplice ragionamento di simmetria, valgono anche le identità $b(ab - ba)b = 0, b(ab - ba)a = 0$.
Ricaviamo $(ab - ba)^3 = 0$ (svolgere i conti per convincersene) e dunque, dal testo $ab - ba = 0 \Leftrightarrow ab = ba$ da cui la commutatività cercata.

Esercizio 2

Consideriamo l'anello A delle funzioni continue $[0, 1] \to \mathbb{R}$, dove la struttura di anello è data dalla somma puntuale e dal prodotto puntuale. Siano adesso, per $n \geq 2$, $f_1, \ldots, f_n$ delle date funzioni. Sappiamo che non si annullano tutte contemporaneamente.

1. Mostrare che l'ideale da loro generato $(f_1, \ldots, f_n)$ è tutto A.

2. Provare a capire chi sono gli ideali massimali $I \subset A$ e conseguentemente chi è il campo A/I.

Soluzione

La chiave qui è notare la libertà che si ha nel "prodotto interno": se f è una funzione continua che **non si annulla mai** allora anche $\frac{1}{f}$ è una funzione continua. Ma allora se f appartiene ad un certo ideale I, la chiusura per prodotto ci garantisce che anche $f \cdot \frac{1}{f} \in I$ ossia $I = (1)$. Abbiamo appena mostrato che un ideale $I \subset A$ è uguale ad A se e solo se esiste $f \in I$ che non si annulla mai.
Proseguiamo con l'esercizio.
1) Basta mostrare che esiste f mai nulla dentro $(f_1, \ldots, f_n)$: possiamo considerare $f_1^2 + f_2^2 + \cdots + f_n^2$. Non si annulla mai perché è una somma di quadrati mai contemporaneamente nulli (ipotesi del testo).
2) Sicuramente tutte le funzioni $f \in I$ devono annullarsi in almeno un punto (altrimenti l'ideale sarebbe tutto A), inoltre per il punto precedente **non** deve esistere un sottoinsieme di funzioni di I che non si annulla contemporaneamente. In altre parole, tutte le funzioni devono condividere "uno zero". Dato che, fissato un $x_0 \in [0,1]$, $\{f \in I | f(x_0) = 0\}$ è un ideale, è anche massimale per le considerazioni di prima e tutti i massimali provengono da qui. In tutti i casi il quoziente è $\mathbb{R}$: fissato x_0 che definiva il massimale I possiamo osservare la surgezione $A \xrightarrow{f \mapsto f(x_0)} \mathbb{R}$ e notare che il suo kernel è proprio I. Concludiamo per il primo teorema di isomorfismo.

Esercizio 3

Definiamo *caratteristica* di un anello A in maniera grezza come "il minimo numero n tale che sommando n volte consecutive il neutro della moltiplicazione, si arriva a 0". Tale caratteristica può essere 0 quando n è infinito (ossia non arrivo mai a 0) oppure un numero positivo.

Supponiamo adesso A campo.

1. Che valori può avere n?

2. Esiste un campo con n elementi? Se sì, quanti omomorfismi di anelli esistono $\mathbb{F}_n \to A$? Questi oggetti si chiamano "*oggetti iniziali*" (in un appropriato contesto).

3. Cosa abbiamo usato di A campo? Verificare che tutto ciò che abbiamo detto funziona usando solo A dominio.

4. Esiste un dominio con 15 elementi? E con 64?

Soluzione

1) I valori ammissibili per n sono tutti e soli i numeri primi. Chiaramente loro sono ottenuti, ad esempio da $\mathbb{Z}_n$. Inoltre, qualsiasi caratteristica di un campo è prima: sia n non primo fattorizzabile come $n = h \cdot k$ (non 1) la caratteristica di un campo $\mathbb{F}$. Questo vuol dire che $\overbrace{1+1+\cdots+1}^{n} = 0$ in $\mathbb{F}$ ed in particolare $\overbrace{\overbrace{1+\cdots+1}^{h}+\cdots+\overbrace{1+\cdots+1}^{h}}^{k} = 0$ quindi $k \cdot \overbrace{1+\cdots+1}^{h} = 0$ da cui ($\mathbb{F}$ campo) $\overbrace{1+\cdots+1}^{h} = 0$ che è un assurdo per minimalità di n. Segue che non esistono fattorizzazioni non banali di n e dunque è primo.
2) Si: $\mathbb{Z}_n$ con n primo (condizione garantita dal primo punto essendo n la caratteristica di A) è un anello con tutti i non zero invertibili (è un campo). Esiste solo 1 morfismo: un omomorfismo di anelli unitari manda $\mathbb{F}_n \ni 1 \mapsto 1 \in A$ ed ha kernel banale. Tuttavia 1 genera additivamente $\mathbb{F}_n$ (cosa spesso falsa, basti pensare a $\mathbb{Q}$ o ad un qualsiasi anello di polinomi) pertanto aver fissato l'immagine di 1 implica aver fissato l'omomorfismo.
3) Nei discorsi appena fatti abbiamo solo utilizzato la legge di annullamento del prodotto. Questa vale nei domini, pertanto ne concludiamo che la caratteristica di un dominio è prima.
4) I domini finiti sono campi: dobbiamo esibire l'invertibilità di un elemento $a \in A$ non zero. Osserviamo che la mappa $A \to A$(solo insiemisticamente) di moltiplicazione per a è iniettiva (per via dell'annullamento del prodotto), dunque è surgettiva per ipotesi di finitezza. Allora esiste un b tale che $1 = b \cdot a$ che è proprio l'inverso di a (esiste inverso da entrambi i lati e questi sono uguali, è un altro esercizietto). Adesso possiamo concludere in due modi: sappiamo dalla teoria che i campi finiti hanno cardinalità tutte e sole le potenze dei primi pertanto non esiste un campo di 15 elementi. Alternativamente potevamo notare (senza ragionamenti sull'essere campo) che un dominio di 15 elementi ha caratteristica 3 oppure 5 e dunque sarebbe rispettivamente uno spazio vettoriale (di dimensione finita) sul campo $\mathbb{Z}_3$ o $\mathbb{Z}_5$: nel primo

caso avrebbe cardinalità una potenza di 3, nel secondo una potenza di 5, ma 15 non è nessuno dei due.
Per 64 la risposta è affermativa: esiste un campo con 64 elementi: una qualsiasi estensione di grado 8 di $\mathbb{Z}_2$ va bene.

Esercizio 4

L'unità immaginaria i è contenuta nell'estensione dei razionali $\mathbb{Q}(\sqrt[4]{-2})$? E $\sqrt{5}$ in $\mathbb{Q}(\sqrt[3]{2})$?

Soluzione

Notiamo preliminarmente che $\mathbb{Q}(\sqrt[4]{-2})$ è una estensione di grado 4 di $\mathbb{Q}$ e che contiene $\sqrt[2]{-2} = i\sqrt{2}$. Se contenesse i allora conterrebbe anche $i\sqrt{2}/i = \sqrt{2}$ quindi in particolare $\mathbb{Q}(i, \sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{-2})$. Dato che sono entrambe estensioni di grado 4 su $\mathbb{Q}$ ricaviamo $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\sqrt[4]{-2})$ tuttavia nella parte a sinistra è contenuta una radice quarta di -1 pertanto se contenesse anche $\sqrt[4]{-2}$ allora in particolare conterrebbe $\sqrt[4]{2}$. Questa cosa è un assurdo: varrebbe $\sqrt[4]{2} \in \mathbb{Q}(i, \sqrt{2}) \cap \mathbb{R} = \mathbb{Q}(\sqrt{2})$ ma il polinomio minimo su $\mathbb{Q}$ di $\sqrt[4]{2}$ ha grado 4 mentre l'estensione $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ ha grado 2.
Ne concludiamo che $i \notin \mathbb{Q}(\sqrt[4]{-2})$.
Per il secondo punto basta osservare che $\mathbb{Q}(\sqrt{5})$ è un'estensione di grado 2 di $\mathbb{Q}$ e per il teorema sul grado di una torre di estensioni, se fosse contenuta in $\mathbb{Q}(\sqrt[3]{2})$, dovremmo avere $2|[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Questo è un assurdo pertanto $\sqrt{5} \notin \mathbb{Q}(\sqrt[3]{2})$.

Esercizio 5

Quanti polinomi irriducibili di grado n esistono nell'anello $\mathbb{F}_p[x]$?

Soluzione e commenti

Questo esercizio è difficile. Mi sono confuso sulla richiesta (avevo risolto un esercizio differente e ho ricordato male) ed è uscita fuori questa cosa..
Ritengo sia istruttiva: sostanzialmente tutto il procedimento è identico, solo il conto finale utilizza uno strumento che probabilmente non avete visto.
Primo **lemma importante**: il prodotto di tutti i polinomi *monici* irriducibili

di grado che divide n in $\mathbb{F}_p[x]$ è $x^{p^n} - x$.
La dimostrazione di questo fatto non è difficile.
Osserviamo che sicuramente ogni monico irriducibile divide $x^{p^n} - x = p(x)$ infatti basta verificare (qui usiamo l'ipotesi *monico*) che tutte le radici di ogni polinomio monico di grado d (che chiamiamo $q(x)$) azzerino anche $p(x)$. Sappiamo che il campo di spezzamento di $q(x)$ è proprio il campo $\mathbb{F}_{p^d}$ e che $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n} \Leftrightarrow d|n$ ed inoltre $\alpha \in \mathbb{F}_{p^n} \Leftrightarrow \alpha^{p^n} - \alpha = 0$: abbiamo appena mostrato che tutte le radici di $q(x)$ azzerano $p(x)$. D'altronde ogni zero di $p(x)$ proviene da un certo polinomio minimo di grado che divide n (per il se e solo se del contenimento di campi appena enunciato) e gli zeri sono tutti distinti fra loro per il criterio della derivata.
Segue il **lemma**.
Adesso ci siamo quasi. Chiamiamo $S(d)$ il numero di polinomi *monici* e **irriducibili** di grado d (questo è quasi ciò che cerchiamo, basterà moltiplicare per le $p-1$ scelte del termine di testa per ottenere quelli **non** monici) e adesso contiamo in due maniere diverse il numero di soluzioni (che ricordo essere tutte diverse) di $x^{p^n} - x = 0$.
Da un lato, queste soluzioni sono esattamente il grado p^n (ricordiamo che le radici sono proprio gli elementi di $\mathbb{F}_{p^n}$).
D'altro canto, abbiamo d radici **distinte** provenienti da *ognuno* (qui usiamo il **lemma**) dei polinomi monici di grado d irriducibili in $\mathbb{F}_p[x]$ per ogni $d|n$ che sono proprio $S(d)$.
Il double-counting ci permette di ottenere

$$p^n = \sum_{d|n} d \cdot S(d)$$

che è molto vicina a dirci $S(n)$.
Qua arriva la parte tecnica (oserei dire anche *non voluta*) dell'esercizio che però ho deciso di riportare per completezza.
DEFINIZIONE Indichiamo con $\mu(n)$ la *funzione di Möbius* definita da

$$\begin{cases} 0 & \text{se } n \text{ è diviso da un quadrato} \\ -1 & \text{se } n \text{ è prodotto di un numero pari di fattori primi distinti} \\ 1 & \text{se } n \text{ è prodotto di un numero pari di fattori primi distinti.} \end{cases}$$

La funzione di Möbius permette di risolvere dei problemi di "inversione" (intesa come "ricavare" f da una somma che coinvolge f) come quello che ci

interessa.
Enunciamo la proposizione principale, nonché quella che ci permette di ottenere la risposta finale.

TEOREMA DI INVERSIONE DI MÖBIUS
Date f, g funzioni $\mathbb{N} \to \mathbb{C}$ tali che

$$f(n) = \sum_{d|n} g(d)$$

allora

$$g(n) = \sum_{d|n} \mu(d) \cdot f(n/d).$$

La dimostrazione è un esercizio di riarrangiamento che si basa sul fatto che $\sum_{d|n} \mu(d)$ fa 1 per $n = 1$ e 0 altrimenti.

Possiamo concludere. Una diretta applicazione del teorema alle funzioni $n \cdot S(n)$ e p^n ci dà

$$n \cdot S(n) = \sum_{d|n} \mu(d) \cdot p^{n/d}$$

da cui

$$(p-1) \cdot S(n) = \frac{p-1}{n} \cdot \sum_{d|n} \mu(d) \cdot p^{n/d}$$

è proprio la risposta cercata.