$\odot$ MATRICOLA: .... **A**: ... **B**: ... **C**: ... **D**: ... VOTO: ......

COGNOME: .... NOME: ....

Algebra 1 – Prova Intermedia: II Esonero 20.01.16

Rispondere alle domande su questo foglio usando gli appositi spazi e giustificando brevemente ma esaurientemente tutte le risposte.

A Sia $\mathbb{Z}[i]$ l'anello degli interi di Gauss.

1. L'ideale $(1-2i) \subseteq \mathbb{Z}[i]$ è proprio ? [Sì] 2

Sia A un anello commutativo con unità e sia a un elemento di A. Sappiamo che (a)=A se e solo se a è invertibile. Nell'anello degli interi di Gauss gli elementi invertibili sono 1, -1, i, -i, pertanto (1-2i) è un ideale proprio.

2. È vero che $5 = 0$ in $\mathbb{Z}[i]/(1-2i)$? [Sì] 2

Infatti 5=(1-2i)(1+2i) appartiene all'ideale generato da 1-2i.

3. $1-2i$ è irriducibile in $\mathbb{Z}[i]$? [Sì] 2

La norma di 1-2i è 5, dunque un intero primo. Sappiamo che gli interi di Gauss la cui norma sia un intero primo sono primi. Dunque 1-2i è primo, il che equivale ad essere irriducibile.

4. L'ideale $(1-2i) \subset \mathbb{Z}[i]$ è massimale ? [Sì] 2

L'anello degli interi di Gauss è un P.I.D., dunque gli ideali massimali sono tutti e soli gli ideali primi. Poiché, come si è visto, 1-2i è un intero di Gauss primo, esso genera un ideale primo.

B Sia A un anello commutativo unitario e $\mathrm{M}_2(A)$ le matrici 2×2 con entrate in A. Sia

$$G_A \stackrel{\text{def}}{=} \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid (a,b) \neq (0,0)\ a,b \in A \right\} \subset \mathrm{M}_2(A)$$

dove $(\mathrm{M}_2(A), \ \cdot \ , I)$ è considerato come monoide rispetto al prodotto righe per colonne. Sia $\mathrm{GL}_2(A) \stackrel{\text{def}}{=} \mathrm{M}_2(A)^*$ il gruppo moltiplicativo delle matrici invertibili.

1. Se A è un campo ordinato allora G_A è un sottogruppo di $\mathrm{GL}_2(A)$? [Sì] | 3 | |

Le matrici invertibili sono tutte e sole quelle il cui determinante è invertibile nell'anello dei coefficienti. Nel nostro caso, l'elemento $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in G_A$ ha determinante a^2+b^2, e in un campo ordinato la somma di due quadrati è nulla solo se gli addendi sono nulli. Dunque $G_A \subseteq GL_2(A)$. Inoltre G_A è chiuso rispetto al prodotto e all'inversione; infatti:

$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac-bd & -ad-bc \\ bc+ad & -bd+ac \end{pmatrix} \in G_A$, (notare che quest'ultima matrice non può essere nulla, perché è prodotto di due invertibili..) e $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}^{-1} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \frac{1}{a^2+b^2}$ è in G_A.

2. Se $A = \mathbb{Z}$ allora $G_\mathbb{Z} \subset \mathrm{M}_2(\mathbb{Z})$ è un sottomonoide ? [Sì] È un gruppo ? [No] | 2 | |

Si ha che $G_\mathbb{Z}$ contiene la matrice identica ed è chiuso rispetto al prodotto (vedi sopra), dunque è un sottomonoide. D'altra parte, ad esempio, l'elemento $\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ ha determinante 2, dunque non è invertibile in $G_\mathbb{Z}$.

3. Se $A = \mathbb{R}$ la funzione $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \rightsquigarrow a + ib$ è un isomorfismo $G_\mathbb{R} \cong \mathbb{C}^*$? [Sì] | 2 | |

Indichiamo con f la funzione in esame. Si vede immediatamente che f è biettiva. Inoltre:

$$f\left(\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\begin{pmatrix} c & -d \\ d & c \end{pmatrix}\right) = f\left(\begin{pmatrix} ac-bd & -ad-bc \\ bc+ad & -bd+ac \end{pmatrix}\right) =$$

$$= (ac-bd) + i(ad+bc) = (a+ib)\cdot(c+id) =$$

$$= f\left(\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\right) \cdot f\left(\begin{pmatrix} c & -d \\ d & c \end{pmatrix}\right).$$

C Siano $A \stackrel{\text{def}}{=} \mathbb{Z}_5[X]/(X^3+2X+2)$ e $B \stackrel{\text{def}}{=} \mathbb{Z}_5[X]/(X^3-2X+2)$ gli anelli ottenuti come quozienti di $\mathbb{Z}_5[X]$ con gli ideali principali generati dai polinomi X^3+2X+2 e X^3-2X+2 rispettivamente.

1. La cardinalità di A è $|A| = 5^3$ La cardinalità di B è $|B| = 5^3$ 2

Come osservato a lezione, l'anello A è in biezione con l'insieme dei polinomi a coefficienti in $\mathbb{Z}_5$ il cui grado è strettamente minore di 3, e tale insieme ha ovviamente cardinalità 5^3.
Lo stesso argomento vale per l'anello B.

2. Esiste un isomorfismo di anelli $A \cong B$? [No] 2

Il polinomio X^3+2X+2 ha radice 1, dunque è divisibile per $X-1$ ed è pertanto riducibile. Invece, il polinomio X^3-2X+2 non ha radici in $\mathbb{Z}_5$, dunque (essendo di grado 3) possiamo concludere che è irriducibile. Concludiamo che A non è un campo, mentre B lo è, dunque nessun isomorfismo può esistere tra i due anelli.

3. Per ciascuno degli anelli A e B si fornisca un esempio (ove possibile) di
   (a) un elemento invertibile non equivalente a un polinomio costante 1

Ricordiamo che, negli anelli del tipo in questione, gli elementi invertibili sono tutte e sole le classi di equivalenza di polinomi coprimi col generatore dell'ideale con cui si quozienta.
Si ha $X^3+2X+2 = (X-1)^2 \cdot (X+2)$, dunque, ad esempio, la classe di equivalenza del polinomio $X+1$ risulta invertibile sia in A che in B.

   (b) uno zero-divisore 1

Si ha che (X-1)• [(X-1)(X+2)] è equivalente a 0 in A, dunque la classe di equivalenza di X-1 è uno zero-divisore in A. Per quanto riguarda B, esso è un campo e dunque non ha zero-divisori.

   (c) un elemento nilpotente non nullo 1

Si ha $((X-1)(X+2))^2 = (X-1)^2 \cdot (X+2)^2 = (X^3+2X+2) \cdot (X+2)$,
che in A è equivalente a 0. Dunque la classe di $(X-1) \cdot (X+2)$ è un elemento nilpotente di A.
Poiché B è un campo, non ha ovviamente elementi nilpotenti diversi da 0.

D Sia $A = \mathbb{Z}[\sqrt{-7}]$.

1. Esiste un massimo comune divisore di $2 + 2\sqrt{-7}$ e 8 in A ? [No] $\boxed{4}$

Sia d un massimo comune divisore tra i due elementi. Poiché $8 = (1 + i\sqrt{7}) \cdot (1 - i\sqrt{7})$, evidentemente $1 + i\sqrt{7}$ è un divisore comune, e pertanto divide d. Segue che $8 = N(1 + i\sqrt{7})$ divide la norma di d, che a sua volta divide $N(2 + 2i\sqrt{7}) = 32$, dunque la norma di d è 8, 16 o 32. Escludiamo 16, perchè altrimenti si avrebbe $2 + 2i\sqrt{7} = d \cdot z$, con $N(z) = 2$, il che è impossibile. Analogamente (ragionando con 8) si esclude 32. Dunque la norma di d è 8, da cui d= $\pm 1 \pm i\sqrt{7}$.

D'altra parte, 2 è un divisore comune che non divide alcun possibile valore di d.

2. Esiste un massimo comune divisore di $\sqrt{-7}$ e 21 in A ? [Sì] $\boxed{2}$

$i\sqrt{7}$ divide 21, dunque è un massimo comune divisore.

3. Esiste un massimo comune divisore di 8 e 21 in A ? [Sì] $\boxed{2}$

Si tratta di elementi aventi norme coprime, dunque l'insieme dei divisori comuni contiene solo elementi di norma 1. In altre parole, 1 è un massimo comune divisore.