TRENTO, A.A. 2021/22
CORSO DI ALGEBRA A
FOGLIO DI ESERCIZI # 13

Esercizio 13.1. Sia A un dominio dotato di una norma N.
Mostrate che se $a, b \in A$, e $b \mid a$, allora $N(b) \mid N(a)$.

Esercizio 13.2.

(1) Mostrate che in $\mathbf{Z}[\sqrt{-5}]$ non ci sono elementi di norma 2 o 3.
(2) Mostrate che in $\mathbf{Z}[\sqrt{-5}]$ gli elementi $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ sono irriducibili.
(3) Sfruttando l'eguaglianza
$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$
mostrate che gli elementi $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ non sono primi in $\mathbf{Z}[\sqrt{-5}]$.
(4) (Assolutamente facoltativo) Mostrate che in $\mathbf{Z}[\sqrt{-5}]$ non esiste il massimo comun divisore fra
$$a = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \qquad \text{e} \qquad b = 2 \cdot (1 + \sqrt{-5}).$$
(SUGGERIMENTO: Si ha $N(a) = 36$, e $N(b) = 24$. Dunque, procedendo per assurdo, se esistesse il massimo comun divisore d fra a e b, per l'Esercizio 13.1 si avrebbe $N(d) \mid N(a)$ e $N(d) \mid N(b)$, dunque $N(d) \mid \gcd(N(a), N(b)) = \gcd(36, 24) = 12$. D'altra parte 2 divide sia a che b, dunque divide d, e $4 = N(2) \mid N(d)$. Poi $1+\sqrt{-5}$ divide sia a che b, dunque divide d, e $6 = N(1+\sqrt{-5}) \mid N(d)$. Se ne deduce che $12 = \operatorname{lcm}(4, 6) \mid N(d)$, e dunque $N(d) = 12$. Ora si tratta di vedere che in $\mathbf{Z}[\sqrt{-5}]$ non ci sono elementi di norma 12. Per esempio si può argomentare che se fosse $a_0^2 + 5a_1^2 = 12$, allora $a_0^2 \equiv 12 \equiv 2 \pmod 5$, ma 2 non è un quadrato modulo 5.)

Esercizio 13.3.

(1) Date la definizione di dominio a fattorizzazione unica (UFD).
(2) Mostrate che se A è un dominio atomico, sono equivalenti
   (a) in A gli irriducibili sono primi, e
   (b) A è un dominio a fattorizzazione unica (UFD).
(3) Mostrate che $\mathbf{Z}[\sqrt{-5}]$ non è un UFD.

Esercizio 13.4.

(1) Date la definizione di dominio euclideo.
(2) Mostrate che riguardando $\mathbf{Z}$ come un dominio euclideo, quoziente e resto della divisione con resto non sono più unici
(3) Mostrate che la norma di un dominio euclideo è speciale, dunque un dominio euclideo è atomico.
(4) Mostrate che in un dominio euclideo si può fare l'algoritmo di Euclide esteso, dunque esiste il massimo comun divisore, e valgono i Lemmi Aritmetici.
(5) Mostrate che in un dominio euclideo gli irriducibili sono primi, e dunque un dominio euclideo è un UFD.

Esercizio 13.5.

(1) Si mostri che gli interi di Gauss sono un dominio euclideo.
(2) Si trovi il MCD fra 4 e $3 + 5i$ negli interi di Gauss.
(3) Si elenchino le unità degli interi di Gauss.
(4) Si trovi la decomposizione di 2 come prodotto di irriducibili negli interi di Gauss.
(5) Si mostri che se un primo dispari è somma di due quadrati, allora è congruo a 1 modulo 4.
(6) Si mostri che gli interi che sono primi e congrui a 3 modulo 4 sono irriducibili negli interi di Gauss.

Esercizio 13.6. Sia p un numero primo *dispari*, e scriviamo

$$F = \mathbf{Z}/p\mathbf{Z} = \{\, 0, 1, \ldots, p-1 \,\}.$$

(1) Si mostri che se $a \in F^\star$, allora $a \neq -a$.
(2) Si mostri che l'insieme dei quadrati non nulli

$$Q = \left\{\, a^2 : a \in F^\star \,\right\}$$

ha

$$\frac{p-1}{2}$$

elementi.
(3) Si mostri che Q è l'insieme delle radici del polinomio

$$x^{(p-1)/2} - 1 \in F[x].$$

(4) Si mostri che se $a \in F^\star$, allora

$$a^{(p-1)/2} = \begin{cases} 1 & \text{se } a \text{ è un quadrato in } F, \text{ dunque } a \in Q \\ -1 & \text{se } a \text{ non è un quadrato in } F, \text{ dunque } a \notin Q. \end{cases}$$