TRENTO, A.A. 2011/12
CORSO DI ALGEBRA
FOGLIO DI ESERCIZI # 9

Esercizio 9.1 (Questo è un esempio che mostra come ci sono dominî in cui un elemento di norma 1 non è necessariamente invertibile.).

Sia $A = \mathbf{Z}[x]$ l'anello dei polinomi a coefficienti interi.

- Si mostri che la funzione N su A data da
$$N(a) = 2^{\text{grado}(a)}$$
è una norma.
- Si trovino gli elementi di norma 1 di A.
- Si trovino le unità (cioè gli elementi invertibili) di A.

Esercizio 9.2. Si trovino gli elementi invertibili di $\mathbf{Z}[i]$.

Esercizio 9.3. Sia A un dominio, $a \in A$, $a \neq 0$ e a non invertibile.

Si mostri che a è *riducibile* (cioè non irriducibile) se e solo se esistono $u, v \in A$ tali che $a = uv$, ma né u né v è invertibile.

Esercizio 9.4. Sia p un primo dispari in $\mathbf{Z}$. Si mostri che se $p = a^2 + b^2$ per $a, b \in \mathbf{Z}$, allora $p \equiv 1 \pmod 4$.

Esercizio 9.5. Sia A un dominio dotato di una norma N *speciale*. (Dunque $a \in A$ è invertibile in A se e solo se $N(a) = 1$.)

Sia $a \in A$. Si mostri che se $N(a)$ è un numero primo in $\mathbf{Z}$, allora a è irriducibile in A.

Sia $A = \mathbf{Z}[i]$. Si mostri che 3 è irriducibile in $\mathbf{Z}[i]$, ma $N(3) = 9$ non è primo in $\mathbf{Z}$.

(Suggerimento: Se 3 fosse riducibile in $\mathbf{Z}[i]$, allora si dovrebbe scrivere nella forma $3 = uv$, ove né u né v è invertibile. Dunque $N(u) \neq 1 \neq N(v)$. Dato che $9 = N(3) = N(uv) = N(u)N(v)$, dovrebbe essere $N(u) = 3 = N(v)$. Ma se $u = u_0 + iu_1$, allora $3 = u_0^2 + u_1^2$, contro l'Esercizio 9.4.)

Esercizio 9.6. Sia $p \in \mathbf{Z}$, p primo, $p \equiv 3 \pmod 4$.

Si mostri che p è irriducibile in $\mathbf{Z}[i]$.

Esercizio 9.7. Con l'algoritmo visto a lezione, si scrivano come somma di due quadrati alcuni dei seguenti numeri primi p. Per i più grandi si raccomanda di usare GAP.
$$29, 41, 53, 97, 433, 809, 997, 10000173481.$$
Per i primi p considerati, se ne scriva anche la fattorizzazione come prodotto di irriducibili in $\mathbf{Z}[i]$.

E se vi avessi chiesto di scrivere come somma di due quadrati il numero primo
$$10751759?$$

Esercizio 9.8. Si enunci e dimostri la formula per le terne pitagoriche.

Esercizio 9.9. Nel parlare di terne pitagoriche a lezione, siamo partiti con una terna pitagorica primitiva (a, b, c) (dunque $a, b, c \in \mathbf{Z}$, con $a^2 + b^2 = c^2$, si ha $(a, b) = 1$, e a e b hanno diversa parità), e siamo arrivati a vedere che

$$a + ib = \varepsilon(x + iy)^2,$$

per un intero di Gauss $x + iy$, e un'unità $\varepsilon \in \mathbf{Z}[i]$. A lezione abbiamo visto solo il caso $\varepsilon = 1$. Vedete quello che succede negli altri casi $\varepsilon \in \{ i, -1, -i \}$.

Esercizio 9.10 (Facoltativo). Nella formula

$$\begin{cases} a = s^2 - t^2, \\ b = 2st, \\ c = s^2 + t^2, \end{cases}$$

per le terne pitagoriche, si mostri che (a, b, c) è una terna pitagorica *primitiva* se e solo se $(s, t) = 1$, e s, t hanno diversa parità.

Esercizio 9.11. Si mostri che $\mathbf{Z}[i]$ è un dominio euclideo.

Esercizio 9.12 (Facoltativissimo). Nel piano reale, sia C la circonferenza di centro l'origine O, e raggio 1, dunque $C = \{ (x, y) : x^2 + y^2 = 1 \}$.

Sia r una retta passante per i punti $P = (-1, 0)$ e $Q = (1, 2t)$. Sia $R = (1, 0)$.

Sia $Z = (x, y)$ il punto di intersezione fra r e C, diverso da P.

Si mostri che t è la tangente dell'angolo $\widehat{QPR}$, e che quest'angolo è la metà dell'angolo $\widehat{ZOR}$.

Si scrivano x, y in funzione di t.

Esercizio 9.13 (Facoltativo). Si determinino le terne (x, y, z) di interi tali che $x^2 + y^2 = 2z^2$.

Esercizio 9.14. Siano $a, b \in \mathbf{Z}$. Si mostri che esistono $u, v \in \mathbf{Z}$ tali che

$$\begin{cases} a = u + v \\ b = u - v \end{cases}$$

se e solo se a e b hanno la stessa parità, cioè sono entrambi pari o entrambi dispari. In questo caso, si trovi anche una formula per u, v in funzione di a, b.

Esercizio 9.15.

(1) Si dica quali numeri primi di $\mathbf{Z}$ sono somma di due quadrati, e perché.
(2) Si dica quali sono i numeri primi in $\mathbf{Z}[i]$, e perché.
(3) Si scrivano come prodotto di primi in $\mathbf{Z}[i]$ i numeri

$$6, 10, 15, 374, 406, 1271.$$