MA3202: Algebra II

Satvik Saha, 19MS154 February 27, 2022

Exercise 1 Find all units in $\mathbb{Z}[i]$.

Solution Let $u, v \in Z[i]$ be units with $uv = 1$. Further let $u = a + ib$, $v = c + id$. Then, taking square norms gives

$$(a^2 + b^2)(c^2 + d^2) = 1,$$

from which we must have $a^2 + b^2 = c^2 + d^2 = 1$. This forces $u = \pm 1, \pm i$, which are the only units in $\mathbb{Z}[i]$.

Exercise 2 Prove that $\mathbb{Z}[i]$ is a Euclidean domain.

Solution It can be shown that the map $d\colon \mathbb{Z}[i] \setminus \{0\} \to \mathbb{Z}_{n \geq 0}$, $a + ib \mapsto a^2 + b^2$ is an algorithm map. Let $x = a + ib$, $y = c + id$, whence $d(xy) = d(x)d(y)$ immediately gives $d(x) \leq d(xy)$. Next, note that

$$\frac{x}{y} = \frac{a + ib}{c + id} = \frac{(a + ib)(c - id)}{c^2 + d^2} = \frac{(ac + bd) + i(bc - ad)}{c^2 + d^2}.$$

Thus, we can set $x = (r + is)y$, where r, s are rational. Furthermore, we can choose integers m, n such that

$$|r - m| \leq \frac{1}{2}, \qquad |s - n| \leq \frac{1}{2}.$$

Set $q = m + in \in \mathbb{Z}[i]$,

$$w = \frac{x}{y} - q = (r - m) + i(s - n), \qquad wy = x - qy \in \mathbb{Z}[i].$$

Thus, we claim that $x = qy + wy$, with $d(wy) < d(y)$. Indeed,

$$d(w) = (r - m)^2 + (s - n)^2 \leq \frac{1}{2^2} + \frac{1}{2^2} = \frac{1}{2},$$

so

$$d(wy) = d(w)d(y) \leq \frac{1}{2}d(y) < d(y).$$

Exercise 3 Show that if F is a field, then $F[X]$ is a Euclidean domain.

Solution The map which sends a polynomial to its degree is a Euclidean domain. Note that $\deg(pq) = \deg(p) + \deg(q)$, so $\deg(p) \leq \deg(pq)$.

Exercise 4 Is 5 a prime element in $\mathbb{Z}[\sqrt{2}]$?

Solution Suppose that $5 \mid xy$, with $x = a + b\sqrt{2}$, $y = c + d\sqrt{2}$. Note that $xy = (ac + 2bd) + (ad + bc)\sqrt{2}$. Define $d(x) = |a^2 - 2b^2|$, whence

$$d(xy) = |(ac + 2bd)^2 - 2(ad + bc)^2| = a^2c^2 + 4b^2d^2 - 2a^2d^2 - 2b^2c^2,$$

and $d(x)d(y) = a^2c^2 - 2a^2d^2 - 2b^2c^2 + 4b^2d^2$. In other words, $d(x)d(y) = d(xy)$. Thus, we must have $5^2 \mid |(a^2 - 2b^2)(c^2 - 2d^2)|$.

Without loss of generality, we have $5 \mid a^2 - 2b^2$. Now, $a, b \equiv 0, \pm 1, \pm 2 \pmod 5$, hence $a^2 \equiv 0, \pm 1 \pmod 5$. As a result, $a^2 - 2b^2 \equiv 0 \pmod 5$ only when $a, b \equiv 0 \pmod 5$. Thus, $5 \mid a + b\sqrt{2} = x$. This proves that 5 is prime in $\mathbb{Z}[\sqrt{2}]$.

Exercise 5 Show that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain.

Solution We have already shown that the map defined by $d(a+b\sqrt{2}) = |a^2 - 2b^2|$ is multiplicative, hence $d(x) \leq d(xy)$. Now, let $x = a+b\sqrt{2}$, $y = c+d\sqrt{2}$. Then note that

$$\frac{x}{y} = \frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{(a+b\sqrt{2})(c-d\sqrt{2})}{c^2-2d^2} = \frac{(ac-2bd)+(bc-ad)\sqrt{2}}{c^2-2d^2}.$$

Thus, we can set $x = (r+s\sqrt{2})y$, where r, s are rational. Furthermore, we can choose integers m, n such that

$$|r-m| \leq \frac{1}{2}, \qquad |s-n| \leq \frac{1}{2}.$$

Set $q = m + n\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$,

$$w = \frac{x}{y} - q = (r-m) + (s-n)\sqrt{2}, \qquad wy = x - qy \in \mathbb{Z}[\sqrt{2}].$$

Thus, we claim that $x = qy + wy$, with $d(wy) < d(y)$. Indeed,

$$d(w) = |(r-m)^2 - 2(s-n)^2| \leq |r-m|^2 + 2|s-n|^2 \leq \frac{1}{2^2} + 2\cdot\frac{1}{2^2} = \frac{3}{4},$$

so

$$d(wy) = d(w)d(y) \leq \frac{3}{4}d(y) < d(y).$$

Exercise 6 Is a subring of a Euclidean domain a Euclidean domain? What about principal ideal domains?

Solution Note that $\mathbb{Z}[X]$ is not a principal ideal domain, since $(X, 2)$ is an ideal but not principal. Thus, $\mathbb{Z}[X]$ cannot be a Euclidean domain. However, $\mathbb{R}[X]$ is a Euclidean domain since $\mathbb{R}$ is a field, and $\mathbb{Z}[X] \subset \mathbb{R}[X]$ is a subring.

The same shows that a subring of a principal ideal domain need not be a principal ideal domain.

Exercise 7 Let R be a principal ideal domain, and P be a prime ideal of R. Show that R/P is a principal ideal domain. Is this true for Euclidean domains?

Solution Note that this is trivial if $P = \{0\}$. Otherwise, since R is a principal ideal domain and P is a prime ideal, P is a maximal ideal. Thus, R/P is a field, hence a simple ring with only two ideals (0) and (1), hence a principal ideal domain.

Note that this R/P is also a Euclidean domain, since it is a field with the trivial algorithm map $x \mapsto 1$.

Exercise 8 Let R be a Euclidean domain, and $x \in R$. Then, show that x is a unit if and only if $d(x) = d(1)$.

Solution First suppose that x is a unit, with $xy = 1$. Then, $d(x) \leq d(xy) = d(1)$. On the other hand, $d(1) \leq d(1x) = d(x)$, hence $d(x) = d(1)$.

Next, suppose that $d(x) = d(1)$. Write $1 = qx + r$; if $r = 0$, then x is a unit. Otherwise, we demand $d(r) < d(1)$, but this is impossible since $d(1) \leq d(1r) = d(r)$.

Exercise 9 Let R be a factorisation domain in which any two elements have a gcd. Show that R is a unique factorisation domain.

Solution We need only show that every irreducible element is a prime. Let $p \in R$ be irreducible, and $p \mid ab$. Also suppose that $p \nmid a$; we claim that $p \mid b$. Note that $\gcd(ab, pb) = \gcd(a, p)b$, but $\gcd(a, p) = 1$. Thus, $p \mid ab, pb$ shows that $p \mid \gcd(ab, pb)$ so $p \mid b$.

Exercise 10 Let R be a principal ideal domain, S be an integral domain, and $\varphi\colon R \to S$ be a surjective ring homomorphism which is not one-one. Show that S is a field.

Solution Set $P = \ker\varphi$. Then, we have $R/P \cong S$ which is an integral domain, hence P is a prime ideal. Now $P = 0$ would imply that φ is an isomorphism. Thus, $P \neq 0$, hence P is maximal in R, hence $R/P \cong S$ is a field.