Partial HW9 Solutions

3.9 Find all the units in the commutative ring $\mathcal{F}(\mathbb{R})$ defined in Example 3.11(i).
Solution. We claim that f is a unit if and only if $f(r) \neq 0$ for every $r \in \mathbb{R}$. If f is a unit, there is $g \in \mathcal{F}(\mathbb{R})$ with $fg = 1$; that is, $f(r)g(r) = 1$ for all $r \in \mathbb{R}$, and so $f(r) \neq 0$ for all $r \in \mathbb{R}$.

Conversely, if $f(r) \neq 0$ for all $r \in \mathbb{R}$, define $g \in \mathcal{F}(\mathbb{R})$ by $g(r) = 1/f(r)$; then $fg = 1$ and f is a unit.

3.13 Prove that the only subring of $\mathbb{Z}$ is $\mathbb{Z}$ itself.
Solution. Every subring R of $\mathbb{Z}$ contains 1, hence $1+1$, $1+1+1$, etc, so that R contains all positive integers (one needs induction), and finally, R contains the additive inverses of these, i.e., all negative integers, as well.

3.15 **(i)** Is $R = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ a domain?
Solution. It suffices to show that R contains 1 and is closed under addition and multiplication. Each of these is routine: for example,

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}.$$

(ii) Is $R = \{\frac{1}{2}(a + b\sqrt{2}) : a, b \in \mathbb{Z}\}$ a domain?
Solution. R is not a subring of $\mathbb{R}$, hence is not a domain, for $(\frac{1}{2})^2 = \frac{1}{4} \notin R$.

(iii) Using the fact that $\alpha = \frac{1}{2}(1+\sqrt{-19})$ is a root of $x^2 - x + 5$, prove that $R = \{a + b\alpha : a, b \in \mathbb{Z}\}$ is a domain.
Solution. It is clear that R contains 1, and one shows easily that if $a, a' \in A$ and $b, b' \in B$, then R contains $a - a'$, $b - b'$, $a - b$, and aa'. Write $a = \alpha + \alpha'\sqrt{5}$, $b = \frac{1}{2}(\beta + \beta')\sqrt{5}$, and $b' = \frac{1}{2}(\gamma + \gamma')\sqrt{5}$. It is easy to see that $ab \in A$ if α and α' have the same parity, while $ab \in B$ otherwise; in either case, $ab \in R$. Finally, write

$$\begin{aligned} bb' &= \left[\tfrac{1}{2}(\beta + \beta')\sqrt{5}\right]\left[\tfrac{1}{2}(\gamma + \gamma')\sqrt{5}\right] \\ &= \tfrac{1}{4}\left[(\beta\gamma + 5\beta'\gamma') + \sqrt{5}(\beta\gamma' + \beta'\gamma)\right]. \end{aligned}$$

Expand and substitute $\beta = 2p + 1$, $\beta' = 2p' + 1$, $\gamma = 2q + 1$, and $\gamma' = 2q' + 1$ (for β, β', γ, and γ' are odd). After collecting terms, one sees that both the constant term and the coefficient of

$\sqrt{5}$ are even; moreover, the quotients obtained after dividing each by 2 have the same parity. It follows that $bb' \in R$.

This example can be generalized by replacing 5 by any integer D with $D \equiv 1 \bmod 4$; the ring R is a special case of the ring of integers in a quadratic number field of the form $\mathbb{Q}(\sqrt{D})$.

3.20 Prove that every domain R with a finite number of elements must be a field.
Solution. Let $R^\times$ denote the set of nonzero elements of R. The cancellation law can be restated: for each $r \in R^\times$, the function $\mu_r : R^\times \to R^\times$, defined by $\mu_r : x \mapsto rx$, is an injection $R^\times \to R^\times$. Since $R^\times$ is finite, Exercise 2.13 shows that every μ_r must also be a surjection. Hence, there is $s \in R^\times$ with $1 = \mu_r(s) = rs$, and so r has an inverse.

3.21 Find all the units in the ring $\mathbb{Z}[i]$ of Gaussian integers.
Solution. If $z = a + ib$ has an inverse, then there is $u \in \mathbb{Z}[i]$ with $zu = 1$. By Corollary 1.23, $1 = |zu| = |z||u|$. Here, both $|z|$ and $|u|$ are integers, so that $|z| = \pm 1$. But $|z| = a^2 + b^2$, where $a, b \in \mathbb{Z}$. Therefore, either $a = \pm 1$ and $b = 0$, or $a = 0$ and $b = \pm 1$. That is, there are only four units: $1, -1, i$, and $-i$.

3.23 **(i)** Show that $F = \{a + bi : a, b \in \mathbb{Q}\}$ is a field.
Solution. It is straightforward to check that F is a subring of $\mathbb{C}$, and so it is a commutative ring; it is a field because the inverse of $a + bi$ is $r^{-1}(a - bi) \in F$, where $r = a^2 + b^2$.

(ii) Show that every $u \in F$ has a factorization $u = \alpha\beta^{-1}$, where $\alpha, \beta \in \mathbb{Z}[i]$. (See Exercise 3.50.)
Solution. Write

$$a + bi = (p/q) + (r/s)i = (ps + qri)(qs)^{-1},$$

where $p, q, r, s \in \mathbb{Z}$.