Problem §1 (3.5) For any integer $D \in \mathbb{Z}$ that is not the square of an integer, we can form a ring

$$\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}.$$

If $D > 0$, then $\mathbb{Z}[\sqrt{D}]$ is a subring of $\mathbb{R}$, while if $D < 0$, then in any case it is a subring of $\mathbb{C}$.

(a) Let $\alpha = 2 + 3\sqrt{5}$, $\beta = 1 - 2\sqrt{5}$ be elements of $\mathbb{Z}[\sqrt{5}]$. Compute the quantitties

$$\alpha + \beta, \alpha \cdot \beta, \alpha^2.$$

(b) Prove that the map

$$\phi : \mathbb{Z}[\sqrt{D}] \longrightarrow \mathbb{Z}[\sqrt{D}],\ \phi(a + b\sqrt{D}) = a - b\sqrt{D}$$

is a ring homomorphism (where $\overline{\alpha}$ denotes the conjugate of α).

(c) With notation as in (b), prove that

$$\alpha \cdot \overline{\alpha} \in \mathbb{Z} \text{ for every } \alpha \in \mathbb{Z}[\sqrt{D}].$$

Solution:

(a) $\alpha = 2 + 3\sqrt{5},\ \beta = 1 - 2\sqrt{5},\ \alpha, \beta \in \mathbb{Z}[\sqrt{5}]$.

$$\alpha + \beta = 3 + \sqrt{5}$$
$$\alpha \cdot \beta = (2 + 3\sqrt{5})(1 - 2\sqrt{5}) = 2 - 4\sqrt{5} + 3\sqrt{5} - 6 \cdot 5 = -28 - \sqrt{5}$$
$$\alpha^2 = (2 + 3\sqrt{5})^2 = 4 + 12\sqrt{5} + 45 = 49 + 12\sqrt{5}.$$

(b) $\phi : \mathbb{Z}[\sqrt{5}] \to \mathbb{Z}[\sqrt{5}]$, $\phi(\alpha) = \overline{\alpha}$.

- First, observe that $1_{\mathbb{Z}[\sqrt{D}]} = 1 + 0\sqrt{D} = 1$. Then $\phi(1_{\mathbb{Z}[\sqrt{D}]}) = 1 - 0\sqrt{D} = 1_{\mathbb{Z}[\sqrt{D}]}$. Hence $\phi(1_{\mathbb{Z}[\sqrt{D}]}) = 1_{\mathbb{Z}[\sqrt{D}]}$.
- Let $\alpha = a + b\sqrt{D},\ \beta = c + d\sqrt{D}$. Then $\alpha + \beta = (a + c) + (b + d)\sqrt{D}$, so

  $$\phi(\alpha + \beta) = (a + c) - (b + d)\sqrt{D} = a - b\sqrt{D} + c - d\sqrt{D} = \phi(\alpha) + \phi(\beta)$$

  by additive associativity, so $\phi(\alpha + \beta) = \phi(\alpha) + \phi(\beta)$.
- Let α, β as before. Then $\alpha \cdot \beta = ac - ad\sqrt{D} - bc\sqrt{D} + bdD = (ac + bdD) + (ad + bc)\sqrt{D}$, and $\phi(\alpha) = a - b\sqrt{D},\ \phi(\beta) = c - d\sqrt{D}$. Then

  $$\phi(\alpha \cdot \beta) = ac + bdD - (ad + bc)\sqrt{D} \quad \phi(\alpha) \cdot \phi(\beta) = ac - ad\sqrt{D} - bc\sqrt{D} + bdD = (ac + bdD) - (ad + bc)\sqrt{D}.$$

  Hence $\phi(\alpha \cdot \beta) = \phi(\alpha) \cdot \phi(\beta)$, and so ϕ is a ring homomorphism.

(c) $\alpha = a + b\sqrt{D},\ \overline{\alpha} = \phi(\alpha) \cdot \phi(\beta)$. Then

$$\alpha \cdot \overline{\alpha} = a - ab\sqrt{D} + ab\sqrt{D} - b^2 D = a - b^2 D \in \mathbb{Z}.$$

(All of $a, b, D \in \mathbb{Z}$ and $\mathbb{Z}$ is closed under addition).

Problem §2 (3.15) For a quaternion $\alpha = a + bi + cj + dk \in \mathbb{H}$, we let $\overline{\alpha} = a - bi - cj - dk$.

(a) Prove that $\alpha\overline{\alpha} \in \mathbb{R}$.

(b) Prove that $\alpha\overline{\alpha} = 0$ if and only if $\alpha = 0$.

(c) Suppose that $\alpha, \beta \in \mathbb{H}$ and that $\alpha\beta = 0$. Prove that either $\alpha = 0$ or $\beta = 0$.

(d) Let $\alpha, \beta \in \mathbb{H}$. Prove that

$$\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta} \text{ and } \overline{\alpha \cdot \beta} = \overline{\beta} \cdot \overline{\alpha}.$$

(e) Let $\alpha \in \mathbb{H}$ with $\alpha \neq 0$. Prove that there is a $\beta \in \mathbb{H}$ satisfying $\alpha\beta = \beta\alpha = 1$, i.e. every non-zero element of $\mathbb{H}$ has a multiplicative inverse.

Solution:

(a) For $\alpha = a + bi + cj + dk \in \mathbb{H}$, $a, b, c, d \in \mathbb{R}$, we have

$$\alpha\overline{\alpha} = (a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2 \in \mathbb{R}.$$

(b) Suppose $\alpha\overline{\alpha} = 0$. Then $a^2 + b^2 + c^2 + d^2 = 0$. Since $x^2 \geq 0$ for all $x \in \mathbb{R}$, with $x^2 = 0$ only when $x = 0$, then $a = b = c = d = 0$, and so $\alpha = 0$.

Now, suppose $\alpha = 0$. Then $a + bi + cj + dk = 0$, and so $a = b = c = d = 0$ (by definition, if any of $a, b, c, d \neq 0$, one can clearly see $\alpha \neq 0$, since i, j, k dont cancel each other individually, i.e. $ai + yj = 0$ only when $x, y = 0$). Hence $\alpha\overline{\alpha} = 0^2 + 0^2 + 0^2 + 0^2 = 0$.

(c) Suppose $\alpha, \beta \in \mathbb{H}$, with $\alpha = a + bi + cj + dk$, $\beta = w + xi + yj + zk$ and $\alpha \cdot \beta = 0$. First, we note that $\alpha\overline{\alpha} = \overline{\alpha}\alpha = a^2 = b^2 + c^2 + d^2$. Then

$$\begin{aligned} \alpha\beta &= 0 \\ \overline{\alpha}\alpha\beta &= \overline{\alpha} \cdot 0 \\ (a^2 + b^2 + c^2 + d^2)\beta\overline{\beta} &= 0 \cdot \overline{\beta} \\ (a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2) &= 0. \end{aligned}$$

Since $x^2 \geq 0$ for any $x \in \mathbb{R}$, and $x^2 = 0$ only when $x = 0$, we see that either $a = b = c = d = 0$ or $w = x = y = z = 0$.

(d) Let $\alpha, \beta \in \mathbb{H}$ as before. Then $\alpha + \beta = (a + w) + (b + x)i + (c + y)j + (d + z)k$. We have

$$\overline{\alpha + \beta} = (a + w) - (b + x)i - (c + y)j - (d + z)k,$$

and

$$\overline{\alpha} + \overline{\beta} = a - bi - cj - dk + w - xi - yj - zk = \overline{\alpha + \beta} = (a + w) - (b + x)i - (c + y)j - (d + z)k.$$

Thus $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$.

$\overline{\alpha \cdot \beta} = (aw - bx - cy - dz) - (ax + bw + cz - dy)i - (ay - bz + cw + dx)j - (az + by - cx + dw)k$, and $\overline{\beta} \cdot \overline{\alpha} = (aw - bx - cy - dz) - (ax + bw + cz - dy)i - (ay - bz + cw + dx)j - (az + by - cx + dw)k$, so $\overline{\alpha \cdot \beta} = \overline{\beta} \cdot \overline{\alpha}$.

(e) Note that $\alpha\overline{\alpha} = a^2 + b^2 + c^2 + d^2$. For $\alpha\overline{\alpha} = 1$, we need $\frac{\alpha\overline{\alpha}}{a^2+b^2+c^2+d^2}$. Thus, let $\beta = \frac{\overline{\alpha}}{a^2+b^2+c^2+d^2} \in \mathbb{H}$ (since $\alpha \neq 0$, not all a, b, c, d are zero). Then $\alpha\beta = \frac{\alpha\overline{\alpha}}{a^2+b^2+c^2+d^2} = \frac{a^2+b^2+c^2+d^2}{a^2+b^2+c^2+d^2} = 1$. Hence any non-zero α has a multiplicative inverse.

Problem §3

- (3.17) Let R be a field. Prove that R is an integral domain.
- (3.18) Let R be a ring. Prove that R is an integral domain if and only if R has the cancellation property.

Solution:

- Let R be a field. Then R is a commutative ring, and for any $a \in R$, $a \neq 0$, there exists a $b \in R$ such that $ab = 1$.

Let $a \in R$, $a \neq 0$, and suppose for some $b \in R$, $ab = 0$. Since R is a field, there exists some $c \in R$ such that $ac = ca = 1$. Then

$$\begin{aligned} ab &= 0 \\ cab &= c \cdot 0 \\ 1 \cdot b &= 0 \\ b &= 0. \end{aligned}$$

Thus for any non-zero $a \in R$, if, for some $b \in R$, $ab = 0$, then $b = 0$; in other words, R has no zero divisors, and thus is an integral domain.

- Let R be a ring, and suppose R has the cancellation property; that is, for every $a, b, c \in R$, if $ab = ac$ and $a \neq 0$, then $b = c$. Let $a, b \in R$ such that $a \neq 0$ and $ab = 0$. Thus $ab = 0$ implies

$$ab = a \cdot 0,$$

and by the cancellation property, $b = 0$. Thus if $a, b \in R$, $a \neq 0$, and $ab = 0$, then $b = 0$. Hence R has no zero divisors, and so R is an integral domain.

Conversely, suppose R is an integral domain. Then for any $ab = 0$, $a \neq 0$, then $b = 0$. Let $a, b, c \in R$ with $a \neq 0$, and suppose $ab = ac$. Then

$$ab - ac = a(b - c) = 0.$$

Since R is an integral domain and $a \neq 0$, $b - c$ must be 0. Thus $b = c$, and so R has the cancellation property.

Problem §4 (3.23 a-c) Let R be a ring, and $a \in R$. a is **nilpotent** if $a^n = 0$ for some $n \geq 1$. a is **unipotent** if $a - 1$ is nilpotent (e.g. $(a-1)^n = 0$ for some $n \geq 1$). a is **idempotent** if $a^2 = a$.

(a) If R is an integral domain, describe all nil/uni/idempotent elements of R. How many are there of each?

(b) Let $p \in \mathbb{Z}$ and let $k \geq 1$. Describe all the nilpotent elements of $\mathbb{Z}/p^k\mathbb{Z}$. In particular, how many are there?

(c) Let $a \in R$ be unipotent. Prove that a is a unit, i.e. it has a multiplicative inverse.

Solution:

(a) Let a ring R be an integral domain.

- **Nilpotent elements**: Clearly, $a = 0$ is nilpotent, so suppose $a \neq 0$. Then $a(a^{n-1}) = 0$ implies $a^{n-1} = 0$ by property of the integral domain. Repeating until $a \cdot a = 0$, if $a \neq 0$, then $a = 0$, a contradiction. Hence if a is nilpotent, $a = 0$.
- **Unipotent elements**: Clearly, $a = 1$ is unipotent (since $a - 1 = 0$ is nilpotent), so suppose $a \neq 1$. Like before, since R is an integral domain, $(a-1)(a-1)^{n-1} = 0$ implies $(a-1)^{n-1} = 0$, and repeating this process until $(a-1)(a-1) = 0$, we get $a - 1 = 0$, or $a = 1$, a contradiction. Hence if a is unipotent, then $a = 1$.
- **Idempotent elements**: Clearly, 0 and 1 are idempotent elements. If $a^2 = a$, then $a^2 - a = a(a-1) = 0$. If $a \neq 0$, then $a - 1 = 0$, so $a = 1$. If $a - 1 \neq 0$, then $a = 0$. Hence 0 and 1 are the only idempotent elements.

(b) Suppose $p \in \mathbb{Z}$ is a prime number, and $k \geq 1$. Consider $\mathbb{Z}/pk\mathbb{Z}$. For any multiple of p in $\mathbb{Z}/p^k\mathbb{Z}$ (e.g. $ap \in \mathbb{Z}/p^k\mathbb{Z}$ for some $a < p^{k-1}$), we have that $(ap)^k = a^k p^k \equiv 0 \mod p^k$; thus any multiple of p in $\mathbb{Z}/p^k\mathbb{Z}$ is nilpotent. Additionally, 0 is trivially nilpotent; thus we have p^{k-1} nilpotent elements, at least.

Now, we make an observation: given $a, p \in \mathbb{Z}$ and p prime, if p^k divides a, then p divides a. Equivalently, if $a \equiv 0 \mod p^k$, then $a \equiv 0 \mod p$ (since p^k divides a, any $p, p^2, p^3, \ldots, p^{k-1}$ divides a). Taking its contrapositive, if p does not divide a, then p^k does not divide a.

For any $a \in \mathbb{Z}/p^k\mathbb{Z}$ where a is not a multiple of p, we have that $a = np + b \equiv b \mod p$ for some $b, n \in \mathbb{Z}_{\geq 0},\ 0 \leq b < p$; then $b^{p-1} \equiv 1 \mod p$ by Fermat's Little Theorem. Clearly, $b^s \not\equiv 0 \mod p$ for any $0 \leq s < p$ (since otherwise we would get $b^{p-1} \equiv b^{s+i} \equiv 0 \mod p$ for some $i \in \mathbb{Z}$); and for any $i \in \mathbb{Z},\ i \geq p-1$, for some $q, r \in \mathbb{Z},\ 0 \leq r < p-1$, any $b^i = b^{q(p-1)+r} \equiv b^r \not\equiv 0 \mod p$ (since any $a^r \not\equiv 0 \mod p$ for $0 \leq s < p$ from before). Thus $a^m \not\equiv 0 \mod p$ for any $m \geq 1$, and so $a^m \not\equiv 0 \mod p^k$. Thus $a \in \mathbb{Z}/p^k\mathbb{Z}$ is nilpotent only if a is a multiple of p in $\mathbb{Z}/p^k\mathbb{Z}$, and so $\mathbb{Z}/p^k\mathbb{Z}$ has p^{k-1} nilpotent elements.

(c) Suppose $a \in R$ is unipotent; then for some $n \in N$, $(a-1)^n = 0$. By the Binomial Theorem, we have

$$a^n + \binom{n}{n-1}(-1)a^{n-1} + \ldots + \binom{n}{1}(-1)^{n-1}a + (-1)^n = a\left(a^{n-1} + \binom{n}{n-1}(-1)a^{n-1} + \ldots + \binom{n}{1}(-1)^{n-1}\right) + (-1)^n = 0,$$

so we have

$$a(a^{n-1} + \binom{n}{n-1}(-1)a^{n-1} + \ldots + \binom{n}{1}(-1)^{n-1}) = (-1)^{n+1}.$$

Let $b = a^{n-1} + \binom{n}{n-1}(-1)a^{n-1} + \ldots + \binom{n}{1}(-1)^{n-1}$. If n even, then $a(-b) = -1$, so $ab = 1$; and if n odd, then $ab = 1$. In either case, $\pm b \in R$ (by closure of ring addition and multiplication), so a is a unit.

Problem §5 (3.25)

(a) Compute the unit group $\mathbb{Z}^*$.

(b) Compute the unit group $\mathbb{Q}^*$.

(c) Compute the unit group $\mathbb{Z}[i]^*$.

(d) Consider the ring $\mathbb{Z}[\sqrt{2}]$. Prove that $1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]^*$. Prove that the powers of $1 + \sqrt{2}$, or $(1 + \sqrt{2})^n$ for $n = 1, 2, \ldots$ are all different, and use the fact to deduce that $\mathbb{Z}[\sqrt{2}]^*$ has infinitely many elements.

(e) Prove that $\mathbb{R}[x]^* = \mathbb{R}^*$.

(f) Prove that $1 + 2x$ is a unit in the ring $\mathbb{Z}/4\mathbb{Z}[x]$.

Solution:

(a) $\mathbb{Z}^* = \{\pm 1\}$, since $1 \cdot 1 = -1 \cdot -1 = 1$, and for any $|x| > 1$, $xy \neq 1$ for any $y \in \mathbb{Z}$ (since $\frac{1}{x} \notin \mathbb{Z}$ if $|x| > 1$).

(b) $\mathbb{Q}^* = \{a \in \mathbb{Q} \mid a \neq 0\}$, since for any non-zero $a \in \mathbb{Q}$, we can take $a \cdot \frac{1}{a} = 1$.

(c) Let $\alpha, \beta \in \mathbb{Z}[i]$, $\alpha = a + bi,\ \beta = c + di$. Then $\alpha\beta = (a + bi)(c + di) = (ac - bd) + (ad + bc)i$. In order for $\alpha\beta = 1$, we need both $ac - bd = 1$ and $ad + bc = 0$. Isolating for $d = -\frac{bc}{a}$ and plugging in, we get

$$ac + \frac{b^2c}{a} = \frac{c}{a}(a^2 + b^2) = 1,$$

and so $c = \frac{a}{a^2+b^2}$. Plugging c into $ad + bc = 0$, we get

$$ad + \frac{ab}{a^2 + b^2} = 0,$$

and so $d = -\frac{b}{a^2+b^2}$. Thus $\beta = \alpha^{-1} = (\frac{a}{a^2+b^2}) - (\frac{b}{a^2+b^2})i$; but since $\frac{a}{a^2+b^2}, \frac{b}{a^2+b^2} \in \mathbb{Z}$, we must have either $a = \pm 1, b = 0$ or $a = 0, b = \pm 1$ (since $a^2 \geq a$, and $k(a^2+b^2) = |a|$ only when $k = 1, a = \pm 1, b = 0$). Thus $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.

(d) Consider $(1+\sqrt{2})(a+b\sqrt{2}) = (a+2b)+(a+b)\sqrt{2}$. For $a=-1, b=1$, we get $(-1+2)(-1+1)\sqrt{2} = 1$; thus $(1+\sqrt{2})(-1+\sqrt{2}) = 1$, and so $1+\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^*$.

Now, we prove a lemma:

Lemma 1. *For any $n \in \mathbb{N}$, $(1+\sqrt{2})^n = a+b\sqrt{2}$ for some $a, b \in \mathbb{N}$. Moreover, the sequence $s_n = (1+\sqrt{2})^n$ is strictly increasing.*

Proof. We use induction: clearly, $a = b = 1 \in \mathbb{N}$, so the base case holds.

Now, suppose $(1+\sqrt{2})^n = a+b\sqrt{2}$ for some $a, b \in \mathbb{N}$. Then $(1+\sqrt{2})^n(1+\sqrt{2}) = (a+b\sqrt{2})(1+\sqrt{2}) = (a+2b)+(a+b)\sqrt{2}$; and since $a, b \in \mathbb{N}$, we have $a+2b, a+b \in \mathbb{N}$ as well. Hence for any $n \in \mathbb{N}$, if $(1+\sqrt{2})^n = a+b\sqrt{2}$ for some positive $a, b \in \mathbb{N}$, we have $(1+\sqrt{2})^{n+1} = a' + b'\sqrt{2}$, $a, b \in \mathbb{N}$ as well; and since the base case holds, we have that $(1+\sqrt{2})^n = a+b\sqrt{2}$, $a, b \in \mathbb{N}$ for any $n \in \mathbb{N}$.

From this, we can also clearly see that s_n is strictly increasing: for any $n \in \mathbb{N}$, $(1+\sqrt{2})^n = a+b\sqrt{2} < (a+2b)+(a+b)\sqrt{2} = (1+\sqrt{2})^{n+1}$, so $s_n < s_{n+1}$, as required[1]. □

Now, since $(1+\sqrt{2})^n < (1+\sqrt{2})^{n+1}$, it naturally follows that for any $j, k \in \mathbb{N}$, $j \neq k$ (supposing without loss of generality that $j < k$), $(1+\sqrt{2})^j \neq (1+\sqrt{2})^k$, and so all $(1+\sqrt{2})^n$ are different for $n \in \mathbb{N}$ (in other words, there are infinitely many $\alpha \in \mathbb{Z}[\sqrt{2}]$). Moreover, for any $(1+\sqrt{2})^n$, we have $(1+\sqrt{2})^n(-1+\sqrt{2})^n = 1$, since $(1+\sqrt{2})(-1+\sqrt{2}) = 1$. Thus any $(1+\sqrt{2})^n \in \mathbb{Z}[\sqrt{2}]^*$; and since there are infinitely many $(1+\sqrt{2})^n$, there are infinitely many elements in $\mathbb{Z}[\sqrt{2}]^*$.

(e) Clearly, $\mathbb{R}^* \subseteq \mathbb{R}[x]^*$ (since $\mathbb{R}$ is a field, and we can choose $a + 0x + 0x^2 + \ldots \in \mathbb{R}[x]^*$ given an $a \in \mathbb{R}^*$). Suppose $\alpha, \ \beta \in \mathbb{R}[x]$ where $\alpha = a_0 + a_1x + \ldots + a_nx^n$, $\beta = b_0 + b_1x + \ldots + b_mx^m$, and n, m respectively are the highest powers of x with non-zero coefficients. In order for $\alpha\beta = c_0 + \ldots + c_{m+n}x^{m+n} = 1$, we need $a_0b_0 = 1$, and $c_i = 0$ for any $0 < i \leq m+n$. However, $a_nb_m \neq 0$ by definition, and so the highest power $c_{m+n}x^{m+n} = a_nb_mx^{m+n}$ has a non-zero coefficient; thus $a_0b_0 + \ldots + a_nb_mx^{m+n} \neq 1$ for any $m+n > 0$. It naturally follows that we need $m = n = 0$, and so $\alpha\beta = 1$ only when $\alpha = a_0$, $\beta = b_0$, $a_0b_0 = a_0 \cdot \frac{1}{a_0} = 1$. In other words, for any $\alpha \in \mathbb{R}[x]^*$, we have $\alpha \in \mathbb{R}^*$; thus $\mathbb{R}[x]^* \subseteq \mathbb{R}^*$, and so $\mathbb{R}^* = \mathbb{R}[x]^*$.

(f) Let $1+2x \in \mathbb{Z}/4\mathbb{Z}$. Then

$$(1+2x)(1+2x) = 1 + 4x + 4x^2 \equiv 1 + 0x + 0x^2 = 1.$$

Hence $1+2x \in (\mathbb{Z}/4\mathbb{Z})[x]^*$.

[1] Many thanks to MATH1010 and Tamarkin Assistant Professor Huy Quang Nguyen for his illuminating insights into sequences.