9. Let i be the complex number $\sqrt{-1}$. Show that the ring $\mathbf{Z}[i]$ is principal, and hence factorial. What are the units?

Proof. A Euclidean domain is an entire ring R for which there exists a "norm" $N : R \to \mathbf{Z}^+ \cup \{0\}$ such that, for all $a, d \in \mathbf{R}$ $(d \neq 0)$ there are some $q, r \in R$ such that $a = dq + r$ and either $N(r) < N(d)$ or $r = 0$. We will first show that any Euclidean domain is principal.

Let R be a Euclidean domain, and let $I \subseteq R$ be an ideal. Let $b \in I$ be such that $N(b) \leq N(x)$ for all $x \in I$. For any $a \in R$, we can write $a = dq + r$ where either $N(r) < N(d)$ or $r = 0$. But $r = a - dq \in I$, therefore $N(r) < N(d)$ would contradict the minimality of $N(d)$. So $r = a - dq = 0$, and so $a = dq$. Therefore, $I \subseteq (d)$. Clearly, $(d) \subseteq I$, thus $I = (d)$ is principal.

Next, observe that $\mathbf{Z}[i]$ is a Euclidean domain. Clearly, $\mathbf{Z}[i]$ is entire because $\mathbf{C}$ is entire. Equipped with the norm $N(a + bi) = a^2 + b^2$ (the square of the magnitude of $a + bi$), we can design a Euclidean algorithm as follows. First, note that every point in the complex plane has distance < 1 from some $\alpha \in \mathbf{Z}[i]$. This is because every point $z \in \mathbf{C}$ falls inside some square whose vertices are $(a + \frac{1}{2}) + (b + \frac{1}{2})i, (a + \frac{1}{2}) + (b - \frac{1}{2})i, (a - \frac{1}{2}) + (b + \frac{1}{2})i, (a - \frac{1}{2}) + (b - \frac{1}{2})i$ for some $a, b \in \mathbf{Z}$ (we include the boundary of the square), and any point on this square falls at most a distance $\frac{1}{\sqrt{2}}$ from $a + bi$.

Given some $a, d \in \mathbf{Z}[i]$, if $\frac{a}{d} \in \mathbf{Z}[i]$ we can simply take $q = \frac{a}{d}$ and $r = 0$. Otherwise, we can take q to be any point in $\mathbf{Z}[i]$ that has distance less than $\frac{1}{\sqrt{2}}$ from $\frac{a}{d}$. This means that $N(\frac{a}{d} - q) < 1$. Letting $r = a - dq$, we see that $N(r) = N(\frac{r}{d})N(d) < N(d)$ (the complex magnitude operator is known to distribute over multiplication). So $\mathbf{Z}[i]$ is a Euclidean domain, and thus is a principal entire ring. By Theorem 5.2, $\mathbf{Z}[i]$ is factorial.

Suppose $\alpha \in \mathbf{Z}[i]$ is a unit. Since N is multiplicative, we have $1 = N(1) = N(\alpha \cdot \alpha^{-1}) = N(\alpha)N(\alpha^{-1})$. But the codomain of N is nonnegative integers, so the only possibility is $N(\alpha) = N(\alpha^{-1}) = 1$. But the only choices of $a, b \in \mathbf{Z}$ such that $a^2 + b^2 = 1$ are where one of a and b is 0 and the other is 1. Thus, the units are $1, -1, i$, and $-i$. □

10. Let D be an integer ≥ 1, and let R be the set of all elements $a + b\sqrt{-D}$ with $a, b \in \mathbf{Z}$.

(a) Show that R is a ring.

Proof. As a subset of $\mathbf{C}$, R inherits a commutative addition and an associative multiplication, and the fact that addition distributes over multiplication. Since $0 = 0 + 0\sqrt{-D} \in R$ and $1 = 1 + 0\sqrt{-D} \in R$, R contains the additive and multiplicative identities. Given two elements $\alpha = a + b\sqrt{-D}$ and $\beta = c + d\sqrt{-D}$, we have $\alpha + \beta = (a + c) + (b + d)\sqrt{-D} \in R$ and $\alpha\beta = ac - bdD + (ad + bc)\sqrt{-D} \in R$, hence R is closed under addition and multiplication. □

(b) Using the fact that complex conjugation is an automorphism of $\mathbf{C}$, show that complex conjugation induces an automorphism of R.

Proof. Since conjugation is an automorphism on $\mathbf{C}$, its restriction to R gives an embedding of R into $\mathbf{C}$. All there is to show is that the image of R under conjugation is again R. This is obvious, since $\overline{a + b\sqrt{-D}} = a - b\sqrt{-D} \in R$ for all $a, b \in \mathbf{Z}$, and any $a + b\sqrt{-D} \in R$ is the image of $a - b\sqrt{-D} \in R$. □

(c) Show that if $D \geq 2$, then the only units in R are ± 1. Show that 3, $2 + \sqrt{-5}$, and $2 - \sqrt{-5}$ are irreducible elements in $\mathbf{Z}[\sqrt{-5}]$.

Proof. As shown in the proof of the previous exercise, $a + b\sqrt{-D}$ is a unit only if $N(a + \sqrt{-D}) = a^2 + b^2D = 1$. When $D \geq 2$, the only solutions occur when $b = 0$ and $a = \pm 1$.

For the next part, note also that α is actually a unit *if and only if* $N(\alpha) = 1$, since in this case we have $\alpha \cdot \overline{\alpha} = N(\alpha) = 1$, thus $\alpha^{-1} = \overline{\alpha} \in R$. Now, let $R = \mathbf{Z}[\sqrt{-5}]$ and suppose an element γ such that $N(\gamma) = 9$ factors as $\gamma = \alpha\beta$ for some $\alpha, \beta \in R$. Then $9 = N(\gamma) = N(\alpha)N(\beta)$. There are no integer solutions to $a^2 + 5b^2 = 3$, hence $N(\alpha)$ is either 1 or 9. In the first case, α is a unit; in the second, β is a unit. Therefore, γ is irreducible. Since 3, $2 + \sqrt{-5}$, and $2 - \sqrt{-5}$ all have norm 9, they are all irreducible. □

12. Let P be the set of positive integers and R the set of functions defined on P with values in a commutative ring K. Define the sum in R to be the ordinary addition of functions, and define the convolution product by the formula

$$(f * g)(m) = \sum_{xy=m} f(x)g(y),$$

where the sum is taken over all pairs (x, y) of positive integers such that $xy = m$.

(a) Show that R is a commutative ring, whose unit element is the function δ such that $\delta(1) = 1$ and $\delta(x) = 0$ if $x \neq 1$.

Proof. The addition in R is obviously associative and commutative, with the zero function as its identity. Convolution is obviously commutative - just switch $f(x)$ and $g(y)$ within the summation to obtain $g * f$ from $f * g$. To check that the multiplication is associative, let $m \in P$, $f, g, h \in R$, and observe that

$$\begin{aligned}
((f * g) * h)(m) &= \sum_{xy=m} (f * g)(x)h(y) \\
&= \sum_{xy=m} \left(\sum_{ab=x} f(a)g(b) \right) h(y) \\
&= \sum_{aby=m} f(a)g(b)h(y) \\
&= \sum_{xy=m} f(x) \left(\sum_{ab=y} g(a)h(b) \right) \\
&= (f * (g * h))(m)
\end{aligned}$$

Finally, for any $f \in R$ and $m \in P$ we have

$$(\delta * f)(m) = \sum_{xy=m} \delta(x)f(y) = \delta(1)f(m) = f(m)$$

so $\delta * f = f$. Since $*$ is commutative, $f * \delta = f$ as well. □

(b) A function f is said to be multiplicative if $f(mn) = f(m)f(n)$ whenever m and n are relatively prime. If f and g are multiplicative, show that $f * g$ is multiplicative.

Proof. Suppose f and g are multiplicative, and let $m, n \in P$ be relatively prime. Then

$$\begin{aligned}
(f * g)(mn) &= \sum_{xy=mn} f(x)g(y) && (1) \\
&= \sum_{x|mn} f(x)g\left(\frac{mn}{x}\right) && (2) \\
&= \sum_{a|m} \sum_{b|n} f(ab)g\left(\frac{mn}{ab}\right) && (3) \\
&= \sum_{a|m} \sum_{b|n} f(a)f(b)g\left(\frac{m}{a}\right) g\left(\frac{n}{b}\right) && (4) \\
&= \sum_{a|m} f(a)g\left(\frac{m}{a}\right) \sum_{b|n} f(b)g\left(\frac{n}{b}\right) && (5) \\
&= \sum_{xy=m} f(x)g(y) \sum_{xy=n} f(x)g(y) && (6) \\
&= (f * g)(m) \cdot (f * g)(n). && (7)
\end{aligned}$$

A brief explanation: the step from line (2) to line (3) happens because m and n are relatively prime, thus $\{x \mid mn\} = \{ab : a \mid m, b \mid n\}$. On line (4), we know that a and b are relatively prime because a is a divisor of m and b of n, so $f(ab) = f(a)f(b)$. The same logic applies to $\frac{m}{a}$ and $\frac{n}{b}$, so that g distributes over their product. Therefore, $f * g$ is multiplicative if f and g are. □

(c) Let μ be the Möbius function such that $\mu(1) = 1$, $\mu(p_1 \cdots p_r) = (-1)^r$ if $p_1, \ldots, p_r$ are distinct primes, and $\mu(m) = 0$ if m is divisible by p^2 for some prime p. Show that $\mu * \varphi_1 = \delta$, where φ_1 denotes the constant function having the value 1. The Möbius inversion formula of number theory is then nothing else but the relation $\mu * \varphi_1 * f = f$.

Proof. Clearly, φ_1 is multiplicative. We will show that μ is also multiplicative. Let m, n be relatively prime. Suppose, without loss of generality, that m is divisible by p^2 for some prime p. Then so is mn, hence $\mu(mn) = 0 = 0\mu(n) = \mu(m)\mu(n)$. So we may assume that $m = p_1 \cdots p_j$ and $n = q_1 \cdots q_k$ where the p_i are a distinct set of primes and the q_i are also a distinct set of primes. Since m and n are relatively prime, however, we know the entire set $p_1, \ldots, p_j, q_1 \ldots, q_k$ contains no duplicates. Therefore,

$$\mu(mn) = \mu(p_1 \cdots p_j q_1 \cdots q_k) = (-1)^{j+k} = (-1)^j(-1)^k = \mu(p_1 \cdots p_j)\mu(q_1 \cdots q_k) = \mu(m)\mu(n)$$

so μ is multiplicative, and thus so is $\mu * \varphi_1$.

Now,

$$(\mu * \varphi_1)(1) = \sum_{xy=1} \mu(1)\varphi_1(1) = 1 = \delta(1)$$

and for any prime p we have

$$(\mu * \varphi_1)(p) = \sum_{xy=p} \mu(x)\varphi_1(y) = \mu(1)\varphi_1(p) + \mu(p)\varphi_1(1) = 1 + (-1) = 0.$$

Therefore, if $m > 1$ then m is divisible by some prime p, thus

$$(\mu * \varphi_1)(m) = (\mu * \varphi_1)(p)(\mu * \varphi_1)\left(\frac{m}{p}\right) = 0 \cdot (\mu * \varphi_1)\left(\frac{m}{p}\right) = 0 = \delta(m).$$

So $\mu * \varphi_1 = \delta$.

In this language, the Möbius inversion formula simply states, "For any $f, g \in R$, $f = g * \varphi_1$ if and only if $g = f * \mu$." This is equivalent to saying, "For any $f \in R$, $f = (f * \mu) * \varphi_1$." But since $*$ is commutative and associative, this reduces to $\mu * \varphi_1 * f = f$. But we have just shown that $\mu * \varphi = \delta$ is the identity, which proves the Möbius inversion formula. □

1. Suppose that $1 \neq 0$ in A. Let S be a multiplicative subset of A not containing 0. Let $\mathfrak{p}$ be a maximal element in the set of ideals of A whose intersection with S is empty. Show that $\mathfrak{p}$ is prime.

Proof. Suppose for some $x, y \in A$ that $xy \in \mathfrak{p}$. Suppose, for a contradiction, that neither of x and y are in $\mathfrak{p}$. Then $\mathfrak{p} \subsetneq \mathfrak{p} + (x)$ and $\mathfrak{p} \subsetneq \mathfrak{p} + (y)$, therefore $\mathfrak{p} + (x) \cap S \neq \emptyset$ and $\mathfrak{p} + (y) \cap S \neq \emptyset$. Thus there are some elements $\alpha = p + ax \in \mathfrak{p} + (x)$ and $\beta = q + by \in \mathfrak{p} + (y)$. $\alpha\beta \in S$ because S is multiplicative, but we also have

$$\alpha\beta = pq + abxy + axq + byp \in \mathfrak{p}$$

because $pq, xy, p, q \in \mathfrak{p}$. Thus $\alpha\beta \in S \cap \mathfrak{p}$, a contradiction. □

2. Let $f : A \to A'$ be a surjective homomorphism of rings, and assume that A is local, $A' \neq 0$. Show that A' is local.

Proof. This is an obvious result of the "lattice isomorphism theorem" or "correspondence theorem" for rings, which states that, for a given ideal K of a ring A, there is an inclusion preserving bijection (given by the natural projection) between the ideals of A containing K and the ideals of A/K.

First, note that the preimage of an ideal under $\varphi : R \to S$ is an ideal: let I be an ideal of S; for any $a, b \in f^{-1}(I)$ and $c \in A$ we have $f(a+b) = f(a) + f(b) \in I$ and $f(ca) = f(c)f(a) \in I$, so $a + b, ca \in f^{-1}(I)$.

Any ideal J of A/K is the image, under the natural projection, of an ideal I of A that contains K. Thus, $J = I/K$. This correspondence is obviously inclusion preserving. In fact, this whole paragraph follows from the correspondence theorem for groups, since ideals are subgroups of the ring's underlying additive group, and the previous paragraph shows that the subgroup correspondence must restrict to a correspondence of the ideals.

Let $\mathfrak{m}$ be the unique maximal ideal of A, and let $K = \ker f$. Since $A/K \cong A'$, $K \neq A$ because $A' \neq 0$. Therefore, K is contained in a maximal ideal of A, which must be $\mathfrak{m}$. Identifying A' with A/K, this means that every ideal of A' corresponds to an ideal of A containing K. Since the correspondence is inclusion preserving, every ideal of A' must be contained in $\mathfrak{m}/K$, which is properly contained in A' because the correspondence is a bijection. This makes $\mathfrak{m}/K$ the unique maximal ideal of A'. Therefore, A' is local. $\square$