From the text (pages 98 – 106): 21, 22

1. If $I = \langle 1+2i \rangle$ is the principal ideal generated by $1+2i$ in the ring of Gaussian integers $\mathbb{Z}[i]$, then show that $\mathbb{Z}[i]/I$ is a finite field, and find its order.

   ▶ **Solution.** Define a ring homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}[i]/I$ by $\varphi(n) = n + I$. Note that the following calculations are true in the quotient ring $\mathbb{Z}[i]/I$:

$$\begin{array}{rccc} & (1+2i)+I & = & 0+I \\ \Longrightarrow & 1+I & = & -2i+I \\ \Longrightarrow & i+I & = & 2+I \\ \Longrightarrow & bi+I & = & 2b+I \\ \Longrightarrow & a+bi+I & = & a+2b+I. \end{array}$$

   The last equality says that φ is surjective since every coset $a + bi + I \in \mathbb{Z}[i]/I$ has an integer representative $n+I$ where $n = a+2b$. That is, $\varphi(a+2b) = a+2b+I = a+bi+I$.

   Now observe that $\mathrm{Ker}(\varphi) = 5\mathbb{Z}$. To see this suppose that $n \in \mathrm{Ker}(\varphi)$. This means that $\varphi(n) = 0 + I$, i.e, $n \in I$ so that $n = (1 + 2i)(a + bi)$ for some a, $b \in \mathbb{Z}$. Thus $n = (a - 2b) + (2a + b)i$ so that we must have $2a + b = 0$ and $n = a - 2b$. Hence $b = -2a$ and then $n = a - 2b = a + 4a = 5a \in 5\mathbb{Z}$. Moreover, all multiples of 5 are in $\mathrm{Ker}(\varphi)$ since $5 = (1 + 2i)(1 - 2i)$. Therefore, the isomorphism theorem states that $\mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}[i]/I$, so that $\mathbb{Z}[i]/I$ is the finite field $\mathbb{Z}_5$ with 5 elements. ◀

2. Express the polynomial $X^4 - 2X^2 - 3$ as a product of irreducible polynomials over each of the following fields: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_5$.

   ▶ **Solution.** The factorization $X^4 - 2X^2 - 3 = (X^2 - 3)(X^2 + 1)$ is valid over $\mathbb{Z}$ and hence over each of the given fields. The further factorization of the two quadratics in a given field is dependent upon whether there is a root of the quadratic in that field. The results are tabulated in the following table.

Field	**Factorization**
$\mathbb{Q}$	$(X^2-3)(X^2+1)$
$\mathbb{R}$	$(X-\sqrt{3})(X+\sqrt{3})(X^2+1)$
$\mathbb{C}$	$(X-\sqrt{3})(X+\sqrt{3})(X+i)(X-i)$
$\mathbb{Z}_5$	$(X^2-3)(X+2)(X-2)$

◀

3. Let R be the quadratic integer ring $\mathbb{Z}[\sqrt{-5}]$. Define 3 ideals of R: $I_2 = \langle 2,\, 1+\sqrt{-5} \rangle$, $I_3 = \langle 3,\, 2+\sqrt{-5} \rangle$, and $I_3' = \langle 3,\, 2-\sqrt{-5} \rangle$.

   (a) Prove that each of the ideals I_2, I_3 and I_3' is a nonprincipal ideal of R.

► **Solution.** For each $z = a + b\sqrt{-5}$, define $N(z) = |z|^2 = z\overline{z} = a^2 + 5b^2$. This is a norm function on $\mathbb{Z}[\sqrt{-5}]$ such that $N(zw) = N(z)N(w)$. Now suppose that $I_2 = \langle a + b\sqrt{-5}\rangle$ is a principal ideal. Since $2 \in I_2$ we must have an equation $2 = (a+b\sqrt{-5})(c+d\sqrt{-5})$, and applying the norm function to this equation gives $4 = (a^2 + 5b^2)(c^2 + 5d^2)$ and this equation takes place in the ordinary integers $\mathbb{Z}$. From the unique factorization in $\mathbb{Z}$ we conclude that $a^2 + 5b^2 \in \{1, 2, 4\}$. The only way this can occur is if $b = 0$ and $a = \pm 1$ or $a = \pm 2$.

Case 1: $a = \pm 1$.

In this case we are assuming that $I_2 = \langle 1\rangle = \mathbb{Z}[\sqrt{-5}]$. Suppose that we have an equation

$$1 = 2(r + s\sqrt{-5}) + (u + v\sqrt{-5})(1 + \sqrt{-5})$$

where r, s, v, and v are integers. This gives an equation

$$1 = 2r + u - 5v + (2b + u + v)\sqrt{-5}$$

which implies that

$$\begin{aligned} 1 &= 2r + u - 5v \\ 0 &= 2b + u + v. \end{aligned}$$

Subtracting the second equation from the first gives an equation in integers

$$1 = 2(r - b - 3v).$$

This is clearly impossible since 2 does not divide 1 in $\mathbb{Z}$, so $I_2 \neq \langle 1\rangle$.

Case 2: $a = \pm 2$.

In this case we are assuming that $I_2 = \langle 2\rangle$. Since $1 + \sqrt{-5} \in I_2$, this means that we can write

$$1 + \sqrt{-5} = 2(r + s\sqrt{-5})$$

for some r, $s \in \mathbb{Z}$. This would force $2r = 1$, which is not possible in $\mathbb{Z}$.

Since we have excluded both cases $a = \pm 1$ and $a = \pm 2$, we conclude that the supposition that I_2 is principal is not valid.

The cases for I_3 and I_3' are similar. ◄

(b) Show that $I_2^2 = \langle 2\rangle$, so that the product of nonprincipal ideals can be a principal ideal.

► **Solution.** Since $I_2^2 = \langle 4,\ 2+2\sqrt{-5},\ -4+2\sqrt{-5}\rangle \subseteq \langle 2\rangle$ because each generator of I_2^2 is a multiple of 2, it is sufficient to show that $2 \in I_2^2$, since this will imply that $\langle 2\rangle \subseteq I_2^2$ and hence that $I_2^2 = \langle 2\rangle$. But $2 \in I_2^2$ since

$$2 = (2 + 2\sqrt{-5}) - (4 + (-4 + 2\sqrt{-5})),$$

which is a $\mathbb{Z}[\sqrt{-5}]$-linear combination of the generators of I_2^2. ◄

(c) Similarly, prove that $I_2I_3 = \langle 1-\sqrt{-5}\rangle$ and $I_2I_3' = \langle 1+\sqrt{-5}\rangle$ are principal. Deduce that the principal ideal $\langle 6\rangle$ is a product of 4 ideals:

$$\langle 6\rangle = I_2^2 I_3 I_3'.$$

▶ **Solution.** By multiplying the generators of I_2 and I_3 we conclude that

$$I_2I_3 = \langle 6,\, 4+2\sqrt{-5},\, 3+3\sqrt{-5},\, -3+3\sqrt{-5}\rangle.$$

From the calculations

$$\begin{aligned} 6 &= (1-\sqrt{-5})(1+\sqrt{-5}) \\ 4+2\sqrt{-5} &= -(1-\sqrt{-5})^2 \\ 3+3\sqrt{-5} &= (1-\sqrt{-5})(-2+\sqrt{-5}) \\ -3+3\sqrt{-5} &= -3(1-\sqrt{-5}), \end{aligned}$$

it follows that each generator of I_2I_3 is in $\langle 1-\sqrt{-5}\rangle$, and hence

$$I_2I_3 \subseteq \langle 1-\sqrt{-5}\rangle.$$

It remains to show that $1-\sqrt{-5} \in I_2I_3$. But $1-\sqrt{-5} = (4+2\sqrt{-5})-(3+3\sqrt{-5}) \in I_2I_3$. Hence, $\langle 1-\sqrt{-5}\rangle \subset I_2I_3$ and we conclude that $I_2I_3 = \langle 1-\sqrt{-5}\rangle$.
The other equality $I_2I_3' = \langle 1+\sqrt{-5}\rangle$ follows from the one just completed by taking complex conjugations. Then putting the two results together gives

$$\langle 6\rangle = \langle 1-\sqrt{-5}\rangle\langle 1+\sqrt{-5}\rangle = I_2I_3I_2I_3' = I_2^2I_3I_3'.$$

◀

Text Exercises:

21. (a) If $R=\mathbb{Z}$ or $R=\mathbb{Q}$ and d is not a square in R, show that $R[\sqrt{d}] \cong R[X]/\langle X^2-d\rangle$.

▶ **Solution.** Define a substitution homomorphism $\varphi : R[X] \to \mathbb{C}$ by $\varphi(f(X)) = f(\sqrt{d})$. Then $\operatorname{Im}(\varphi) = R[\sqrt{d}]$ so $R[X]/\operatorname{Ker}(\varphi) \cong \operatorname{Im}(\varphi) = R[\sqrt{d}]$ and it is only necessary to show that $\operatorname{Ker}(\varphi) = \langle X^2-d\rangle$. To see this, let $f(X) \in \operatorname{Ker}(\varphi)$ and divide $f(X)$ by X^2-d in $R[X]$ to get $f(X) = (X^2-d)q(X)+aX+b$ where $aX+b \in R[X]$. Since $f(X) \in \operatorname{Ker}(\varphi)$ we conclude that the complex number $\sqrt{d}$ satisfies

$$0 = f(\sqrt{d}) = ((\sqrt{d})^2-d)q(\sqrt{d}) + a\sqrt{d}+b = a\sqrt{d}+b,$$

where a and b are in $R=\mathbb{Z}$ or $R=\mathbb{Q}$. If $a\neq 0$, then we get an equation $\sqrt{d} = -b/a \in \mathbb{Q}$. But, d is assumed to not be a square in R. If $R=\mathbb{Q}$ we have an immediate contradiction, while if $R=\mathbb{Z}$, the rational root theorem shows that any solution of X^2-d in $\mathbb{Q}$ is already a solution in $\mathbb{Z}$. Hence, we conclude that $a=0$, which then gives $b=0$ so X^2-d divides $f(X)$. Thus, $\operatorname{Ker}(\varphi) = \langle X^2-d\rangle$, and the proof is complete. ◀

(b) If $R = \mathbb{Z}$ or $R = \mathbb{Q}$ and d_1, d_2, and d_1/d_2 are not squares in $R \setminus \{0\}$, show that $R[\sqrt{d_1}]$ and $R[\sqrt{d_2}]$ are not isomorphic.

▶ **Solution.** Suppose that $R[\sqrt{d_1}]$ and $R[\sqrt{d_2}]$ are isomorphic via a ring isomorphism $\varphi : R[\sqrt{d_1}] \to R[\sqrt{d_2}]$. We show that this leads to a contradiction. Let $\varphi(\sqrt{d_1}) = a + b\sqrt{d_2} \in R[\sqrt{d_2}]$, where a, $b \in R$. Since φ is a ring homomorphism, and since $\varphi(1) = 1$, we see that $(a + b\sqrt{d_2})^2 = (\varphi(\sqrt{d_1}))^2 = \varphi(d_1) = d_1$, so that

$$a^2 + 2ab\sqrt{d_2} + b^2 d_2 = d_1.$$

If a or b is 0, this shows that d_1 or d_1/d_2 is a square in R, both of which we have excluded. Thus, both a and b are not 0, and hence,

$$\sqrt{d_2} = \frac{d_1 - a^2 - b^2 d_2}{2ab}.$$

Thus we would conclude that d_2 is a square in R, which is also excluded by choice. Hence, there can be no ring isomorphism of $R[\sqrt{d_1}]$ and $R[\sqrt{d_2}]$. ◀

(c) Let $R_1 = \mathbb{Z}_p[X]/(X^2 - 2)$ and $R_2 = \mathbb{Z}_p[X]/(X^2 - 3)$. Determine if $R_1 \cong R_2$ in case $p = 2$, $p = 5$, or $p = 11$.

Case 1: $p = 2$.

▶ **Solution.** In this case $R_1 = \mathbb{Z}_2[X]/\langle X^2\rangle$ and $R_2 = \mathbb{Z}_2[X]/\langle X^2 - 1\rangle = \mathbb{Z}_2[X]/\langle (X-1)^2\rangle$. The substitution homomorphism $\varphi : \mathbb{Z}_2[X] \to R_2$ given by $\varphi(X) = (X - 1) + \langle (X-1)^2\rangle$ has $\mathrm{Ker}(\varphi) = \langle X^2\rangle$ so the first isomorphism theorem gives an isomorphism between R_1 and R_2. ◀

Case 2: $p = 5$.

▶ **Solution.** In this case, the polynomials $X^2 - 2$ and $X^2 - 3$ are both irreducible in $\mathbb{Z}_5[X]$ since, by inspection $1^2 = 4^2 = 1$, $2^2 = 3^3 = 4$ in $\mathbb{Z}_5$ so neither polynomial has a root in $\mathbb{Z}_5$. To find an isomorphism from $R_1 = \mathbb{Z}_5[X]/\langle X^2 - 2\rangle$ to $R_2 = \mathbb{Z}[X]/\langle X^2 - 3\rangle$, it is sufficient to find a root of the polynomial $X^2 - 2$ in R_2. So, look for $(aX + b)^2 \equiv 2 \pmod{(X^2 - 3)}$ where the congruence is in $\mathbb{Z}_5[X]$. Thus, we want to find a and b in $\mathbb{Z}_5$ with

$$(aX + b)^2 - 2 = a^2X^2 + 2abX + b^2 - 2 = c(X^2 - 3).$$

This is true if $b = 0$, $c = a^2$ and $-3c = -2$. The last equation gives $c = 4$ so $a = 2$. Thus, define $\varphi : \mathbb{Z}_5[X] \to R_2$ by $\varphi(X) = 2X + \langle X^2 - 3\rangle$. Since

$$\varphi(X^2 - 2) = 4X^2 - 2 + \langle X^2 - 3\rangle = 4(X^2 - 3) + \langle X^3 - 3\rangle = 0 + \langle X^3 - 3\rangle,$$

it follows that $\mathrm{Ker}(\varphi) = \langle X^2 - 2\rangle$, so the first isomorphism theorem give a ring isomorphism from $R_1 = \mathbb{Z}_5/\langle X^2 - 2\rangle$ to R_2. ◀

Case 3: $p = 11$.

▶ **Solution.** The squares in $\mathbb{Z}_{11}$ are $1 = (\pm 1)^2$, $4 = (\pm 2)^2$, $9 = (\pm 3)^2$, $5 = (\pm 4)^2$, and $3 = (\pm 5)^2$. Hence, the polynomial $X^2 - 2$ is irreducible over $\mathbb{Z}_{11}$, so $R_1 = \mathbb{Z}_{11}[X]/\langle X^2 - 2\rangle$ is a field (with $11^2 = 121$ elements), while the polynomial $X^2 - 3$ factors in $\mathbb{Z}_{11}[X]$ as $X^2 - 3 = X^2 - 25 = (X - 5)(X + 5)$, so that $R_2 = \mathbb{Z}_{11}[X]/\langle X^2 - 3\rangle$ is not an integral domain. Thus R_1 is not isomorphic to R_2. ◀

1. Recall that R^* denotes the group of units of the ring R.

   (a) Show that $(\mathbb{Z}[\sqrt{-1}])^* = \{\pm 1, \pm\sqrt{-1}\}$.

   ▶ **Solution.** Let $N(z) = N(a + b\sqrt{-1}) = z\overline{z} = \left|a + b\sqrt{-1}\right|^2 = a^2 + b^2 \in \mathbb{Z}^+$ be the norm on the ring $\mathbb{Z}[\sqrt{-1}]$. Since this is just the square of the modulus function on $\mathbb{C}$, it follows that N is multiplicative. That is, $N(zw) = N(z)N(w)$ for all z, $z \in \mathbb{Z}[\sqrt{-1}]$. If z is a unit, then $zw = 1$ so $1 = N(zw) = N(z)N(w)$, and this is an equation among nonnegative integers, so we must have $N(z) = 1$. Conversely, if $N(z) = 1$, then $z\overline{z} = 1$ so z is a unit. Thus, $z = a + b\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$ is a unit if and only if $1 = N(z) = a^2 + b^2$. Since a and b are integers, this can only happen if $a = \pm 1$ and $b = 0$; or $a = 0$ and $b = \pm 1$. Hence, the set of units of $\mathbb{Z}[\sqrt{-1}]$ is $\left\{\pm 1, \pm\sqrt{-1}\right\}$. ◀

   (b) If $d < -1$ show that $(\mathbb{Z}[\sqrt{-d}])^* = \{\pm 1\}$.

   ▶ **Solution.** The argument is the same as the previous paragraph, except that we use the norm function $N(z) = N(a + b\sqrt{-d}) = |a^2 - db^2|$. As above, $N(zw) = N(z)N(w)$ as we conclude that $z = a + b\sqrt{-d}$ is a unit if and only if $N(z) = 1$. But, $d < -1$, so $a^2 - db^2 = 1$ if and only if $a = \pm 1$ and $b = 0$. Thus, $(\mathbb{Z}[\sqrt{-d}])^* = \{\pm 1\}$. ◀

   (c) Show that

   $$\mathbb{Z}\left[\frac{(1 + \sqrt{-3})}{2}\right]^* = \left\{\pm 1,\ \pm\frac{1 + \sqrt{-3}}{2},\ \pm\frac{-1 + \sqrt{-3}}{2}\right\}.$$

   ▶ **Solution.** Let $\omega = (1 + \sqrt{-3})/2$, so that $\mathbb{Z}[\omega] = \{m + n\omega : m, n \in \mathbb{Z}\}$. As in the calculations above, if $\alpha = m + n\omega \in \mathbb{Z}[\omega]$, then we define the norm of α by $N(\alpha) = \alpha\overline{\alpha} = |\alpha|^2 \in \mathbb{Z}^+$. Thus the norm of α is the square of the modulus of α as a complex number. Moreover, α is a unit if and only if $N(\alpha) = 1$. If $\alpha = m + n\omega$, then α is a unit if and only if

   $$\begin{aligned} N(\alpha) &= N(m + n\omega) = N\left(m + n\left(\frac{(1 + \sqrt{-3})}{2}\right)\right) = \left|\left((m + \frac{n}{2}) + \frac{n\sqrt{3}i}{2}\right)\right| \\ &= \left(m + \frac{n}{2}\right)^2 + \frac{3}{4}n^2 = 1. \end{aligned}$$

Since m and n are integers, the only possibilities for this last equation are $n = 0$, $m = \pm 1$; $n = 1$, $m = 0$; $n = 1$, $m = -1$; $n = -1$, $m = 0$, or $n = -1$, $m = 1$. These six choices for the pair (m, n) give the units of $\mathbb{Z}[\omega]$, as required. ◀

(d) Let $d > 0 \in \mathbb{Z}$ not be a perfect square. Show that if $\mathbb{Z}[\sqrt{d}]$ has one unit other than ± 1, it has infinitely many.

▶ **Solution.** Suppose that $u \neq \pm 1$ is a unit of $\mathbb{Z}[\sqrt{d}]$ where $d > 0 \in \mathbb{Z}$. Since $\mathbb{Z}[\sqrt{d}] \subset \mathbb{R}$, by multiplying by -1 if necessary, we can assume that $u > 0$. Since u is a unit, this means that there is a $v \in \mathbb{Z}[\sqrt{d}]$ with $uv = 1$. Then, for every $n \in \mathbb{N}$, $u^n v^n = (uv)^n = 1$, so u^n is also a unit. Since $u > 0$ and $u \neq 1$, it follows that the real numbers u^n are all distinct. Thus, there are infinitely many units of $\mathbb{Z}[\sqrt{d}]$. ◀

(e) It is known that the hypothesis in part (d) is always satisfied. Find a unit in $\mathbb{Z}[\sqrt{d}]$ other than ± 1 for $2 \leq d \leq 15$, $d \neq 4, 9$.

▶ **Solution.** The norm in the ring $\mathbb{Z}[\sqrt{d}]$ is given by

$$N(m + n\sqrt{d}) = \left|(m + n\sqrt{d})(m - n\sqrt{d})\right| = \left|m^2 - dn^2\right|,$$

and $\alpha = m + n\sqrt{d}$ is a unit if and only if $N(\alpha) = 1$, in which case the equation $(m+n\sqrt{d})(m-n\sqrt{d}) = m^2 - dn^2 = \pm 1$ shows that $\alpha^{-1} = \pm(m - n\sqrt{d})$. Therefore, the strategy for finding a unit in $\mathbb{Z}[\sqrt{d}]$ is to look for m and n in $\mathbb{Z}$ such that $m^2 - dn^2 = \pm 1$. For small values of d, this can be accomplished by trial and error, or by doing some calculations in Maple or in a spreadsheet. The following units were found in this experimental manner.

d	α	α^{-1}
2	$1 + \sqrt{2}$	$-1 + \sqrt{2}$
3	$2 + \sqrt{3}$	$2 - \sqrt{3}$
5	$2 + \sqrt{5}$	$-2 + \sqrt{5}$
6	$5 + 2\sqrt{6}$	$5 - 2\sqrt{6}$
7	$8 + 3\sqrt{7}$	$8 - 3\sqrt{7}$
8	$3 + \sqrt{8}$	$3 - \sqrt{8}$
10	$3 + \sqrt{10}$	$-3 + \sqrt{10}$
11	$10 + 3\sqrt{11}$	$10 - 3\sqrt{11}$
12	$7 + 2\sqrt{12}$	$7 - 2\sqrt{12}$
13	$18 + 5\sqrt{13}$	$-18 + 5\sqrt{13}$
14	$15 + 4\sqrt{14}$	$15 - 4\sqrt{14}$
15	$4 + \sqrt{15}$	$4 - \sqrt{15}$

◀