

1. Let $R = 3Z \oplus 4Z$, let $A = 9Z \oplus 4Z$.
- a. **Show that A is an ideal of R .**
 Given $x, y \in A$, say $x = (9m, 4n)$, $y = (9i, 4j)$, $x - y = (9(m-i), 4(n-j))$
 so $x - y \in A$. If $z = (3u, 4v) \in R$, then $xz = (27mu, 16nv) = (9 \cdot 3mu, 4 \cdot 4nv)$
 so $xz \in A$. Thus, A is an ideal
- b. **Determine whether A is a prime ideal of R .**
 A is not a prime ideal: $(3, 0), (6, 0)$ are not in A , but their product,
 $(18, 0) = (9 \cdot 2, 4 \cdot 0)$ is in A .
- c. **Determine whether A is a maximal ideal of R .**
 Suppose $A \subseteq I \subseteq R$ but $A \neq I$. Then there is an element $x \in I, x \notin A$.
 This x must have the form $(3a, 4b)$ for some integers a, b , but a is not
 a multiple of 3. We can write $a = 3q + r, r = 1$ or 2 , and say
 $x = (9q + 3r, 4b)$. Since $(9q, 4b) \in A \subseteq I, x - (9q, 4b) = (3r, 0)$ is in I .
 If $r = 1$, then $(3, 0) \in I$. If $r = 2$, $(6, 0) \in I$ and $(9, 0) - (6, 0) \in I$. Either
 way, I contains $(3, 0)$ and $(0, 4)$, so I contains $\langle (3, 0), (0, 4) \rangle = R$. Thus
 A IS a maximal ideal.
- d. **Write out the addition and multiplication tables for R/A . Is R/A a field? An integral domain? Why does this not contradict the theorems on page 259 of the book? ← That should have been page 267 (Theorems 14.3, 14.4)**

$$R/A = \{A, (3, 0) + A, (6, 0) + A\} = \{0, a, b\}$$

$R/A, +$	0	a	b
0	0	a	b
a	a	b	0
b	b	0	a

$R/A, \times$	0	a	b
0	0	0	0
a	0	0	0
b	0	0	0

R/A has zero divisors so it is neither a field nor an integral domain. This does not contradict Theorem 14.3 and Theorem 14.4 because they apply to commutative rings **WITH UNITY**, and R does not have a unity.

2. **Show that $\mathbb{R}[x]/\langle x - 5 \rangle \cong \mathbb{R}$.**

Define $\varphi : \mathbb{R}[x] \rightarrow \mathbb{R}$ by $\varphi(f(x)) = f(5)$. Then φ is an onto homomorphism since $\varphi(x + r - 5) = r$. The kernel of φ consists of all polynomials $p(x)$ with $p(5) = 0$, and this is $\langle x - 5 \rangle$. The First Isomorphism Theorem now says $\mathbb{R}[x]/\langle x - 5 \rangle \cong \mathbb{R}$.

3. **Show that $\mathbb{Z}[\sqrt{n}]/\langle \sqrt{n} \rangle \cong \mathbb{Z}_n$ if n is not a square. Hint: define $\varphi : \mathbb{Z}[\sqrt{n}] \rightarrow \mathbb{Z}_n$ by $\varphi(a + b\sqrt{n}) = a \pmod{n}$.**

Following the hint, define φ by $\varphi(a + b\sqrt{n}) = a \pmod{n}$, which only makes sense if n is not a square. (For example, in the case of $n = 4$, $3 + \sqrt{4} = 5$, so does $\varphi(3 + \sqrt{4}) = 3 \pmod{4}$ or $1 \pmod{4}$?)

The kernel of φ consists of all things of the form $a + b\sqrt{n}$ where $a = 0 \pmod{n}$, or $nq + b\sqrt{n}$. These can all be written as $\sqrt{n}(b + q\sqrt{n})$, so $\ker(\varphi) = \langle \sqrt{n} \rangle$, and the result again follows from the First Isomorphism Theorem.

4. **Show that every field is a principal ideal domain.**

A field F only has two ideals, $\{0\}$ and F . For if I is an ideal and $I \neq \{0\}$, then for any $a \neq 0$ in I , $a^{-1}a \in I$ (by multiplicative closure) so $1 \in I \Rightarrow I = F$. Now $\{0\} = \langle 0 \rangle$ and $F = \langle 1 \rangle$, so every ideal in F is a principal ideal.

5. **Factor $x^{12} - 1$ into irreducible polynomials over \mathbb{Q} . Justify that each term is, in fact, irreducible.**

We have $x^{12} - 1 = (x^6 - 1)(x^6 + 1) = (x^3 - 1)(x^3 + 1)(x^6 + 1)$
 $= (x - 1)(x + 1)(x^2 + x + 1)(x^2 - x + 1)(x^2 + 1)(x^4 - x^2 + 1)$.

This is the factorization of $x^{12} - 1$ into irreducibles. To see this, $x - 1$, $x + 1$ are irreducible because they have degree 1. By the rational root theorem, the only possible rational zeros of $x^{12} - 1$ are 1, -1. Thus, these are the only rational zeros of any divisor of $x^{12} - 1$. It is easy to check that none of the last 4 polynomials has 1 or -1 as a zero. As $x^2 + x + 1$, $x^2 - x + 1$, $x^2 + 1$ have degree 2 and no zeros, they are irreducible. This leaves $x^4 - x^2 + 1$. By Gauss's theorem, if this factors over the rationals, it must factor over the integers so try $x^4 - x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d)$, $a, b, c, d \in \mathbb{Z}$. If we multiply this out, $x^4 - x^2 + 1 = x^4 + (a + c)x^3 + (ac + b + d)x^2 + (ad + bc)x + bd$. This tells us $a + c = 0$, $ac + b + d = -1$, $ad + bc = 0$, $bd = 1$. Since b and d are integers, either $b = d = 1$ or $b = d = -1$. In the first case, $a + c = 0$, $ac = -3$. But if

$a + c = 0$, then $c = -a$, and we get $-a^2 = -3$, or $a^2 = 3$ which has no integer solutions. If $b = d = -1$, we have $a + c = 0$, $ac = 1$. Here, again $c = -a$, so we need $-a^2 = 1$, or $a^2 = -1$, and again there are no solutions. Thus, $x^4 - x^2 + 1$ is irreducible over \mathbb{Q} .

6. **Find all irreducible polynomials of degree 2 and 3 over \mathbb{Z}_2 . Use this to show that $x^6 + x^3 + 1$ is irreducible over \mathbb{Z}_2 .**

Degree 2: $x^2 + x + 1$ is the only one ($x^2 + 1 = (x + 1)^2 \pmod{2}$).

Degree 3: $x^3 + x + 1$, $x^3 + x^2 + 1$ are the only ones.

(I am using the result that $p(x)$ of degree 2 or 3 is irreducible if and only if it has no zeros. Here, we need only check $x = 0$, $x = 1$. For example, $x^3 + 1$ is reducible because $x = 1$ is a zero).

Now $x^6 + x^3 + 1$ has no zeros, so it has no linear factors. If it were reducible, it would have to be divisible by either an irreducible of degree 2 or one of degree 3. I'll let you do the long division by each of the three irreducibles listed above to show that $x^6 + x^3 + 1$ is not divisible by any of them. I'll mention, though, that as a check on your work, one division result is:

$$x^6 + x^3 + 1 = (x^3 + x + 1)(x^3 + x) + x^2 + x + 1.$$

7. a. **Show that $\langle 2 \rangle$ is a maximal ideal in \mathbb{Z} but not in $\mathbb{Z}[i]$.**

For the second part, $2 = (1 + i)(1 - i)$, and neither $1 + i$ nor $1 - i$ is in $\langle 2 \rangle$ since $\langle 2 \rangle = \{2a + 2bi \mid a, b \in \mathbb{Z}\}$. For the first part, suppose that $\langle 2 \rangle \subseteq I \subseteq \mathbb{Z}$, but $\langle 2 \rangle \neq I$. Then there is an $m \in I$ with $m \notin \langle 2 \rangle$. This means that m must be odd, $m = 2k + 1$. Since $2k \in \langle 2 \rangle \subseteq I$, $m - 2k = 1$ is in I , so $I = \mathbb{Z}$.

- b. **Show that $\langle 3 \rangle$ is a maximal ideal in \mathbb{Z} AND in $\mathbb{Z}[i]$.**

$\langle 3 \rangle$ is maximal in \mathbb{Z} : Let $\langle 3 \rangle \subseteq I \subseteq \mathbb{Z}$, but $\langle 3 \rangle \neq I$. Then there is an $m \in I$ with $m \notin \langle 3 \rangle$. Writing $m = 3q + r$, $r = 1$, or 2 , we have (as we have seen several times) that $r \in I$. If $r = 1$, then $1 \in I$. If $r = 2$, then $2, 3 \in I \Rightarrow 1 \in I$. Thus, in both cases, $1 \in I$ so $I = \mathbb{Z}$.

Next, consider $\langle 3 \rangle \subseteq I \subseteq \mathbb{Z}[i]$, but $\langle 3 \rangle \neq I$. Here, $\langle 3 \rangle = \{3x + 3yi\}$. Let $a = u + vi \in I$, $a \notin \langle 3 \rangle$. If we write $u = 3q_1 + r$, $v = 3q_2 + s$, then as we've seen many times, we have that $r + si \in I$, and that $r = 0, 1, 2$, $s = 0, 1, 2$, and r, s are not both 0. If we multiply $r + si$ by $r - si$, we get that I contains $r^2 + s^2$, and the possible values of $r^2 + s^2$ are: 1, 2, 4, 5, 8. I contains all integer multiples of 3. Subtracting these

I contains 1 or 2. Finally, since $3 - 2 = 1$, we are forced to conclude that I contains 1, so $I = \mathbb{Z}[i]$.

8. a. **Show that $\langle \sqrt{5} \rangle$ is a maximal ideal of $\mathbb{Z}[\sqrt{5}]$.**

Suppose that $\langle \sqrt{5} \rangle \subseteq I \subseteq \mathbb{Z}[\sqrt{5}]$ and $I \neq \langle \sqrt{5} \rangle$. Now $\langle \sqrt{5} \rangle = \{ \sqrt{5}(a + b\sqrt{5}) \} = \{ 5x + y\sqrt{5} \mid x, y \in \mathbb{Z} \}$. Let $u \in I$, $u \notin \langle \sqrt{5} \rangle$. Then $u = a + b\sqrt{5}$ where a is not divisible by 5. Writing $a = 5q + r$, with $r = 1, 2, 3$, or 4 , we have $u - (5q + b\sqrt{5}) \in I$, so $r \in I$. Cheap trick: If $r \in I$, then $r^4 \in I$. Also, $5k \in I$ for all integers k . Now $r^4 = 1$, or $16 = 1 + 3 \cdot 5$, or $81 = 1 + 16 \cdot 5$ or $256 = 1 + 51 \cdot 5$. In any case, subtracting the right multiple of 5, $1 \in I$ so $I = \mathbb{Z}[\sqrt{5}]$. This shows that $\langle \sqrt{5} \rangle$ is maximal.

b. **Show that $\langle \sqrt{6} \rangle$ is not a maximal ideal of $\mathbb{Z}[\sqrt{6}]$.**

Here, $\langle \sqrt{6} \rangle = \{ \sqrt{6}(a + b\sqrt{6}) \} = \{ 6x + y\sqrt{6} \mid x, y \in \mathbb{Z} \}$.

Let $I = \{ 2x + y\sqrt{6} \mid x, y \in \mathbb{Z} \}$. I'll let you check that I is an ideal, and $\langle \sqrt{6} \rangle \subseteq I \subseteq \mathbb{Z}[\sqrt{6}]$, with each inclusion being proper.