Solutions for Some Ring Theory Problems

1. Suppose that I and J are ideals in a ring R. Assume that $I \cup J$ is an ideal of R. Prove that $I \subseteq J$ or $J \subseteq I$.

SOLUTION. Assume to the contrary that I is not a subset of J and that J is not a subset of I. It follows that there exists an element $i \in I$ such that $i \notin J$. Also, there exists an element $j \in J$ such that $j \notin I$. Note that $i \in I \cup J$ and $j \in I \cup J$. Since we are assuming that $I \cup J$ is an ideal of R, it follows that $i + j \in I \cup J$.

Let $k = i + j$. If $k \in I$, then $k - i \in I$ too. That is, $j \in I$. This is not true and hence $k \notin I$. If $k \in J$, then $k - j \in J$ too. That is, $i \in J$. However, this is not true and hence $k \notin J$. We have shown that $k \notin I$ and $k \notin J$. That is, $k \notin I \cup J$. Thus, $i + j \notin I \cup J$, contradicting what was found in the previous paragraph.

This contradiction prove the stated assertion.

2. Find an example of an integral domain R with identity and two ideals I and J of R with the following properties: Both I and J are principal ideals of R, but $I + J$ is not a principal ideal of R.

SOLUTION. Let $R = \mathbb{Z}[\sqrt{-5}]$. We gave examples in class of non-principal maximal ideals in R. One such example arose by considering the homomorphism

$$\varphi : \mathbb{Z}[\sqrt{-5}] \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

defined by $\varphi(a + b\sqrt{-5}) = a + b + 2\mathbb{Z}$ for all $a, b \in \mathbb{Z}$. This definition is based on the fact that $(1 + 2\mathbb{Z})^2 = -5 + 2\mathbb{Z}$.

Let $K = Ker(\varphi)$. Then K is a maximal ideal in R. Notice that K contains 2 and $1 + \sqrt{-5}$. Let $I = (2)$ and let $J = (1 + \sqrt{-5})$. Then I and J are principal ideals in R. Furthermore, $I \subseteq K$ and $J \subseteq K$. Note that $2 \notin J$ and $1 + \sqrt{-5} \notin I$. This is true because $N(2) = 4$ and $N(1 + \sqrt{-5}) = 6$, and neither of these norms divides the other.

Since $I \subseteq K$ and $J \subseteq K$, it follows that $I + J \subseteq K$. Furthermore, suppose that $\kappa \in K$. Then $\kappa = a + b\sqrt{-5}$, where $a, b \in \mathbb{Z}$. We have

$$\varphi(\kappa) = a + b + 2\mathbb{Z} = 0 + 2\mathbb{Z}$$

and so we have $a + b \in 2\mathbb{Z}$. We also clearly have $a - b = a + b - 2b \in 2\mathbb{Z}$. That is, $a - b = 2c$ for some $c \in \mathbb{Z}$. It then follows that

$$\kappa = a + b\sqrt{-5} = a + b(1 + \sqrt{-5}) - b = 2c + b(1 + \sqrt{-5} \in I + J .$$

We have proven that $K \subseteq I+J$. Since, $I+J \subseteq K$ is also true, it follows that $K = I+J$.

Finally, we will show that K is not a principal ideal. In fact, this was shown in class one day. Suppose to the contrary that $K = (\kappa)$. Since $2 \in K$, it follows that κ divides 2 in the ring R. Thus, $2 = \kappa\lambda$, where $\lambda \in R$. Therefore, $N(2) = N(\kappa)N(\lambda)$. Now $N(2) = 4$. Furthermore, κ is not a unit in R because $K \neq R$. Also, λ is not a unit in R because $K \neq I$. The fact that $K \neq I$ is true is true because $1+\sqrt{-5}$ is in K, but not in I. It follows that $N(\kappa) \neq 1$ and $N(\lambda) \neq 1$. Thus, $N(\kappa) = 2$. But the equation $a^2 + 5b^2 = 2$ has no solutions where $a, b \in \mathbb{Z}$. Therefore, it follows that K cannot be a principal ideal.

In summary, I and J are principal ideals in R, but $K = I+J$ is not a principal ideal in R.

3. Suppose that R is a commutative ring with identity and that K is an ideal of R. Let $R' = R/K$. The correspondence theorem gives a certain one-to-one correspondence between the set of ideals of R containing K and the set of ideals of R'. If I is an ideal of R containing K, we let I' denote the corresponding ideal of R'. Show that if I is principal, then so is I'. Show by example that the converse is not true in general.

SOLUTION. Let $\varphi : R \longrightarrow R'$ be defined by $\varphi(r) = r + K$. Then φ is a surjective ring homomorphism from R to R'. Suppose that I is an ideal of R which contains K. The corresponding ideal in R' is $\varphi(I) = \{\ \varphi(i) \mid i \in I\ \}$.

Suppose that I is a principal ideal in R. Then $I = (a)$ for some $a \in R$. That is, we have $I = \{\ ra \mid r \in R\ \}$. Then

$$I' \;=\; \varphi(I) \;=\; \{\ \varphi(ra) \mid r \in R\ \} \;=\; \{\ \varphi(r)\varphi(a) \mid r \in R\ \} \;=\; \{\ r'\varphi(a) \mid r' \in R'\ \}\ .$$

The last equality is true because $\varphi : R \to R'$ is a surjective map. It follows that $I' = \big(\varphi(a)\big)$, the principal ideal in R' generated by $\varphi(a)$.

4. Suppose that R is an integral domain with identity. Suppose that I and J are ideals in R and that $I = (b)$ where $b \in R$. Prove that $I + J = R$ is and only if $b + J$ is a unit in the ring R/J.

SOLUTION. First of all, assume that $I + J = R$. Then there exists $i \in I$ and $j \in J$ such that $i + j = 1_R$. Furthermore, since $i \in (b)$, we have $i = rb$ for some $r \in R$. Therefore, we have $rb + j = 1_R$. This implies that $1_R \in rb + J$. Therefore, we have

$$1_R + J \;=\; rb + J \;=\; (r+J)(b+J)$$

The multiplicative identity element in R/J is $1_R + J$. Note that since R is a commutative ring, so is R/J. It follows that

$$(r+J)(b+J) = 1_R + J \qquad \textit{and} \qquad (b+J)(r+J) = 1_R + J \quad .$$

It follows that $b+J$ is indeed a unit in the ring R/J. Its inverse in that ring is $r+J$.

Now assume that $b+J$ is a unit in the ring R/J. Thus, for some $r \in R$, we have

$$(r+J)(b+J) = 1_R + J \quad .$$

Thus, $rb + J = 1_R + J$ and hence $1_R \in rb + J$. Thus, $1_R = rb + j$ for some $j \in J$. Let $i = rb$. Since $I = (b)$, it follows that $i \in I$. Thus,

$$1_R \; = \; i + j \; \in \; I + J$$

and therefore, for any $s \in R$, we have $s = s1_R \in I + J$. It follows that $I + J = R$, as we wanted to prove.

5. Suppose that R is an integral domain and that $a, b \in R$. We say that a and b are *"relatively prime"* if $(a) + (b) = R$. Suppose that $c \in R$. Assume that a and b are relatively prime and that $a|bc$ in R. Prove that $a|c$ in R.

SOLUTION. We will give two arguments. First of all, since $(a) + (b) = R$, there exist elements $s, t \in R$ such that

$$sa \; + \; tb \; = \; 1_R \quad .$$

Multiply this equation by c. We obtain $c = sac + tbc$. Note that $sac = (sc)a$ is a multiple of a in R and hence is in the ideal (a). Furthermore, bc is a multiple of a in R (as stated in the problem) and hence bc is in the ideal (a). Thus, $t(bc)$ is in (a) too. It follows that $sac + tbc \in (a)$. That is, $c \in (a)$. Therefore, $a|c$ in R, as we wanted to prove.

Alternatively, we can use the result in problem 4. Let $I = (b)$ and $J = (a)$. We have $I + J = R$. Thus $b + J$ is a unit in the ring R/J. Since $a|bc$ in R, we have $bc \in J$. Therefore, we have

$$(b+J)(c+J) \; = \; bc + J \; = \; 0_R + J$$

in the ring R/J. However, $b+J$ is a unit in the ring R/J. Multiplying by the inverse of $b+J$, we find that $c + J = 0_R + J$. That is, we have $c \in J$. This means that c is a multiple of a in R. Therefore, $a|c$ in R, as we wanted to prove.

6. Suppose that R is a PID. Suppose that a, b are nonzero elements of R and that they are relatively prime. Prove that $(a) \cap (b) = (ab)$. Furthermore, consider the map

$$\varphi : R/(ab) \longrightarrow R/(a) \times R/(b)$$

defined by $\varphi(\, r+(ab)\,) = \big(\, r+(a),\; r+(b)\,\big)$ for all $r \in R$. Prove that φ is a well-defined map and that it is a ring isomorphism. (This result is often referred to as the *Chinese Remainder Theorem.*)

SOLUTION. First of all, recall the result from problem set 1 which states that the intersection of two ideals in a ring R is also an ideal in R. Thus, $(a) \cap (b)$ is an ideal in R. Since R is a PID, we must have $(a) \cap (b) = (k)$, where $k \in R$. Since $k \in (k)$ and $(k) \subseteq (b)$, it follows that $k \in (b)$ and hence $b|k$ in R. We can therefore write $k = bc$, where $c \in R$. Since $(k) \subseteq (a)$, it follows that $a|k$ in R. That is, $a|bc$ in R. Furthermore, it is assumed that a and b are relatively prime. We can use the result in problem 5 to conclude that $a|c$ in R. Thus, $c = ad$, where $d \in R$. It follows that $k = bc = bad = dab$, which is an element in the ideal (ab). We have proved that $k \in (ab)$ and hence that $(k) \subseteq (ab)$.

On the other hand, it is clear that $ab \in (a)$ and that $ab \in (b)$. Hence we have $(ab) \subseteq (a)$ and $(ab) \subseteq (b)$. Therefore, we have

$$(ab) \subseteq (a) \cap (b) = (k) \subseteq (ab)$$

and this implies that $(ab) = (a) \cap (b)$, which is the first statement that we wanted to prove.

We now discuss the map φ. First of all, consider the map

$$\psi : R \longrightarrow R/(a) \times R/(b)$$

defined by $\psi(\, r\,) = \big(\, r + (a),\; r + (b)\,\big)$ for all $r \in R$. We will show that ψ is a surjective ring homomorphism. To verify this, suppose that $r, s \in R$. Then

$$\psi(r+s) = \big(\, r+s+(a),\; r+s+(b)\,\big) = \Big(\, r+(a) \;+\; s+(a),\; r+(b) \;+\; s+(b)\,\Big)$$

$$= \big(\, r+(a),\; r+(b)\,\big) + \big(\, s+(a),\; s+(b)\,\big) = \psi(r) + \psi(s)$$

and

$$\psi(rs) = \big(\, rs+(a),\; rs+(b)\,\big) = \Big(\, \big(r+(a)\big)\big(s+(a)\big),\; \big(r+(b)\big)\big(s+(b)\big)\,\Big)$$

$$= \big(\, r+(a),\; r+(b)\,\big)\big(\, s+(a),\; s+(b)\,\big) = \psi(r)\psi(s)$$

Therefore, ψ is indeed a ring homomorphism. To prove surjectivity, we use the fact that $(a)+(b)=R$. This is true because a and b are assumed to be relatively prime.

It follows that there exist elements $u, v \in R$ such that $ua+vb=1_R$. Therefore,

$$\psi(ua) \;=\; \big(\; ua+(a),\; ua+(b) \;\big) \;=\; \big(\; 0_R+(a),\; 1_R+(b) \;\big)$$

The second equality is true because $ua \in (a)$ and $ua - 1_R = -vb \in (b)$. We also have

$$\psi(vb) \;=\; \big(\; vb+(a),\; vb+(b) \;\big) \;=\; \big(1_R+(a),\; 0_R+(b) \;\big)$$

The second equality is true because $vb - 1_R = -ua \in (a)$ and $vb \in (b)$

To complete the proof that ψ is surjective, every element in $R/(a) \;\times\; R/(b)$ has the form $\big(\; s+(a),\; t+(b)\big)$, where $s, t \in R$. Let $r = svb + tua$. Then, $r \in R$ and we have

$$\psi(r) \;=\; \psi(s)\psi(vb) + \psi(t)\psi(ua)$$

$$= \;\big(\; s+(a),\; s+(b) \;\big)\big(1_R+(a),\; 0_R+(b) \;\big) \;+\; \big(\; t+(a),\; t+(b) \;\big)\big(0_R+(a),\; 1_R+(b) \;\big)$$

$$= \;\big(\; s+(a),\; 0_R+(b) \;\big) \;+\; \big(\; 0_R+(a),\; t+(b) \;\big) \;=\; \big(\; s+(a),\; t+(b)\big)$$

This proves the surjectivity of the ring homomorphism ψ.

We now determine the kernel of ψ. The additive identity element of $R/(a) \;\times\; R/(b)$ is $\big(\; 0_R+(a),\; 0_R+(b) \;\big)$. An element $r \in R$ is in $Ker(\psi)$ if and only if

$$\psi(r) \;=\; \big(\; r+(a),\; r+(b) \;\big) \;=\; \big(\; 0_R+(a),\; 0_R+(b) \;\big) \;\;.$$

Thus, $r \in Ker(\psi)$ if and only if $r+(a) = 0_R+(a)$ and $r+(b) = 0_R+(b)$. That is,

$$Ker(\psi) \;=\; \{\; r \;\big|\; r \in (a) \quad and \quad r \in (b) \;\} \;=\; (a) \cap (b) \;.$$

By the first isomorphism theorem, it follows that the map φ defined in the problem is indeed a ring isomorphism.

7. Suppose that $R = \mathbb{Z}[\sqrt{2}]$. Suppose that M_1 and M_2 are maximal ideals of R. True or False: If the rings R/M_1 and R/M_2 are isomorphic, then $M_1 = M_2$. If true, give a proof. If false, give a counterexample.

SOLUTION. The statement is false. We will give a counterexample based on an example discussed in class. Let $F = \mathbb{Z}/7\mathbb{Z}$. Notice that $2+7\mathbb{Z}$ is a square in $\mathbb{Z}/7\mathbb{Z}$, namely we have $2+7\mathbb{Z} = (3+7\mathbb{Z})^2$. As discussed in class, we can define a surjective ring homomorphism

$$\varphi : \mathbb{Z}[\sqrt{2}] \;\longrightarrow\; F$$

by

$$\varphi(a+b\sqrt{2}) \;=\; (a+7\mathbb{Z}) \;+\; (b+7\mathbb{Z})(3+7\mathbb{Z}) \quad .$$

Note that $-3+1\sqrt{2} \in Ker(\varphi)$. Furthermore, $Ker(\varphi)$ is a maximal ideal in R because F is a field. We call this maximal ideal M_1. We have $R/M_1 \cong F$.

However, we could have chosen a different element in F whose square is $2+7\mathbb{Z}$, namely the element $4+7\mathbb{Z}$. We can then define a surjective ring homomorphism

$$\psi : \mathbb{Z}[\sqrt{2}] \;\longrightarrow\; F$$

by

$$\psi(a+b\sqrt{2}) \;=\; (a+7\mathbb{Z}) \;+\; (b+7\mathbb{Z})(4+7\mathbb{Z}) \quad .$$

Then $Ker(\varphi)$ is a maximal ideal in R. Call this maximal ideal M_2. We have $R/M_2 \cong F$.

Finally, we will show that $M_1 \neq M_2$. As mentioned above, $-3+1\sqrt{2} \in M_1$. However, $\psi(-3+1\sqrt{2}) = 1+7\mathbb{Z}$ and so $\psi(-3+1\sqrt{2}) \neq 0+7\mathbb{Z}$. Hence, $-3+1\sqrt{2} \notin M_2$. Therefore, $M_1 \neq M_2$, as stated.

8. Give an explicit example of an injective ring homomorphism from $\mathbf{Z}/5\mathbf{Z}$ to $\mathbf{Z}/20\mathbf{Z}$. No justification of your answer is needed.

SOLUTION. We will justify the answer. One idempotent in the ring $\mathbb{Z}/20\mathbb{Z}$ is $16+20\mathbb{Z}$. This element is an idempotent because

$$(16+20\mathbb{Z})(16+20\mathbb{Z}) \;=\; 256+20\mathbb{Z} \;=\; 16+20\mathbb{Z} \quad .$$

Notice also that $16+20\mathbb{Z}$ has order 5 in the additive group of $\mathbb{Z}/20\mathbb{Z}$. We define a map $\varphi : \mathbb{Z} \to \mathbb{Z}/20\mathbb{Z}$ as follows:

$$\varphi(n) \;=\; 16n+20\mathbb{Z}$$

for $n \in \mathbb{Z}$. As discussed in class, this map φ is a ring homomorphism from $\mathbb{Z}/20\mathbb{Z}$. Since $16+20\mathbb{Z}$ has order 5, we have $Ker(\varphi) = 5\mathbb{Z}$. By the first isomorphism theorem, we obtain an injective ring homomorphism $\psi : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/20\mathbb{Z}$ defined by

$$\psi(n+5\mathbb{Z}) \;=\; 16n+20\mathbb{Z} \; .$$

9. Consider the ring $R = \mathbf{Q}[x]/I$, where $I = (x^2-x)$. Show that $\beta = x+I$ is an idempotent element in R, but that $\beta \neq 0_R$ and $\beta \neq 1_R$. Find an idempotent element in R which is not

equal to 0_R, 1_R or β. Prove that $R \cong \mathbb{Q} \times \mathbb{Q}$. (It may be helpful to review the exercises about idempotents.)

SOLUTION. We have $x^2 - x \in I$. Hence $x^2 + I = x + I$. Let $e = x + I$. Then

$$e^2 \;=\; (x+I)^2 \;=\; x^2 + I \;=\; x + I \;=\; e$$

and so e is an idempotent in the ring R. Let $f = 1_R - e = 1 - x + I$. Then f must also be an idempotent in the ring R. Furthermore, as proved in one of the problem sets, we have

$$R \;\cong\; S \times T$$

where $S = Re$ and $T = Rf$. We will show that $S \cong \mathbb{Q}$ and $T \cong \mathbb{Q}$.

Every element of R has the form $a + bx + I$, where $a, b \in \mathbb{Q}$. Thus, an element of S has the form

$$(a + bx + I)(x + I) \;=\; ax + bx^2 + I \;=\; (a + I)(x + I) + (b + I)(x^2 + I)$$

$$=\; (a + I)(x + I) + (b + I)(x + I) \;=\; (c + I)e$$

where $c = a + b \in \mathbb{Q}$. We define a map

$$\varphi : \mathbb{Q} \;\longrightarrow\; S$$

by $\varphi(c) = (c + I)e$ for all $c \in \mathbb{Q}$. Since all elements of S have the form $(c + I)e$, the map φ is surjective. One can then easily verify that φ is a ring isomorphism from $\mathbb{Q}$ to S. Hence $S \cong \mathbb{Q}$.

Similarly, an element of T has the form

$$(ax+b+I)(1-x+I) \;=\; ax(1-x)+b(1-x)+I \;=\; b(1-x)+I \;=\; (b+I)(1-x+I) \;=\; (b+I)f$$

Just as in the previous paragraph, we find that $T \cong \mathbb{Q}$. We have proved that $R \cong \mathbb{Q} \times \mathbb{Q}$.

An alternative proof can be given by noticing that x and $x - 1$ are relatively prime elements in the ring $\mathbb{Q}[x]$. One can use the chinese remainder theorem discussed in problem 6 to conclude that

$$\mathbb{Q}[x]/(x^2 - x) \;\cong\; \mathbb{Q}[x]/(x) \;\times\; \mathbb{Q}[x]/(x-1) \;\;.$$

Note that if $g(x) \in \mathbb{Q}[x]$ and $deg\big(g(x)\big) = 1$, then every element in the ring $\mathbb{Q}[x]/\big(g(x)\big)$ has the form $a + \big(g(x)\big)$, where $a \in \mathbb{Q}$. One can then define an isomorphism

$$\varphi :\; \mathbb{Q} \;\longrightarrow\; \mathbb{Q}[x]/\big(g(x)\big)$$

by $\varphi(a) = a + \big(g(x)\big)$ for all $a \in \mathbb{Q}$. Applying this observation, we then obtain

$$\mathbb{Q}[x]/(x) \;\cong\; \mathbb{Q}, \qquad\qquad \textit{and} \qquad\qquad \mathbb{Q}[x]/(x-1) \;\cong\; \mathbb{Q}$$

and hence we obtain an isomorphism $\mathbb{Q}[x]/(x^2 - x) \cong \mathbb{Q} \times \mathbb{Q}$.

10. This question concerns ring homomorphisms φ from a ring R to a ring S. In each part of this question, give an example of R, S, and φ satisfying the stated requirements. No explanations are needed. You must specify R, S, and φ precisely.

(a) R is a field, S is not a field, and φ is injective.

SOLUTION. We defined an injective ring homomorphism from $R = \mathbb{Z}/5\mathbb{Z}$ to $S = \mathbb{Z}/20\mathbb{Z}$ in problem 8. Note that R is a field and S is not an integral domain, hence S is certainly not a field.

Another example is the following. Let $R = \mathbb{Q}$ and let $S = \mathbb{Q}[x]$. Then R is a subring of S. Here R is a field, but S is not a field. The inclusion of R into S is an injective ring homomorphism.

(b) R and S are integral domains, φ is surjective, but not injective.

SOLUTION. Let $R = \mathbb{Z}$. Let $S = \mathbb{Z}/5\mathbb{Z}$. Then R is an integral domain and S is a field. Hence S is also an integral domain. Define $\varphi : R \to S$ by

$$\varphi(k) \;=\; k + 5\mathbb{Z}$$

for all $k \in \mathbb{Z}$. This map φ is a surjective ring homomorphism, but is not injective.

(c) R is a noncommutative ring, S is an integral domain, and φ is surjective.

SOLUTION. Let $R = \mathbb{H} \times \mathbb{Z}$, where $\mathbb{H}$ is the ring of quaternions. Let $S = \mathbb{Z}$. Every element r in R has the form $r = (h,\ z)$, where $h \in \mathbb{H}$ and $z \in \mathbb{Z}$. Define a map $\varphi : R \to S$ by

$$\varphi\big(\ (h,\ z)\ \big) \;=\; z$$

for all $h \in \mathbb{H}$ and $z \in \mathbb{Z}$. Then one verifies easily that φ is a ring homomorphism from R to S and that φ is surjective. Note that R is a noncommutative ring because $\mathbb{H}$ is noncommutative. Also, S is an integral domain.

11. Give a specific example of a prime ideal in the ring $\mathbf{Q}[x]$ which is not a maximal ideal.

SOLUTION. The zero ideal in $\mathbb{Q}[x]$ is a prime ideal because $\mathbb{Q}[x]$ is an integral domain. However, the zero ideal in $\mathbb{Q}[x]$ is not a maximal ideal because $\mathbb{Q}[x]$ is not a field.

12. This question concerns the ring $\mathbf{Z}[i]$. The integer 11213 is a prime number. Furthermore, it turns out that $11213 = 82^2 + 67^2$. You may use these facts in this question without verifying them.

(a) Find a maximal ideal I in the ring $\mathbf{Z}[i]$ which contains 11213. Explain why your ideal I is actually a maximal ideal in $\mathbf{Z}[i]$.

SOLUTION. Let $\alpha = 82 + 67i$. Then $N(\alpha) = 82^2 + 67^2 = 11213$, which is a prime number. Hence α is an irreducible element in the ring $\mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is a PID, it follows that the principal ideal $I = (\alpha)$ is a maximal ideal in the ring $\mathbb{Z}[i]$. Let $\beta = 82 - 67i$. Then I contains $\beta\alpha = 11213$. Thus, I is a maximal ideal which contains 11213.

(b) Find all of the irreducible elements α in $\mathbf{Z}[i]$ which divide 11213 in that ring.

SOLUTION. Since $11213 \equiv 1 \pmod 4$, we can use a result explained in class to find the irreducible elements in $\mathbb{Z}[i]$ which divide 11213. We have $11213 = (82+67i)(82-67i) = \alpha\beta$, where α and β are as in part (a). Both factors are irreducible in $\mathbb{Z}[i]$. There are eight irreducible elements of $\mathbb{Z}[i]$ which divide 11213. They are of the form $\varepsilon\alpha$ or $\varepsilon\beta$, where $\varepsilon \in \{1, -1, i, -i\}$. Explicitly, the irreducible elements of $\mathbb{Z}[i]$ dividing 11213 are:

$$\pm 82 \pm 67i, \qquad \pm 67 \pm 82i \quad .$$

(c) Prove that $\mathbf{Z}[i]/I$ is isomorphic to $\mathbf{Z}/11213\mathbf{Z}$.

SOLUTION. Let $p = 11213$. Since p is a prime and $p \equiv 1 \pmod 4$, we know that there exists an integer c such that $c^2 \equiv -1 \pmod p$. Let $F = \mathbb{Z}/p\mathbb{Z}$. We can define a map $\varphi : \mathbb{Z}[i] \to F$ as follows:

$$\varphi(a + bi) \;=\; a + bc \;+\; p\mathbb{Z} \quad .$$

We will show that φ is a surjective ring homomorphism. The surjectivity is clear. To verify that φ is a ring homomorphism, consider two elements $\kappa = a + bi$ and $\lambda = e + fi$ in $\mathbb{Z}[i]$. We have

$$\varphi(\kappa + \lambda) \;=\; \varphi(\,(a+e) + (b+f)i\,) \;=\; (a+e) \;+\; (b+f)c \;+\; p\mathbb{Z}$$

$$(a + bc) + (e + fc) \;+\; p\mathbb{Z} \;=\; \varphi(\kappa) + \varphi(\lambda)$$

Also,

$$\varphi(\kappa\lambda) \;=\; \varphi\big(\;(ae-bf)+(af+be)i\;\big) \;=\; (ae-bf)+(af+be)c \;+\; p\mathbb{Z}$$

and

$$\varphi(\kappa)\varphi(\lambda) \;=\; \big(a+bc+p\mathbb{Z}\big)\big(e+fc+p\mathbb{Z}\big) \;=\; (a+bc)(e+fc) \;+\; p\mathbb{Z}$$
$$=\; ae+bfc^2+afc+bec \;+\; p\mathbb{Z}$$

We have $c^2 \equiv -1 \pmod{p}$ and so $ae+bfc^2+afc+bec \equiv (ae-bf)+(af+be)c \pmod{p}$. Therefore,

$$\varphi(\kappa)\varphi(\lambda) \;=\; (ae-bf)+(af+be)c \;+\; p\mathbb{Z} \;=\; \varphi(\kappa\lambda) \;\;.$$

We have verified that φ is a surjective ring homomorphism. Let $K = ker(\varphi)$. By the first isomorphism theorem, we have

$$\mathbb{Z}[i]/K \;\cong\; F$$

where $F = \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/11213\mathbb{Z}$. Also, K is a maximal ideal of $\mathbb{Z}[i]$. Hence $K = (\gamma)$, where γ is an irreducible element of $\mathbb{Z}[i]$. Note that $\varphi(p) = p + p\mathbb{Z} = 0_F$. Hence p is in K. Therefore, γ divides p. By part **(b)**, we know that either $K = (\alpha) = I$ or $K = (\beta) = J$.

If $K = I$, then we have $\mathbb{Z}[i]/I \cong F$, as we want. On the other hand, assume that $K = J$. We can just switch the notation and take J to be the answer to part **(a)** in place of I.