# Problem Set 9 Solutions

Igor Rapinchuk

**1.** The polynomial that $\alpha$ satisfies is $f(x) = x^4 + 4x^2 + 64$. See Artin, pg 499, on how to find this polynomial.

**2.** Suppose $f(X) \in F[X]$ is a unit. Then there exists $g(X) \in F[X]$ such that $f(X)g(X) = 1$. Suppose $f(X) = a_m X^m + a_{m-1}X^{m-1} + \cdots + a_0$ and $g_n(X) = b_n X^n + b_{n-1}X^{n-1} + \cdots + b_0$. Then

$$f(X)g(X) = a_m b_n X^{m+n} + (\text{lower terms}) = 1$$

is impossible if $m + n > 0$ because $a_m b_n \neq 0$. So, $m = n = 0$, i.e. $f = a_0 \in F$ and $g = b_0 \in F$. Since $a_0 b_0 = 1$, $f = a_0$ is a unit in $F$, that is, $f$ is a nonzero element of $F$. Conversely, every nonzero element in $F$ is a unit in $F[x]$.

**3.** The given operation of addition on $R \times R'$ coincides with the operation on $R \times R'$ as the direct product of (abelian) groups $R$ and $R'$ with respect to addition. But we know that the direct product of abelian groups is an abelian groups, implying that $R \times R'$ is an abelian group with respect to the given operation of addition and verifying part (a) of Definition 10.1.3 on p. 346.

For any 3 elements $(a, a'), (b, b'), (c, c') \in R \times R'$ we have

$$((a, a')(b, b'))(c, c') = (ab, a'b')(c, c') = ((ab)c, (a'b')c')$$

and

$$(a, a')((b, b')(c, c')) = (a, a')(bc, b'c') = (a(bc), a'(b'c'))$$

But $R$ and $R'$ are rings, in particular, their multiplications are associative, implying that $(ab)c = a(bc)$ and $(a'b')c' = a'(b'c')$. It follows that

$$((a, a')(b, b'))(c, c') = (a, a')((b, b')(c, c')),$$

verifying associative law for multiplication on $R \times R'$. Next, if $1_R$ and $1_{R'}$ are multiplicative identities for $R$ and $R'$ then $(1_R, 1_{R'})$ is a multiplicative identity for $R \times R'$ because for any $(a, a') \in R \times R'$ we have

$$(1_R, 1_{R'})(a, a') = (1_R \cdot a, 1_{R'} \cdot a') = (a, a')$$

and

$$(a, a')(1_R, 1_{R'}) = (a \cdot 1_R, a' \cdot 1_{R'}) = (a, a')$$

This verifies part (b) of Definition 10.1.3.

For any 3 elements $(a, a'), (b, b'), (c, c') \in R \times R'$ we have

$$((a, a') + (b, b'))(c, c') = (a + b, a' + b')(c, c') = ((a + b)c, (a' + b')c') =$$
$$(ac + bc, a'c' + b'c') = (ac, a'c') + (bc, b'c') = (a, a')(c, c') + (b, b')(c, c')$$

and

$$(c, c')((a, a') + (b, b')) = (c, c')(a + b, a' + b') = (c(a + b), c'(a' + b')) =$$
$$(ca + cb, c'a' + c'b') = (ca, c'a') + (cb, c'b') = (c, c')(a, a') + (c, c')(b, b')$$

as both $R$ and $R'$ are rings, hence satisfy the distributive laws. Thus, $R \times R'$ satisfies both distributive laws, so part (c) of Definition 10.1.3 holds.

Thus, $R \times R'$ satisfies all three parts (a), (b) and (c) of Definition 10.1.3, so it is a ring.

**4.** Proof: Suppose $u \in I$ is a unit. This means that there exists $v \in R$ such that $vu = 1$. Since $I$ is an ideal of $R$, we have $vu \in I$, i.e. $1 \in I$. Then for any $a \in R$, we have $a = a \cdot 1 \in I$. Thus, $I = R$, the unit ideal.

**5.** Let $I \subset \mathbb{Z}[i]$ be a nonzero ideal. Pick a nonzero element $z = a + bi \in \mathbb{Z}[i]$. Consider $\bar{z} = a - bi \in \mathbb{Z}[i]$. Since $I$ is an ideal of $\mathbb{Z}[i]$, we have

$$\bar{z}z = a^2 + b^2 \in I.$$

So, $a^2 + b^2$ is a required nonzero integer in $I$.

**6.** (a) If

$$f(X, Y) = a_0 + b_1X + b_2Y + c_1X^2 + c_2XY + c_3Y^2 + \cdots$$

then $f(0, 0) = a_0$. So, $\ker \varphi$ consists of all polynomials with zero constant terms. Notice that such a polynomial $f(X, Y)$ can be written in the form $f(X, Y) = Xg(X, Y) + Yh(X, Y)$ for some $g, h \in \mathbb{R}[X, Y]$ (for example, the above polynomial when $a_0 = 0$ can be written as $f(X, Y) = X(b_1 + c_1X + c_2Y + \cdots) + Y(b_2 + c_3Y + \cdots)$). Conversely, any polynomial of the form $Xg(X, Y) + Yh(X, Y)$ has zero constant term. It follows that $\ker \varphi$ coincides with the ideal of $\mathbb{R}[X, Y]$ generated by $X$ and $Y$.

(b) **Lemma.** *If $f(X) \in F[X]$ and $c \in F$ is such that $f(c) = 0$ then $f(X) = (X-c)g(X)$ for some $g(X) \in F[X]$.*

**Proof.** By Euclid's algorithm, $f(X) = g(X)(X - c) + r(X)$, where either $r(X) = 0$ of $\deg r(X) < \deg (X - c) = 1$. So, in all cases, $r$ is a constant. Substituting $X = c$ gives

$$0 = f(c) = g(c)(c - c) + r \quad \Rightarrow r = 0$$

Thus, $f(X) = g(X)(X - c)$.

Now, suppose $f(X) \in \ker \varphi$. Then $f(2 + i) = 0$, so by the lemma $f(X) = (X - (2 + i))g(X)$ for some $g(X) \in \mathbb{C}[X]$. Observe that $f(2 - i) = 0$. Indeed,

$$f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_mX^m \quad \text{with} \quad a_i \in \mathbb{R}$$

Then for any $z \in \mathbb{C}$ we have

$$\overline{f(z)} = \overline{a_0 + a_1z + a_2z^2 + \cdots a_mz^m} = a_0 + a_1\bar{z} + a_2\bar{z}^2 + \cdots + a_m\bar{z}^m = f(\bar{z})$$

So, if $f(z) = 0$ then $f(\bar{z}) = 0$. In particular, $f(2 - i) = 0$. So,

$$0 = f(2 - i) = ((2 - i) - (2 + i))g(2 - i) = (-2i)g(2 - i) \quad \Rightarrow g(2 - i) = 0$$

Applying the lemma one more time, we obtain that $g(X) = (X - (2 - i))h(X)$ for some $h(X) \in \mathbb{C}[X]$. Then

$$f(X) = (X - (2 + i))g(X) = (X - (2 + i))(X - (2 - i))h(X) = (X^2 - 4X + 5)h(X)$$

Now, let us show that $h(X) \in \mathbb{R}[X]$. We have

$$f(X) = \overline{f(X)} = \overline{(X^2 - 4X + 5)h(X)} = (X^2 - 4X + 5)\overline{h(X)}$$

So,

$$(X^2 - 4X + 5)h(X) = (X^2 - 4X + 5)\overline{h(X)} \quad \Rightarrow (X^2 - 4X + 5)(h(x) - \overline{h(x)}) = 0$$

It follows that $h(X) = \overline{h(X)}$, and therefore $h(X) \in \mathbb{R}[X]$. Thus, $f(X) = (X^2 - 4X + 5)h(X)$ with $h(X) \in \mathbb{R}[X]$. Conversely, for $f(X) = (X^2 - 4X + 5)h(X)$ we have

$$f(2 + i) = ((2 + i)^2 - 4(2 + i) - 5)h(2 + i) = 0.$$

So, $\ker\varphi$ consists of all multiples of $X^2-4X+5$; thus, $\ker\varphi$ is the principal ideal generated by $X^2-4X+5$.

**7.** (a) By definition, $IJ$ consists of all finite sums $\sum_k i_k j_k$ where $i_k \in I$, $j_k \in J$. For any $i \in I$, $j \in J$ we have $ij \in I$ (because $I$ is an ideal) and $ij \in J$ (because $J$ is an ideal), implying that $ij \in I \cap J$. Since $I \cap J$ is an ideal, hence closed for addition, we have

$$\sum_k i_k j_k \in I \cap J \quad \text{for any} \quad i_k \in I, \quad j_k \in J$$

Thus, $IJ \subset I \cap J$. To prove the opposite inclusion $I \cap J \subset IJ$, we pick $u \in I$, $v \in J$ so that $u+v=1$. Let $x \in I \cap J$. Then

$$x = x \cdot 1 = x(u+v) = xu + xv \in IJ$$

because $xu \in IJ$ as $x \in J$ and $u \in I$, and $xv \in IJ$ as $x \in I$ and $v \in J$. This proves that $IJ = I \cap J$.

(b) Let $u \in I$ and $v \in J$ be such that $u+v=1$. Then

$$u \equiv 0 (\mathrm{mod}\, I) \quad \text{and} \quad u \equiv 1 (\mathrm{mod}\, J) \tag{1}$$

and

$$v \equiv 1 (\mathrm{mod}\, I) \quad \text{and} \quad v \equiv 0 (\mathrm{mod}\, J) \tag{2}$$

It follows from (1) that for any $b \in R$, one has

$$bu \equiv 0 (\mathrm{mod}\, I) \quad \text{and} \quad bu \equiv b (\mathrm{mod}\, J) \tag{3}$$

Similarly, it follows from (2) that for any $a \in R$, one has

$$av \equiv a (\mathrm{mod}\, I) \quad \text{and} \quad av \equiv 0 (\mathrm{mod}\, J) \tag{4}$$

Set $x = av + bu$. Then it follows from (3) and (4) that

$$x \equiv a (\mathrm{mod}\, I) \quad \text{and} \quad x \equiv b (\mathrm{mod}\, J),$$

so $x$ is a required element.

(c) Consider a map $\varphi\colon R \to R/I \times R/J$ defined by

$$\varphi(a) = (a+I, a+J).$$

We have

$$\varphi(a+b) = ((a+b)+I, (a+b)+J) = (a+I, a+J) + (b+I, b+J) = \varphi(a) + \varphi(b)$$

and

$$\varphi(ab) = ((ab)+I, (ab)+J) = (a+I, a+J)(b+I, b+J) = \varphi(a)\varphi(b),$$

so $\varphi$ is a ring homomorphism. It follows from part (b) that this homomorphism is surjective. Clearly, $\ker\varphi$ coincides with $I \cap J$. But by part (a), $I \cap J = IJ$, so $\ker\varphi = IJ$. Thus, $\varphi\colon R \to R/I \times R/J$ is a surjective ring homomorphism with kernel $IJ$. So, by the First Isomorphism Theorem,

$$R/IJ \simeq R/I \times R/J$$

**8.** By the Third Isomorphism Theorem for Rings, $R/M \simeq \overline{R}/\overline{M}$. Suppose, $M$ is maximal. Then $R/M$ is a field. So, $\overline{R}/\overline{M}$ is also a field, which means that $\overline{M}$ is maximal. Similarly, if $\overline{M}$ is maximal, we obtain that $M$ is maximal.

**9.** Let $\varphi\colon \mathbb{C}[X_1,\dots,X_n] \to R = \mathbb{C}[X_1,\dots,X_n]/I$ be the canonical homomorphism. Let $M \subset R$ be a maximal ideal. Set $J = \varphi^{-1}(M)$. Then $J$ is an ideal of $\mathbb{C}[X_1,\dots,X_n]$, and by Proposition 10.4.3,

$$\mathbb{C}[X_1,\dots,X_n]/J \simeq R/M \tag{5}$$

Since $M \subset R$ is maximal, $R/M$ is a field. Then $\mathbb{C}[X_1,\dots,X_n]/J$ is also a field, and therefore $J$ is a maximal ideal of $\mathbb{C}[X_1,\dots,X_n]$. By Theorem 10.7.6 (*Hilbert's Nullstellensatz*), there exists a point $a = (a_1,\dots,a_n) \in \mathbb{C}^n$ such that $J$ coincides with the kernel of the substitution map $s_a\colon \mathbb{C}[X_1,\dots,X_n] \to \mathbb{C}$ which sends $f(X)$ to $f(a)$. Since $s_a$ is obviously surjective, by the First Isomorphism Theorem we have

$$\mathbb{C}[X_1,\dots,X_n]/J = \mathbb{C}[X_1,\dots,X_n]/\ker s_a \simeq \operatorname{im} s_a = \mathbb{C}.$$

Then from (5), we conclude that $R/M \simeq \mathbb{C}$.

**10.** The ring obtained by by adjoining $\alpha$ satisfying $\alpha^2 = 1$ to $\mathbb{R}$ is $R = \mathbb{R}[X]/(X^2-1)$. Suppose we already have an isomorphism $\varphi\colon R \simeq \mathbb{R}\times\mathbb{R}$. Then $\varphi(\alpha) \in \mathbb{R}\times\mathbb{R}$ must satisfy

$$\varphi(\alpha)^2 = \varphi(\alpha^2) = \varphi(1) = 1_{\mathbb{R}\times\mathbb{R}} = (1,1)$$

This gives 4 possibilities for $\varphi(\alpha) : (\pm 1, \pm 1)$. But $\alpha \notin \mathbb{R}$, in particular, $\alpha \neq \pm 1$, implying that $\varphi(\alpha) \neq \pm 1_{\mathbb{R}\times\mathbb{R}}$, ruling out the possibilities $(1,1)$ and $(-1,-1)$ for $\varphi(\alpha)$. Both of the remaining possibilities $(1,-1)$ and $(-1,1)$ work in the sense that there are isomorphisms $R \simeq \mathbb{R}\times\mathbb{R}$ taking $\alpha$ to either of those elements. Let us show this for the element $(1,-1)$; the argument for the element $(-1,1)$ is similar.

Any element of $z \in R$ can be uniquely written in the form $z = a + b\alpha$ with $a, b \in \mathbb{R}$. If we want an isomorphism $\varphi\colon R \to \mathbb{R}\times\mathbb{R}$ to take 1 to $1_{\mathbb{R}\times\mathbb{R}} = (1,1)$ and $\alpha$ to $(1,-1)$ then (assuming that $\varphi$ is $\mathbb{R}$-linear) $z$ must be taken to $(a,a) + (b,-b) = (a+b, a-b)$. So, let us define a map $\varphi\colon R \to \mathbb{R}\times\mathbb{R}$ by

$$\varphi(a + b\alpha) = (a+b, a-b)$$

This map is a bijection, the inverse map being $\psi\colon \mathbb{R}\times\mathbb{R} \to R$ given by

$$\psi(u,v) = \frac{1}{2}((u+v) + (u-v)\alpha)$$

So, it remains to show that $\varphi$ is a ring homomorphism. We have

$$\varphi((a+b\alpha)+(c+d\alpha)) = \varphi((a+c)+(b+d)\alpha) = (a+c+b+d, a+c-b-d) =$$
$$= (a+b, a-b) + (c+d, c-d) = \varphi(a+b\alpha) + \varphi(c+d\alpha)$$

Next,

$$\varphi((a+b\alpha)(c+d\alpha)) = \varphi(ac + bc\alpha + ad\alpha + bd\alpha^2) = \varphi((ac+bd) + (ad+bc)\alpha) =$$
$$= (ac+bd+ad+bc, ac+bd-ad-bc) = (a+b, a-b)(c+d, c-d) =$$
$$= \varphi(a+b\alpha)\varphi(c+d\alpha)$$

So, $\varphi$ is a required isomorphism.