III.E. Homomorphisms of rings

Let R and S be rings.

III.E.1. DEFINITION. (i) A **ring homomorphism** $\varphi\colon R \to S$ is a map which is both a homomorphism of additive groups and multiplicative monoids: $\varphi(r_1+r_2) = \varphi(r_1)+\varphi(r_2)$, $\varphi(r_1r_2) = \varphi(r_1)\varphi(r_2)$, and $\varphi(1_R) = 1_S$.

(ii) A **ring isomorphism** is a homomorphism of rings which is injective and surjective. (Equivalently: there exists a homomorphism $\eta\colon S \to R$ such that $\eta \circ \varphi = \mathrm{id}_R$ and $\varphi \circ \eta = \mathrm{id}_S$.)

III.E.2. WARNING. In contrast to the case of groups, it is essential to include "$\varphi(1_R) = 1_S$" in III.E.1(i). This not only prohibits (say) multiplication-by-2 from giving a ring homomorphism from $\mathbb{Z}$ to $\mathbb{Z}$; it means that there is no such thing as a trivial (zero) ring homomorphism. Both $\mathbb{Z} \overset{\cdot 2}{\to} \mathbb{Z}$ and $\mathbb{Z} \overset{0}{\to} \mathbb{Z}$ are "rng homomorphisms".

III.E.3. PROPOSITION. (i) $\varphi(R)$ *is a subring of* S*, and*
(ii) $\ker(\varphi)$ $(:= \varphi^{-1}(\{0\}))$ *is a proper ideal in* R*.*

PROOF. (i) $\varphi(R)$ contains 1, and given $\alpha = \varphi(r_1)$, $\beta = \varphi(r_2) \in \varphi(R)$, we have $\alpha+\beta = \varphi(r_1+r_2) \in \varphi(R)$ and $\alpha\beta = \varphi(r_1r_2) \in \varphi(R)$.

(ii) Given $r \in R$ and $\kappa_1, \kappa_2 \in \ker(\varphi)$, we have $\varphi(\kappa_1+\kappa_2) = \varphi(\kappa_1)+\varphi(\kappa_2) = 0+0 = 0 \implies \kappa_1+\kappa_2 \in \ker(\varphi)$, and $\varphi(r\kappa_1) = \varphi(r)\varphi(\kappa_1) = \varphi(r)\cdot 0 = 0$ etc. $\implies r\kappa_1, \kappa_1 r \in \ker(\varphi)$. In particular, $-\kappa_1$ and $0\kappa_1 = 0$ are in $\ker(\varphi)$. Finally, $\ker(\varphi)$ is proper because it doesn't contain 1. □

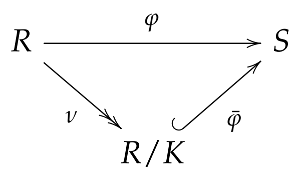
III.E.4. EXAMPLES. (i) "Evaluation" maps $\mathrm{ev}_r\colon R[x] \to R$ sending $P(x) \mapsto P(r)$ (or their products, as in III.A.3(iv)) are homomorphisms.

(ii) An injective homomorphism (or *embedding*) $\varphi\colon \mathbb{H} \hookrightarrow M_2(\mathbb{C})$ is obtained by sending $1 \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\mathbf{i} \mapsto \left(\begin{smallmatrix} \mathbf{i} & 0 \\ 0 & -\mathbf{i} \end{smallmatrix}\right)$, $\mathbf{j} \mapsto \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, and $\mathbf{k} \mapsto \left(\begin{smallmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{smallmatrix}\right)$. This gives an isomorphism of $\mathbb{H}$ with a subring of $M_2(\mathbb{C})$ (specifically, the one from III.C.25). The only thing to check is that the matrices behave "the same" as $\mathbf{i}, \mathbf{j}, \mathbf{k}$ under multiplication.

(iii) The natural map $\nu\colon R \twoheadrightarrow R/I$ sending $r \mapsto r + I$ (or "$\bar{r}$"), where $I \subset R$ is a proper ideal, is clearly consistent with III.E.3.

(iv) $\det\colon M_n(\mathbb{C}) \to \mathbb{C}$ is *not* a ring homomorphism. (Why?)

III.E.5. FUNDAMENTAL THEOREM OF RING HOMOMORPHISMS. *Given* $\varphi\colon R \to S$, *with* $K := \ker(\varphi)$, *there exists a unique ring homomorphism* $\bar{\varphi}\colon R/K \hookrightarrow S$ *making the diagram*



commute. In particular, the image $\varphi(R) \cong R/K$.

PROOF. By III.E.3(ii), R/K is well-defined as a ring; and by II.I.20, there exists a unique additive group homomorphism $\bar{\varphi}$ such that $\bar{\varphi} \circ \nu = \varphi$. It is only left to check that $\bar{\varphi}$ is a ring homomorphism: $\bar{\varphi}(\bar{r}_1\bar{r}_2) = \bar{\varphi}(\nu(r_1)\nu(r_2)) = \bar{\varphi}(\nu(r_1r_2)) = \varphi(r_1r_2) = \varphi(r_1)\varphi(r_2) = \bar{\varphi}(\nu(r_1))\bar{\varphi}(\nu(r_2)) = \bar{\varphi}(\bar{r}_1)\bar{\varphi}(\bar{r}_2)$. $\square$

III.E.6. EXAMPLES. (continuing III.D.21)
(i) Consider the evaluation map

$$\begin{aligned} \mathrm{ev}_{\sqrt{10}}\colon \mathbb{Z}[x] &\twoheadrightarrow \mathbb{Z}[\sqrt{10}] \\ \text{sending} \qquad P(x) &\longmapsto P(\sqrt{10}) \\ \text{and} \qquad x^2 - 10 &\longmapsto 0. \end{aligned}$$

Clearly $x^2 - 10 \in K$ and thus $(x^2 - 10) \subset K := \ker(\mathrm{ev}_{\sqrt{10}})$.

Conversely, if $P(\sqrt{10}) = 0$ and P is even, then $P(x) = Q(x^2)$ for some polynomial $Q(y)$, hence $Q(10) = 0 \implies y - 10 \mid Q(y) \implies x^2 - 10 \mid P(x)$ in $\mathbb{Z}[x]$. If P isn't even, then $P = P_1 + xP_2$ where $P_i(x) = Q_i(x^2)$ and $0 = Q_1(10) + \sqrt{10}Q_2(10) \implies$ again $x^2 - 10 \mid P(x)$. Invoking III.D.16 ("Caesar"), we get $(x^2 - 10) \supset K$. Conclude that

$$\frac{\mathbb{Z}[x]}{(x^2 - 10)} \cong \mathbb{Z}[\sqrt{10}].$$

(ii) If $\mathcal{M}$ is a manifold with submanifold[16] $\mathcal{S}$, then the restriction map

$$\begin{aligned} C^0(\mathcal{M}) &\twoheadrightarrow C^0(\mathcal{S}) \\ f &\longmapsto f|_{\mathcal{S}} \end{aligned}$$

is a surjective homomorphism, with kernel $K = I_{\mathcal{S}}$. So

$$C^0(\mathcal{S}) \cong \frac{C^0(\mathcal{M})}{I_{\mathcal{S}}}.$$

Similar isomorphisms show up in mathematics everywhere from coordinate rings (in algebraic geometry) to multiplier algebras (in operator theory).

(iii) Let's look at the map

$$\begin{aligned} \alpha\colon \mathbb{Z}[\sqrt{10}] &\twoheadrightarrow \mathbb{Z}_9 \\ \text{defined by}\quad a + b\sqrt{10} &\longmapsto \overline{a-b} \\ \text{(which sends}\quad 1 + \sqrt{10} &\longmapsto \bar{0}). \end{aligned}$$

Is this a homomorphism? It sends $1 \mapsto \bar{1}$, respects "+", and satisfies

$$\begin{aligned} \alpha\left((a+b\sqrt{10})(c+d\sqrt{10})\right) &= \alpha\left((ac+10bd)+(ad+bc)\sqrt{10}\right) \\ &= \overline{ac+10bd-(ad+bc)} \\ &= \overline{ac+bd-ad-bc} \\ &= (\overline{a-b})(\overline{c-d}) \\ &= \alpha(a+b\sqrt{10})\cdot\alpha(c+d\sqrt{10}), \end{aligned}$$

so yes. Clearly $(1+\sqrt{10}) \subset \ker(\alpha)$. Conversely,

$$\begin{aligned} a+b\sqrt{10} \in \ker(\alpha) \implies\ & a = b + 9n \quad (n \in \mathbb{Z}) \\ \implies\ & a + b\sqrt{10} = b(1+\sqrt{10}) + 9n \\ & \qquad = \left(b + n(-1+\sqrt{10})\right)(1+\sqrt{10}) \end{aligned}$$

[16] We will not get surjectivity if $\mathcal{S}$ is an arbitrary subset.

shows that $\ker(\alpha) \subset (1+\sqrt{10})$. Conclude that

$$\frac{\mathbb{Z}[\sqrt{10}]}{(1+\sqrt{10})} \cong \mathbb{Z}_9\,;$$

by a similar argument, we can replace $(1+\sqrt{10})$ by $(-1+\sqrt{10})$.

(iii′) What about

$$\begin{aligned} \beta\colon \mathbb{Z}[\sqrt{10}] &\twoheadrightarrow \mathbb{Z}_3 \times \mathbb{Z}_3 \\ a+b\sqrt{10} &\longmapsto (\overline{a+b}, \overline{a-b}) \\ 3 &\longmapsto (\bar{0}, \bar{0})\,? \end{aligned}$$

This sends $1 \mapsto (\bar{1}, \bar{1})$ and $(\overline{a+b}, \overline{a-b}) \cdot (\overline{c+d}, \overline{c-d}) =$ $(\overline{ac+bd+ad+bc},\, \overline{ac+bd-(ad+bc)}) = \beta((a+b\sqrt{10})(c+d\sqrt{10}))$.

So β is a homomorphism with $\ker(\beta) \supset (3)$. Moreover, $a \underset{(3)}{\equiv} b$ and $a \underset{(3)}{\equiv} -b \implies a \underset{(3)}{\equiv} 0 \underset{(3)}{\equiv} b \implies a+b\sqrt{10} \in (3)$. So

$$\frac{\mathbb{Z}[\sqrt{10}]}{(3)} \cong \mathbb{Z}_3 \times \mathbb{Z}_3.$$

(iii″) Finally, for

$$\begin{aligned} \gamma\colon \mathbb{Z}[\sqrt{10}] &\twoheadrightarrow \mathbb{Z}_3 \\ a+b\sqrt{10} &\longmapsto \overline{a-b} \\ 3 &\longmapsto \bar{0} \\ 1+\sqrt{10} &\longmapsto \bar{0} \end{aligned}$$

the general element of $\ker(\gamma)$ is $3n + b(1+\sqrt{10})$

$$\implies \quad \ker(\gamma) = (3, 1+\sqrt{10}) \quad \implies \quad \frac{\mathbb{Z}[\sqrt{10}]}{(3, 1+\sqrt{10})} \cong \mathbb{Z}_3.$$

(iv) For an example of a more general sort, consider (for any ring R)

$$\begin{aligned} \eta\colon \mathbb{Z} &\longrightarrow R \\ 0 &\longmapsto 0_R \\ 1 &\longmapsto 1_R \\ \mathbb{Z}_{>0} \ni n &\longmapsto 1_R + \cdots + 1_R \ \ (n \text{ times}) \\ -n &\longmapsto -(1_R + \cdots + 1_R). \end{aligned}$$

Clearly $\eta(n+m) = \eta(n) + \eta(m)$, and $\eta(nm) = \eta(n)\eta(m)$ (using distributivity). The image $\eta(\mathbb{Z})$ is called the **prime ring**, and is the smallest subring of R. Any ideal of $\mathbb{Z}$ is of the form (n), since these are (as we checked before) the additive subgroups. Conclude that $\eta(\mathbb{Z}) \cong \mathbb{Z}$ if $\text{char}(R) = 0$, and $\eta(\mathbb{Z}) \cong \mathbb{Z}_m$ if $\text{char}(R) = m$ is finite.

III.E.7. REMARK. Given a homomorphism $\varphi\colon R \to S$, we have

$$\begin{array}{ccccc} & & \mathbb{Z} & & \\ & {\scriptstyle \eta_R} \swarrow & & \searrow {\scriptstyle \eta_S} & \\ R & & \xrightarrow{\quad \varphi \quad} & & S\,, \end{array}$$

with $\bar{n} \overset{\varphi}{\mapsto} \bar{n}$. On the one hand, this implies $\text{char}(S) \mid \text{char}(R)$, which could rule out some homomorphisms. If $\text{char}(R) = 0$ it won't rule out anything, but here is something which could: if $\alpha \in R$ satisfies a polynomial equation $0 = \sum_k a_k \alpha^k$, $a_k \in \mathbb{Z}$ (i.e. $\eta_R(\mathbb{Z})$), we must have (writing $\beta := \varphi(\alpha)$) that $0 = \sum_k \bar{a}_k \beta^k$. One could then try to show that S doesn't contain such a β.

With essentially no work, the two isomorphism theorems from §II.I lift to the ring setting:

III.E.8. FIRST ISOMORPHISM THEOREM. *Let $\varphi\colon R \twoheadrightarrow S$ be a surjective ring homomorphism with kernel K. Then φ induces a 1-to-1 correspondence*

$$\left\{\begin{matrix}\text{ideals } I \subset R \\ \text{containing } K\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{ideals} \\ J \subset S\end{matrix}\right\}$$
$$\textit{via} \quad I \quad \longmapsto \quad \varphi(I)\ ,$$

and isomorphisms $R/I \stackrel{\cong}{\to} S/\varphi(I)$.

PROOF. We only need to check that $\varphi(I)$ and $\varphi^{-1}(J)$ are closed under multiplication by R; the rest follows from II.I.25 and III.E.5.

Given $I \subset R$, $S\varphi(I) = \varphi(R)\varphi(I) = \varphi(RI) = \varphi(I) \implies \varphi(I)$ is an ideal.

Given $J \subset S$, $\alpha \in \varphi^{-1}(J)$, and $r \in R$, we have $\varphi(r\alpha) = \varphi(r)\varphi(\alpha) \in SJ = J \implies r\alpha \in \varphi^{-1}(J) \implies \varphi^{-1}(J)$ is an ideal. □

III.E.9. SECOND ISOMORPHISM THEOREM. *Given $I \subset R$ an ideal and $S \subset R$ a subring. Then:*
(i) *$S + I \subset R$ is a subring having I as an ideal;*
(ii) *$S \cap I$ is an ideal in S; and*
(iii) *$s + (S \cap I) \mapsto s + I$ induces an isomorphism $S/(S \cap I) \stackrel{\cong}{\to} (S+I)/I$.*

PROOF. Left to you. □

III.E.10. EXAMPLE. (i) Referring to Example III.E.6(iii), we can apply III.E.8 to $\alpha\colon \mathbb{Z}[\sqrt{10}] \twoheadrightarrow \mathbb{Z}_9$ to determine ideals in $R := \mathbb{Z}[\sqrt{10}]$. Since $S := \mathbb{Z}_9$ contains one nontrivial proper ideal (namely $(\bar{3})$), R contains one proper ideal containing (but $\neq$) $(1+\sqrt{10})$. Clearly, this is $(3, 1+\sqrt{10})$, and so we get for free

$$\frac{\mathbb{Z}[\sqrt{10}]}{(3, 1+\sqrt{10})} \cong \frac{\mathbb{Z}_9}{\mathbb{Z}_3} \cong \mathbb{Z}_3.$$

(ii) With the same R, take $S := \mathbb{Z} \subset R$ and $I = (1+\sqrt{10}) \subset R$. Clearly $S + I = R$, and applying III.E.9 gives

$$\frac{\mathbb{Z}}{\mathbb{Z} \cap (1+\sqrt{10})} \cong \frac{\mathbb{Z}[\sqrt{10}]}{(1+\sqrt{10})},$$

which we know is $\cong \mathbb{Z}_9$. Conclude that $\mathbb{Z} \cap (1+\sqrt{10}) = (9)$.

Here is a more interesting application of the Fundamental Theorem III.E.5.

III.E.11. DEFINITION. We say that two ideals $I, J \subset R$ are **relatively prime** (or **coprime**) if $I + J = R$, or equivalently that there exist elements $\imath \in I$ and $\jmath \in J$ such that $\imath + \jmath = 1$. (You should check that in $\mathbb{Z}$, (m) and (n) are relatively prime iff m and n are, i.e. $\gcd(m,n) = 1$.)

III.E.12. CHINESE REMAINDER THEOREM. *Let $I_1, \ldots, I_m$ be pairwise relatively prime ideals in a ring R; that is, for each $i \neq j$, $I_i + I_j = R$. Then*

$$R/(\cap_{j=1}^{m} I_j) \cong R/I_1 \times \cdots \times R/I_m.$$

PROOF. Clearly

$$\begin{aligned} \varphi \colon R &\longrightarrow R/I_1 \times \cdots \times R/I_m \\ r &\longmapsto (r + I_1, \ldots, r + I_m) \end{aligned}$$

is a homomorphism. We must show that it is surjective with kernel $\cap_{j=1}^{m} I_j =: I$, and then the Fundamental Theorem does the rest of the work.

Suppose the result is known for less than m ideals (with $m \geq 3$). Then setting $I' := \cap_{j=2}^{m} I_j$, we have $R/I' \cong \times_{j=2}^{m} R/I_j$. By assumption, for each pair I_1 and I_j we have elements $\alpha_j \in I_1$ and $\beta_j \in I_j$ such that $\alpha_j + \beta_j = 1$. Hence,[17]

$$1 = \prod_{j=2}^{m} (\alpha_j + \beta_j) \in \prod_{j=2}^{m} (I_1 + I_j) \subset I_1 + I_2 \cdots I_m \subset I_1 + I'$$

[17]Note that all terms of the product $\prod_{j=2}^{m}(I_1 + I_j)$ are contained in I_1 except for the term $I_2 \cdots I_m$.

$\implies I_1 + I' = R$. Hence $R/I \cong R/I' \times R/I_1$ as desired.

What remains is to check the $m = 2$ case. First, $\ker(\varphi)$ consists of those $r \in R$ with $\varphi(r) = (0 + I_1, 0 + I_2)$, or equivalently, $r \in I_1 \cap I_2$.

For surjectivity of φ: given $\mathfrak{a} := (a + I_1, b + I_2) \in R/I_1 \times R/I_2$, $I_1 + I_2 = R \implies$ there exist $\imath_1 \in I_1$, $\imath_2 \in I_2$ such that $a - b = -\imath_1 + \imath_2$ $\implies a + \imath_1 = b + \imath_2 =: r$, with $\varphi(r) = \mathfrak{a}$. □

III.E.13. REMARK. (i) More explicitly, the Theorem is saying that if $r_1, \ldots, r_m$ are elements of R, and $I_1, \ldots, I_m$ pairwise coprime, then:

- there exists an $r \in R$ such that $r \equiv r_i \bmod I_i$ for every i; and
- this r is unique up to the addition of elements in $I_1 \cap \cdots \cap I_m$.

(ii) *If R is commutative and I_1 and I_2 are relatively prime*, with $\alpha \in I_1$ and $\beta \in I_2$ such that $\alpha + \beta = 1$, then $a \in I_1 \cap I_2 \implies a = a(\alpha + \beta) = \alpha a + b\beta \in I_1 I_2$. Conversely, it is immediate that $I_1 I_2 \subset I_1 \cap I_2$; and so $I_1 I_2 = I_1 \cap I_2$. From here, its obviously true for $m > 2$ as well: if R is commutative and the I_j are pairwise coprime, then

$$I_1 \cap \cdots \cap I_m = I_1 \cdots I_m.$$

The original form of III.E.12 is a result about congruences in number theory, a version of which of which was discovered by Sun Tzu in the 3rd Century.

III.E.14. COROLLARY. *Let $k_1, \ldots, k_m$ be pairwise coprime integers; that is, $(k_i, k_j) = 1$ ($\forall i \neq j$). Then*[18]

$$\mathbb{Z}/k_1 \cdots k_m \mathbb{Z} \xrightarrow{\cong} \mathbb{Z}/k_1\mathbb{Z} \times \cdots \times \mathbb{Z}/k_m\mathbb{Z}.$$

Taking units on both sides recovers the results on units in $\mathbb{Z}/m\mathbb{Z}$ from II.E.13-II.E.14.

But one needn't apply the Chinese Remainder Theorem only to integers:

[18] or if you prefer, $\mathbb{Z}_{k_1 \cdots k_m} \cong \mathbb{Z}_{k_1} \times \cdots \times \mathbb{Z}_{k_m}$.

III.E.15. EXAMPLE. In $R = \mathbb{Z}[\sqrt{10}]$, the ideals $I_1 = (1 + \sqrt{10})$ and $I_2 = (-1 + \sqrt{10})$ are coprime, in view of

$$(1 + \sqrt{10})(-1 + \sqrt{10}) - 4(1 + \sqrt{10}) + 4(-1 + \sqrt{10}) = 1.$$

Moreover, $I_1 I_2 = (9)$. So

$$\frac{\mathbb{Z}[\sqrt{10}]}{(9)} \cong \frac{\mathbb{Z}[\sqrt{10}]}{(1 + \sqrt{10})} \times \frac{\mathbb{Z}[\sqrt{10}]}{(-1 + \sqrt{10})} \cong \mathbb{Z}_9 \times \mathbb{Z}_9.$$