MATH3030 Tutorial 8 (Online)

J. SHEN

9 November, 2023

8 Basic theorems of ring theory

8.1 Properties of ring homomorphisms

Proposition 8.1 (Fraleigh 8th ed. thm 30.11)**.** *Let R be a ring (with 1, not assuming commutativity). Let $\phi : R \to R'$ be a ring homomorphism. Then*

1. $\phi(0) = 0$
2. *For any $a \in R$, $\phi(-a) = -\phi(a)$.*
3. *If S is a subring of R, then $\phi(S)$ is a subring of R'*
4. *If S' is a subring of R', then $\phi^{-1}(S')$ is a subring of R.*
5. *If N is an ideal of R, then $\phi(N)$ is an ideal of $\phi(R)$.*
6. *If N' is an ideal of either R' or $\phi(R)$, then $\phi^{-1}(N')$ is an ideal of R. (Ideals mean two-sided ideals.)*

PROOF.

8.2 First isomorphism theorem

Proposition 8.2 (First isomorphism theorem, Artin 11.4.2, Fraleigh 7th 26.17, 8th 30.17)**.** *Let $\phi : R \to R'$ be a ring homomorphism. Then $\phi^{-1}(0) \subseteq R$ is an ideal. Moreover, ϕ induces $\overline{\phi} : R/\phi^{-1}(0) \to \phi(R)$, which is an isomorphism and which satisfies the following commutative diagram:*

More generally, given ideal $I \subseteq \phi^{-1}(0)$, there exists a unique $\overline{\phi} : R/I \to R'$ satisfying $\phi = \overline{\phi} \circ \pi$, where $\pi : R \to R/I$ is the natural surjection $r \mapsto r + I$.

8.3 Correspondence theorem

The following theorem is called the correspondence theorem, or the fourth isomorphism theorem, and is quite useful in identifying rings.

Proposition 8.3 (Artin 11.4.3). *Let $\phi : R \to R'$ be a surjective homomorphism with kernel K. Then there is an order-preserving bijection between*

$\{$*Ideals of* R *containing* $K\} \longleftrightarrow \{$*Ideals of* $R'\}$*, given by*

$\alpha : I \mapsto \phi(I)$*, and* $\beta : \phi^{-1}(I') \leftarrow\!\shortmid I'$

Moreover, $R/I \simeq R'/I'$ *if* $I \leftrightarrow I'$.

Exercise 1. (Artin Q11.4.3) Identify the following rings: **(a)** $\mathbb{Z}[x]/(x^2-3, 2x+4)$, **(b)** $\mathbb{Z}[i]/(2+i)$, **(c)** $\mathbb{Z}[x]/(6, 2x-1)$, **(d)**$\mathbb{Z}[x]/(2x^2-4, 4x-5)$, **(e)** $\mathbb{Z}[x]/(x^2+3, 5)$.

Exercise 2. (Artin Q11.4.4) Are the rings $\mathbb{Z}[x]/(x^2+7)$ and $\mathbb{Z}[x]/(2x^2+7)$ isomorphic?

MATH3030 Tutorial 8 (Online)

J. SHEN

9 November, 2023

8 Basic theorems of ring theory

8.1 Properties of ring homomorphisms

Proposition 8.1 (Fraleigh 8th ed. thm 30.11). *Let R be a ring (with 1, not assuming commutativity). Let $\phi : R \to R'$ be a ring homomorphism. Then*

1. $\phi(0) = 0$
2. *For any $a \in R$, $\phi(-a) = -\phi(a)$.*
3. *If S is a subring of R, then $\phi(S)$ is a subring of R'*
4. *If S' is a subring of R', then $\phi^{-1}(S')$ is a subring of R.*
5. *If N is an ideal of R, then $\phi(N)$ is an ideal of $\phi(R)$.*
6. *If N' is an ideal of either R' or $\phi(R)$, then $\phi^{-1}(N')$ is an ideal of R. (Ideals mean two-sided ideals.)*

Proof. Property 1 and 2 follows from $\phi : (R, +) \to (R', +')$ being a group homomorphism.

3. Since S is a subring of R, it is closed under $-, \times$, and $1_R \in S$. Then for $x, y \in \phi(S)$, there exist $a, b \in S$ such that $\phi(a) = x, \phi(b) = y$. Then $a - b, ab \in S$, and so $x - y = \phi(a - b) \in \phi(S)$, and $xy = \phi(ab) \in \phi(S)$. Moreover, $1_{R'} = \phi(1_R) \in \phi(S)$. It follows that $\phi(S)$ is a subring of R'.

4. Let S' be a subring of R'. Then it is closed under $-, \times$, and $1_{R'} \in S'$. For $a, b \in \phi^{-1}(S')$, $\phi(a), \phi(b) \in S'$. Then $\phi(a - b) = \phi(a) - \phi(b) \in S'$ and $\phi(ab) = \phi(a)\phi(b) \in S'$. Since $\phi(1_R) = 1_{R'} \in S'$, $1_R \in \phi^{-1}(S')$. Therefore, $\phi^{-1}(S')$ is a subring of R.

5. Since N is an ideal of R, it is an additive subgroup of R, and for $r \in R$, $n \in N$, $rn, nr \in N$. Then $\phi(N)$ is an additive subgroup of $\phi(R)$ and for $x \in \phi(R)$, $y \in \phi(N)$, there exists $r \in R, n \in N$ such that $\phi(r) = x, \phi(n) = y$. Then $xy =$

$\phi(r)\phi(n) = \phi(rn) \in \phi(N)$, and $yx = \phi(n)\phi(r) = \phi(nr) \in \phi(N)$. Then, $\phi(N)$ is an ideal of $\phi(R)$.

6. If N' is an ideal of R', then it is also an ideal of $\phi(R)$. So we suppose N' is an ideal of $\phi(R)$. Then $\phi^{-1}(N')$ is an additive subgroup of R. Let $r \in R, n \in \phi^{-1}(N')$, $\phi(r) \in \phi(R)$ and $\phi(n) \in N'$. Then $\phi(rn) = \phi(r)\phi(n) \in N'$, $\phi(nr) = \phi(n)\phi(r) \in N'$. Then $rn, nr \in \phi^{-1}(N')$. It follows that $\phi^{-1}(N')$ is an ideal of R.

8.2 First isomorphism theorem

Proposition 8.2 (First isomorphism theorem, Artin 11.4.2, Fraleigh 7th 26.17, 8th 30.17)**.** *Let $\phi : R \to R'$ be a ring homomorphism. Then $\phi^{-1}(0) \subseteq R$ is an ideal. Moreover, ϕ induces $\overline{\phi} : R/\phi^{-1}(0) \to \phi(R)$, which is an isomorphism and which satisfies the following commutative diagram:*

More generally, given ideal $I \subseteq \phi^{-1}(0)$, there exists a unique $\overline{\phi} : R/I \to R'$ satisfying $\phi = \overline{\phi} \circ \pi$, where $\pi : R \to R/I$ is the natural surjection $r \mapsto r + I$.

Proof. Let $\phi : R \to R'$ be a ring homomorphism. That $\phi^{-1}(0) \subseteq R$ is an ideal follows from part 6 of the previous proposition. By the group version of the 1st isomorphism theorem, ϕ induces $\overline{\phi} : R/\phi^{-1}(0) \to \phi(R)$, which is an additive group isomorphism, such that $\overline{\phi}(\overline{r}) = \phi(r)$ for each $r \in R$. It remains to show that $\overline{\phi}$ is a ring homomorphism. Clearly, $\overline{\phi}(\overline{1_R}) = \phi(1_R) = 1_{R'}$. For $r, r' \in R$, $\overline{\phi}(\overline{r} \cdot \overline{r'}) = \overline{\phi}(\overline{rr'}) = \phi(rr') = \phi(r)\phi(r') = \overline{\phi}(\overline{r})\overline{\phi}(\overline{r'})$. Then ϕ is a ring isomorphism.

The second statement is proved by defining $\overline{\phi}(\overline{r}) = \phi(r)$ and verifying that $\overline{\phi}$ is well-defined and is a ring homomorphism satisfying $\phi = \overline{\phi} \circ \pi$.

8.3 Correspondence theorem

The following theorem is called the correspondence theorem, or the fourth isomorphism theorem, and is quite useful in identifying rings.

Proposition 8.3 (Artin 11.4.3)**.** *Let $\phi : R \to R'$ be a surjective homomorphism with kernel K. Then there is an order-preserving bijection between*

$\{$Ideals of R containing $K\} \longleftrightarrow \{$Ideals of $R'\}$, given by

$\alpha : I \mapsto \phi(I)$, and $\beta : \phi^{-1}(I') \leftarrow\!\shortmid I'$

Moreover, $R/I \simeq R'/I'$ if $I \leftrightarrow I'$.

PROOF. Let $\phi : R \to R'$ be a surjective homomorphism with kernel K. Let $S =\{I$: I is an ideal of R containing $K\}$, and $S' =\{I'$: I' is an ideal of $R'\}$. For $I \in S$, $\phi(I)$ is an ideal of R' by property 5 in 8.1. Then $\alpha : I \mapsto \phi(I)$ defines a map from S to S'. For $I' \in S'$, $\phi^{-1}(I')$ is an ideal of R by property 6 in 8.1. Clearly $K \subseteq \phi^{-1}(I')$. Then β defines a map from S' to S. For $I_1 \subseteq I_2$, $I_1, I_2 \in S$, $\alpha(I_1) = \phi(I_1) \subseteq \phi(I_2) = \alpha(I_2)$. Therefore, α is order-preserving. Similarly, β is also order-preserving.

For $I \in S$, $\beta \circ \alpha(I) = \phi^{-1}(\phi(I)) \supseteq I$. For $a \in \phi^{-1}(\phi(I))$, $\phi(a) \in \phi(I)$. Then there exists some $b \in I$ such that $\phi(a) = \phi(b)$. Then $\phi(a-b) = 0$ and $a-b \in K \subseteq I$. Then $a = a-b+b \in I$. Therefore, $\beta \circ \alpha(I) = \phi^{-1}(\phi(I)) = I$. Since I was arbitrarily chosen, $\beta \circ \alpha = \mathrm{id}_S$.

For $I' \in S'$, $\alpha \circ \beta(I') = \phi(\phi^{-1}(I')) = I' \cap \phi(R) = I' \cap R' = I'$ since ϕ is surjective. Then $\alpha \circ \beta = \mathrm{id}_{S'}$.

Therefore, α and β defines a correspondence (i.e. bijection) between S and S'.

For $I \in S$, let $I' = \alpha(I)$. Then the natural projection $\pi : R' \to R'/I'$ is a surjective ring homomorphism. Since ϕ is also a surjective homomorphism, so is $\psi := \pi \circ \phi : R \to R'/I'$. Let $r \in R$. Then $r \in \ker(\psi) \iff \pi(\phi(r)) = 0 \iff \phi(r) \in I' \iff r \in \beta(I') = \beta\alpha(I) = I$. Then $\ker(\psi) = I$. Since ψ is a surjective ring homomorphism, ψ induces a ring isomorphism $\overline{\psi} : R/I \to R'/I'$ by $\overline{r} \mapsto \psi(r) = \pi \circ \phi(r) = \overline{\phi(r)}$.

Exercise 1. (Artin Q11.4.3) Identify the following rings: **(a)** $\mathbb{Z}[x]/(x^2-3, 2x+4)$, **(b)** $\mathbb{Z}[i]/(2+i)$, **(c)** $\mathbb{Z}[x]/(6, 2x-1)$, **(d)**$\mathbb{Z}[x]/(2x^2-4, 4x-5)$, **(e)** $\mathbb{Z}[x]/(x^2+3, 5)$.

Our strategy is to use the correspondence theorem, which states that if $\phi : R \to R'$ is surjective, and $I \supset \ker(\phi)$, then $R/I \simeq R'/\phi(I)$. We will often choose $\ker(\phi)$ to be $(x-r)$ or (m) for some $r, m \in \mathbb{Z}$.

There is a useful property of a surjective homomorphism ϕ: $\phi((x_1, x_2, ..., x_n)) = (\phi(x_1), \phi(x_2), ..., \phi(x_n))$. The proof is straightforward, and we will use this without further explanation.

Answer. (a) Let $R = \mathbb{Z}[x]$, $I = (x^2-3, 2x+4)$. Then $2x^2+4x \in I$, $4x+6 = 2x^2+4x-2(x^2-3) \in I$, and $2 = 2(2x+4)-(4x-6) \in I$. Let $R' = R/(2) = \mathbb{F}_2[x]$. Let $\phi : R \to R'$ be the natural projection. Then $\phi(I) = (\phi(x^2-3), \phi(2x+4)) = (x^2+1)$, and $I \supseteq \ker(\phi) = (2)$. Then I corresponds to $\phi(I)$ as in the correspondence theorem, so $R/I \simeq R'/\phi(I) = \mathbb{F}_2[x]/(x^2+1) = \mathbb{F}_2[x]/(x+1)^2$.

(b) Let $R = \mathbb{Z}[x]$. The evaluation homomorphism $\phi : \mathbb{Z}[x] \to \mathbb{Z}[i]$ with $\phi(x) = i$ is surjective with $\ker(\phi) = (x^2+1)$. Let $I = (x^2+1, 2+x)$, then $I \supseteq \ker(\phi)$ and $\phi(I) = (0, 2+i)$. Then by the correspondence theorem, $R/I \simeq \mathbb{Z}[i]/(2+i)$.

Let $\psi : R \to \mathbb{Z}$ be the evaluation map such that $\phi(x) = -2$. Then ψ is surjective, $\ker(\psi) = (x+2) \subseteq I$, and $\phi(I) = ((-2)^2+1, -2+2) = (5)$. By the correspondence theorem, $R/I \simeq \mathbb{Z}/(5) \simeq \mathbb{F}_5$.

(c) Let $R = \mathbb{Z}[x]$, and $I = (6, 2x-1)$. Then $3 = 6x - 3(2x-1) \in I$. Let $R' = \mathbb{F}_3[x]$ and $\phi : R \to R'$ be the natural projection. Then $\ker(\phi) = (3) \subseteq I$, and $\phi(I) = (0, -x-1) = (x+1)$. Then by the correspondence theorem, $R/I \simeq \mathbb{F}_3[x]/(x+1) \simeq \mathbb{F}_3$.

(d) Let $R = \mathbb{Z}[x]$, and $I = (2x^2-4, 4x-5)$. Then $5x - 8 = 2(2x^2-4) - x(4x-5) \in I$. Then $x - 3 = 5x - 8 - (4x-5) \in I$. Let $\phi : R \to \mathbb{Z}$ be the evaluation map with $\phi(x) = 3$. Then $\ker(\phi) = (x-3) \subseteq I$, ϕ is surjective, and $\phi(I) = (2 \cdot 3^2 - 4, 4 \cdot 3 - 5) = (14, 7) = (7)$. By the correspondence theorem, $R/I \simeq \mathbb{Z}/(7) \simeq \mathbb{F}_7$.

(e) Let $R = \mathbb{Z}[x]$, $I = (x^2+3, 5)$, and let $\phi : R \to \mathbb{F}_5[x]$ be the natural projection. Then $\ker(\phi) = (5) \subseteq I$, and $\phi(I) = (x^2+3, 0)$. By the correspondence theorem, $\mathbb{Z}[x]/I \simeq \mathbb{F}_5[x]/(x^2+3)$.

Note that x^2+3 is irreducible, $\mathbb{F}_5[x]/(x^2+3)$ is a field of 25 elements, that is $\mathbb{Z}[x]/I \simeq \mathbb{F}_{25}$.

Exercise 2. (Artin Q11.4.4) Are the rings $\mathbb{Z}[x]/(x^2+7)$ and $\mathbb{Z}[x]/(2x^2+7)$ isomorphic?

Proof. No. The two rings are not isomorphic. We give a proof.

Suppose there is a ring isomorphism $\phi : \mathbb{Z}[x]/(2x^2+7) \to \mathbb{Z}[x]/(x^2+7)$. Then $\phi(1) = 1$, and $\phi(x) = ax + b$ for some $a, b \in \mathbb{Z}$. Then $0 = \phi(2x^2+7) = 2(ax+b)^2 + 7 = 2a^2x^2 + 4abx + 2b^2 + 7 = 4abx + 2b^2 + 7 - 14a^2$ in $\mathbb{Z}[x]/(x^2+7)$. Then $4ab = 2b^2 + 7 - 14a^2 = 0$. Since $a, b \in \mathbb{Z}$, $14a^2 = 2b^2 + 7 > 0$. Then $a \neq 0$. Then $b = 0$ by $4ab = 0$, and so $7 = 14a^2$. There is no solution where $a \in \mathbb{Z}$. Contradiction arises. Therefore, the two rings are not isomorphic.