The Chinese University of Hong Kong, Shenzhen
SSE · School of Science and Engineering

Yuanxin Guo · Fall Semester 2021/22

MAT 3004 – Abstract Algebra I

Tutorial 9

Noether's Isomorphism Theorems In abstract algebra, we are always interested in quotient structures. Noether's Isomorphism Theorems (in memory of the female mathematician Emmy Noether) provides a series of results that describe the isomorphic relationship of these objects. Versions of these theorems exist for groups, rings, vector spaces, modules, Lie algebras, and various other algebraic structures. We here describe the theorem for rings.

Theorem 1 (Isomorphism Theorems for Rings).

a) (First Isomorphism Theorem) Let $\phi : R \to S$ be a homomorphism of rings. Then $R/\ker(\phi) \cong \mathrm{im}(\phi)$.
b) (Second Isomorphism Theorem) Let R be a ring, S be a subring of R, I be an ideal of R. Then $(S+I)/I \cong S/(S \cap I)$.
c) (Third Isomorphism Theorem) Let R be a ring, I, J be ideals such that $I \subset J \subset R$, then $(R/I)/(J/I) \cong R/J$.
d) (Correspondence Theorem)[1] Let R be a ring, I be an ideal. Then there is a one-to-one correspondence:

$$\{\text{ideals of } R \text{ containing } I\} \leftrightarrow \{\text{ideals of } R/I\}$$

The first isomorphism theorem is introduced in class, and the corresponding theorem is proven in Homework 8. We hence focus on the Second and the Third Isomorphism Theorems. We need the following preliminary result:

Lemma 2 (Universal Property of Quotient Rings). Let R be a ring, I be an ideal. and let $\pi : R \to R/I$ be the canonical projection onto the quotient ring. Let $\phi : R \to S$ be a ring homomorphism such that $I \subset \ker(\phi)$, then there exists a **unique** homomorphism $\psi : R/I \to S$ such that $\phi = \psi \circ \pi$ and $\ker(\psi) = \ker(\phi)/I$. We can express this statement in terms of a commutative diagram:

$$\begin{tikzcd}
R \arrow[r, "\pi"] \arrow[dr, "\phi"'] & R/I \arrow[d, dashed, "\exists!\,\psi"] \\
& S
\end{tikzcd}$$

In other words, the canonical projection is **universal** among ring homomorphisms on R that map I to the identity.

[1] In fact, in another version of this theorem, we have an one-to-one correspondence between subrings of R containing I and subrings of R/I. Check `https://proofwiki.org/wiki/Fourth_Isomorphism_Theorem` for more details.

Exercise E9.1 (A walk through the isomorphism theorems):
In this exercise, we aim to first prove the lemma, then use it to prove the isomorphism theorems.

a) For the lemma, show that by defining $\psi(r + I) = \phi(r)$ we obtain a well-defined ring homomorphism such that $\phi = \psi \circ \pi$ and $\ker(\psi) = \ker(\phi)/I$.
b) Directly apply this lemma to prove the First Isomorphism Theorem.
c) For the second isomorphism theorem, show by the definition of subrings and ideals that
   - $S + I$ is a subring of R
   - I is an ideal of $S + I$
d) Apply the First Isomorphism Theorem to the canonical projection map restricted on S: $\pi|_S : S \to R/I$. Prove that the Second Isomorphism Theorem holds.
e) For the Third Isomorphism Theorem, show that there exists a ring homomorphism $\psi : R/I \to R/J$ such that $\pi_J = \psi \circ \pi_I$ where $\pi_I : R \to R/I$ and $\pi_J : R \to R/J$ are canonical projections.
f) Apply the First Isomorphism Theorem to ψ constructed in (e) and prove the Third Isomorphism Theorem.

As we have pointed out, ideals are ring analogues of normal subgroups. These isomorphism theorems also have a group theory version, with normal subgroups substituting ideals, subgroups substituting subrings. Try to formulate them on your own and compare your formulation with Wikipedia.

Some constructions of rings We now seek for some connections between rings and algebraic structures that we are familiar with.

Exercise E9.2 (Endomorphism rings):
Let G be an abelian group. Then define

$$\mathrm{End}(G) = \{\phi : G \to G \text{ homomorphism}\}$$

a) Show that with addition being pointwise addition and multiplication being composition, $\mathrm{End}(G)$ forms a unital ring. What is the identity and the unity of this ring?
b) We now show that when G is not abelian, $\mathrm{End}(G)$ need not be a group. Let $G = S_3$ and define homomorphisms $\phi, \psi : S_3 \to S_3$ by

$$\phi(\sigma) = \begin{cases} (1\,2), & \sigma \text{ is a transposition} \\ (1), & \text{otherwise} \end{cases}, \quad \psi(\sigma) = \begin{cases} (1\,3), & \sigma \text{ is a transposition} \\ (1), & \text{otherwise} \end{cases}$$

   Consider the 'sum' $\phi + \psi$, is it still an endomorphism? (Hint: consider the image of $(1\,2)$ under $\phi + \psi$).

Now we consider the vector space analogue. Let V be an n-dimensional vector space over $\mathbb{F}$. Then define

$$\mathrm{End}(V) = \{T : V \to V \text{ linear map}\}$$

c) Identify $\mathrm{End}(V)$ with the matrix ring $M_n(\mathbb{F})$. Conclude that $\mathrm{End}(V)$ has ring structure.

Exercise E9.3 (Group rings):
Let G be a multiplicative group and R be a ring. Define the group ring as

$$R[G] = \{\sum_{g \in G} r_g g \mid r_g \in R, \text{ there are only finitely many } r_g \neq 0\}$$

in other words, $R[G]$ consists of formal linear combinations of G with coefficients in R. Two elements $\sum_{g \in G} r_g g$ and $\sum_{g \in G} s_g g$ are equal in $R[G]$ iff $r_g = s_g$ for all $g \in G$. Define the addition and multiplication in $R[G]$ by

$$\sum_{g \in G} r_g g + \sum_{g \in G} s_g g = \sum_{g \in G} (r_g + s_g) g$$
$$\left(\sum_{g \in G} r_g g\right)\left(\sum_{g \in G} s_g g\right) = \sum_{g \in G}\left(\sum_{hk = g} r_h s_k\right) g$$

a) Prove that $R[G]$ is indeed a ring.
b) Prove that $R[G]$ is commutative if and only if R is commutative and G is abelian.

For the following, assume R is unital with unity 1.

c) Let e be the identity of G. Show that $R[G]$ is unital with unity $1e$.
d) Identify R as a subring of $R[G]$.
e) If G is finite and non-trivial, show that $R[G]$ is not an integral domain. (Hint: try to show that $\sum_{g \in G} 1g$ is a zero divisor).