Abstract Algebra I - Lecture 31

Adam Chapman

Department of Mathematics, Michigan State University, East Lansing, MI 48824

Remark.
Given a ring homomorphism

$$\varphi : R \to S$$

$\varphi(R)$ is a subring of S.

Definition.
The kernel $\ker(\varphi)$ of a homomorphism

$$\varphi : R \to S$$

is the set of all $r \in R$ such that $\varphi(r) = 0$.

Theorem.
Given a ring homomorphism

$$\varphi : R \to S$$

where R is a ring with identity, the kernel $\ker(\varphi)$ is a two-sided ideal in R.

Proof.
If $a, b \in \ker(\varphi)$ then $\varphi(a + b) = \varphi(a) + \varphi(b) = 0 + 0 = 0$, so $a + b \in \ker(\varphi)$. If $a \in \ker(\varphi)$ and $r \in R$ then $\varphi(ar) = \varphi(a)\varphi(r) = 0 \cdot \varphi(r) = 0$, so $\ker(\varphi)$ is a right-ideal. Similarly it can be shown that $\ker(\varphi)$ is a left ideal.

Example.
Consider the homomorphism

$$\varphi : \mathbb{Z} \to \mathbb{Z}_n$$

$$\varphi(x) = [x]_n.$$

The kernel of the this map is $n\mathbb{Z}$, which is indeed an ideal in $\mathbb{Z}$.

Remark.
Given a (not necessarily commutative) ring R with identity and a proper two-sided

Email address: adam1chapman@yahoo.com (Adam Chapman)

Preprint submitted to Elsevier *December 9, 2015*

ideal $I \triangleleft R$, we consider the equivalence relation $x \sim y \Leftrightarrow x - y \in I$. The set of equivalence classes is R/I. It turns out that the addition and multiplication on R are well-defined on this set, and so $(R/I, +, \cdot, 0, 1)$ is a ring.

Example.
If $R = \mathbb{Z}$ and $I = n\mathbb{Z}$ then R/I turns out to be $\mathbb{Z}_n$. This is why in many books they write $\mathbb{Z}/n\mathbb{Z}$ instead of $\mathbb{Z}_n$. (The latter is reserved for another type of ring, the ring of n-adic integers.)

Proposition.
Given R and I as above, there is a natural surjective homomorphism

$$\varphi : R \to R/I$$

that takes each $r \in R$ to its equivalence class. The kernel of that map is I.

Proof.

$$r \in \ker(\varphi) \Leftrightarrow [r] = [0] \Leftrightarrow r - 0 \in I \Leftrightarrow r \in I$$

Remark.
Two-sided ideals are precisely the kernels of ring homomorphisms.

Lemma.
Given a ring homomorphism

$$\varphi : R \to S$$

where R is a ring with identity, and a proper two-sided ideal $I \triangleleft R$ such that $I \subseteq \ker(\varphi)$, there is a natural homomorphism

$$\overline{\varphi} : R/I \to S$$

defined by $\overline{\varphi}([r]) = \varphi(r)$.

Proof.
We first verify that $\overline{\varphi}$ is well-defined: For $[r_1] = [r_2]$, $\varphi(r_2) = \varphi(r_1) + \varphi(r_2 - r_1)$, but $r_2 - r_1 \in I \in \ker(\varphi)$, so $\varphi(r_2 - r_1) = 0$, and therefore $\varphi(r_1) = \varphi(r_2)$.

The properties of a homomorphism are then inherited from φ.

Remark.
The kernel of $\overline{\varphi}$ in the previous lemma is $\ker(\varphi)/I$.

Noether Theorem I.
Given a surjective homomorphism

$$\varphi : R \to S$$

the homomorphism

$$\overline{\varphi} : R/\ker(\varphi) \to S$$

is an isomorphism.

Example.

Consider

$$\varphi : \mathbb{Z} \to \mathbb{Z}_n$$

$$\varphi(x) = [x]_n.$$

Then $\overline{\varphi} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n$ is indeed an isomorphism.

Remark.

If R is a ring and $I, J \lhd R$ with $I \subseteq J$ then J/I is an ideal in R/I.

Noether Theorem II.

Let R be a ring, $I, J \lhd R$ two-sided ideals and $I \subseteq J$. Then the natural homomorphism

$$\varphi : R/I \to R/J$$

is surjective, its kernel is J/I, and the induced homomorphism

$$\overline{\varphi} : (R/I)/(J/I) \to R/J$$

is an isomorphism.

Example.

Consider $R = \mathbb{Z}$ and the ideals $I = 4\mathbb{Z}$ and $J = 2\mathbb{Z}$. Then $J \supseteq I$. By Noether Theorem II, $(R/I)/(J/I) \cong R/J$. Now, $R/J = \mathbb{Z}_2$, $R/I = \mathbb{Z}_4$ and $J/I = \{[0]_4, [2]_4\}$. Therefore $\mathbb{Z}_2$ is isomorphic to $\mathbb{Z}_4/\{[0]_4, [2]_4\}$.

Home exercise.

Consider the homomorphism

$$\varphi : \mathbb{R}[x] \to \mathbb{C}$$

defined by $\varphi(r) = r$ for any $r \in \mathbb{R}$, and $\varphi(x) = i$. Explain why these images determine the image of any polynomial in $\mathbb{R}[x]$. Is φ surjective? Is it injective? If not, what is its kernel? What quotient of $\mathbb{R}[x]$ is isomorphic to $\mathbb{C}$?