Abstract Algebra
Lecture 11
Monday, 10/11/2010

1 Group Homomorphisms

Question: If $f : R \to S$ is a ring homomorphism (R, S have identities), does $f(1_R) = 1_S$?
Answer: No. For example, $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = 0$. Also $f : \mathbb{Z} \to \mathbb{Z}_6$ defined by $f(n) = 3n \mod 6$.

Theorem: Let $f : R \to S$ be a homomorphism. Then
(a) $\text{Im}(f) = \{f(r) \mid r \in R\}$ is a subring of S.
(b) $\ker(f) = \{r \in R \mid f(r) = 0_S\}$ is a subring of R.
(c) $\ker(f)$ has the property that if $r \in R$, $x \in \ker(f)$, then $rx, xr \in \ker(f)$.
In other words, the kernel of f is good at pretending to be 0.

Proof:
(a) It is clearly nonempty. Pick $f(a), f(b) \in \text{Im}(f)$. Then $f(a) - f(b) = f(a-b) \in \text{Im}(f)$. Similarly, $f(a)f(b) = f(ab) \in \text{Im}(f)$. So $\text{Im}(f)$ is closed under our operations, so it is a subring of S.
(b) Pick $a, b \in \ker(f)$. Then $f(a-b) = f(a) - f(b) = 0 - 0 = 0$, so $a - b \in \ker(f)$. Similarly, $f(ab) = f(a)f(b) = 0$, so $ab \in \ker(f)$. So $\ker(f)$ is a subring of R.
(c) Let $r \in R$, $x \in \ker(f)$. Then $f(rx) = f(r)f(x) = f(r)0 = 0$, so $rx \in \ker(f)$. Similar for xr.

■

Theorem: Let R be a ring with identity. Let $f : R \to S$ be a homomorphism. Then $f(1_R) = 1_{\text{Im}(f)}$.

Proof: Pick $f(a) \in \text{Im}(f)$ for some $a \in R$. Then $f(a)f(1_R) = f(a1_R) = f(a)$. Similar on the other side. Thus $f(1_R)$ is the identity in $\text{Im}(f)$. ■

2 Quotient Rings

Defn: If R is a ring, then S is a quotient ring of R if
- The set S is a quotient of the set R,
- The projection $f : R \to S$ is a homomorphism.

First, let's define some equivalence relations on R. Let $I \leq R$. Define $\sim_I$ by $x \sim_I y$ if and only if $x - y \in I$. (Note that this is the same as for groups, except using xy^{-1}

additively, instead of multiplicatively.) Is this an equivalence relation? Yes. It is clearly reflexive, as $x \sim_I x$ since $0 \in I$. If $x \sim_I y$, then $x - y \in I$, so $-(x-y) = y - x \in I$, so $y \sim_I x$, so it is reflexive. If $x \sim_I y$ and $y \sim_I z$, then $x - y \in I$ and $y - z \in I$, so $(x-y) + (y-z) = x - z \in I$, so $x \sim_I z$, so it is transitive.

Theorem: If S is a quotient ring of R, then the equivalence classes that are elements of S are the equivalence classes of $\sim_{\ker(f)}$ where $f : R \to S$ is the projection map.

Proof: Let's describe the equivalences in S. r_1 and r_2 are in the same equivalence class in S if and only if $f(r_1) = f(r_2)$. Then

$$\begin{aligned} f(r_1) = f(r_2) &\iff f(r_1) - f(r_2) = 0 \\ &\iff f(r_1 - r_2) = 0 \\ &\iff r_1 - r_2 \in \ker(f) \\ &\iff r_1 \sim_{\ker(f)} r_2. \end{aligned}$$

■

Let $I \leq R$. What are the equivalence classes of $\sim_I$ look like?

$$\begin{aligned} [x] &= \{y \in R \mid x - y \in I\} \\ &= \{y \in R \mid x - y = i \in I\} \\ &= \{y \in R \mid y - x = i \in I\} \\ &= \{y \in R \mid y = x + i, i \in I\} \\ &= x + I. \end{aligned}$$

Note that this is an additive coset of I by x. These behave exactly like cosets, we hope: $(x+I) + (y+I) = (x+y) + I$, and $(x+I)(y+I) = xy + I$. But we need these to be well defined.

Theorem: These operations are well-defined if and only if I has the property that $ri \in I$ and $ir \in I$ for any $r \in R$, $i \in I$. (In other words, the subgroup I must "absorb" through multiplication.)

Proof: Assume that I is a multiplicative absorber. Addition works because $(I, +) \trianglelefteq (R, +)$ because it is an abelian group under addition so all subgroups are normal. Now, consider $x + I$ and $y + I$. We want to show that $((x+i)+I)((y+j)+I) = (x+I)(y+I)$ for any $x, y \in R$, $i, j \in I$. $((x+i)+I)((y+j)+I) = (x+i)(y+j) + I = xy + xj + iy + ij + I = xy + I$ since $xj, iy \in I$ since it is absorptive.
Assume that the operations are well-defined. The previous calculation shows that, if the operations are well defined, then the only way to achieve equality is if $iy + xj + ij \in I$, or $iy + xj \in I$ for every $x, y \in R$ and $i, j \in I$. In particular, this must be true when $x = 0$ or when $y = 0$, so it must be the case that both $iy \in I$ and $xj \in I$, so I is an absorber. ■

Defn: A subring I with this property is called an **ideal**.

Ex: Let $R = \mathbb{Z}[x]$. Let $S = \mathbb{Z}$, the constant polynomials. So $S \leq R$. But S is not an ideal: $2 \cdot x \notin S$. See that the operations are not well-defined: $(x + \mathbb{Z})(x + \mathbb{Z})$ "should" be $x^2 + \mathbb{Z}$. But $((x + 1) + \mathbb{Z})(x + \mathbb{Z})$ "should" be $x^2 + x + \mathbb{Z}$, which is not the same coset. Let $I = \{a_1 x + a_2 x^2 + \cdots + a_n x^n | a_1 \in Z\}$ the polynomials with no constant term. I is an ideal. If $i \in I$, then $i \cdot f$ will also have zero constant term, for all $f \in R$. So what are the cosets of I? $f \sim_I g \iff f - g$ has no constant term. In other words, $f \sim_I g \iff f$ and g have the same constant term. So if we identify the cosets by their constant term, so cosets look like $\{n + I \mid n \in \mathbb{Z}\}$. The quotient ring $R/I \cong \mathbb{Z}$.