MATH H113: Honors Introduction to Abstract Algebra

2016-03-30

- Quotient rings
- Isomorphism theorems

On the homework (extra problem):
In general, $|x+y|$ *divides* $\operatorname{lcm}|x||y|$
See Ex. 16 on p. 60

Continuing from last time: let $\phi : R \to S$ be a (ring) homomorphism, and let $I = \ker\phi$. Which subrings can be kernels?
The kernel is an additive subgroup; also:
If $a \in I$ and $r \in R$ then $ar \in I$ and $ra \in I$, because $\phi(ra) = \phi(r)\phi(a) = \phi r \cdot 0 = 0$, so $ra \in I$, likewise $ar \in I$.

Definition: Let R be a ring, and let I be a subring of R. Then
a. $r + I = \{r + a : a \in I\}$ (same as the coset of additive groups) b. $rI = \{ra : a \in I\}$ and $Ir = \{ar : a \in I\}$. These are *not* cosets.

Definition: An ideal in a ring R is a subring I of R such that $rI \subseteq I$ and $Ir \subseteq I \; \forall r \in R$. (These are also called *two-sided* ideals. If we leave out $Ir \subset I$ then it's called a left ideal; similarly for right ideals. See the book.)
To check that $I \subseteq R$ is an ideal in R, you only need to check that it's an additive subgroup and $rI \subseteq I$ and $Ir \subseteq I \; \forall r \in R$.
So, every kernel of a homomorphism is an ideal.
Is every ideal in R the kernel of some homomorphism?
Proposition: Let R be a ring and let I be an ideal in R. Let R/I be the quotient group of additive groups. Then:

a. the formula $(a+I)\cdot(b+I) = (ab+I)$ gives a well-defined binary operation on R/I.
b. Using this binary operation as multiplication, R/I is a ring; and
c. The *canonical project* $\pi : R \to R/I$ (from group theory) ($\pi : a \mapsto a + I$) is a ring homomorphism, and it's kernel is I.

Proof: Let $a+I, b \in I$ be in R/I, and suppose $a+I = a'+I$ and $b+I = b'+I$.
Then $a' = a + \alpha$ and $b' = b + \beta$ with $\alpha, \beta \in I$.
$a'b' = (a+\alpha)(b+\beta) = ab + a\beta + \alpha(b+\beta)$
and $a\beta + \alpha(b+\beta) \in I$, so $a'b' + I = ab + I$.
$\therefore (a+I)(b+I)$ is well defined.

b. We already know that R/I is an additive group, so it remains only to check associativity of multoplication and the two distribution laws.

Associativity:
$(a+I)((b+I)(c+I)) = a(bc)+I = (ab)c+I = ((a+I)(b+I))(c+I)$.
Similarly for the distributive laws.

c. Again, we only need to check that $\pi(ab) = \pi(a)\pi(b)$.
This is true because $\pi(ab) = ab+I = (a+I)(b+I) = \pi(a)\pi(b)$.
The kernel of $\pi = I$: comes from group theory.

Corollary: Every ideal is the kernel of some (ring) homomorphism.
Definition: The ring R/I is called the *quotient ring.* If R is commutative, then so is R/I. If R has 1, then so does R/I.

Example: Let $m \in \mathbb{Z}$
Then $m\mathbb{Z} = \{mn : n \in \mathbb{Z}\}$ is an ideal in $\mathbb{Z}$ (it's an additive subgroup $\langle m \rangle$, and if $mn \in m\mathbb{Z}$ and $k \in \mathbb{Z}$ then $k(mn) = (mn)k = m(nk)$ is in $m\mathbb{Z}$. So it's ideal.
Then the quotient ring $\mathbb{Z}/m\mathbb{Z}$ is the same as $\mathbb{Z}/m\mathbb{Z}$ we defined earlier because $\mathbb{Z}/m\mathbb{Z}$ (the quotient ring) is $\mathbb{Z}/m\mathbb{Z}$ as an additive group, and multiplication is the same.

Theorem (First Isomorphism Theorem): Let $\phi : R \to S$ be a ring homomorphism and let $I = \ker\phi$. Then I is an an ideal. Also defined $\psi : R/I \to \operatorname{im}\phi$ by $a+I \mapsto \phi(a)$. This is well defined by group theory, and is bijective by group theory. It is a ring homomorphism because $\psi((a+I)(b+I)) = \psi(ab+I) = \phi(ab) = \phi(a)\phi(b) = \psi(a+I)\psi(b+I)$.
$\therefore$ it's a ring homomorphism. So it's a ring isomorphism.
Then an arbitrary homomorphism $\phi : R \to S$ can be split up as before: let $I = \ker\phi$
$R \xrightarrow{\pi} R/I \xrightarrow{\sim} \operatorname{im}\phi \xrightarrow{S}$.

Definition: Let A and B be *subsets* of a ring R. Then
a. $A+B = \{a+b : a \in A \text{ and } b \in B\}$ (as in group theory). b. $AB = \{\sum i = 1^n a_i b_i : n \in \mathbb{N}, a_i \in A\ \forall i = 1,\dots,n, \text{ and } b_i \in B\ \forall i = 1,\dots,n\}$ (don't forget these are *finite sums*!!)

Theorem (Second Isomorphism Theorem): Let R be a ring, let A be a subring of R and let B be an ideal in R. Then $A+B$ is a subring of R, B is an ideal in $A+B$, $A \cap B$ is an ideal in A, and $A/(A\cap B) \cong (A+B)/B$ (via $a + (A\cap B) \mapsto a+B$).
Proof: $A+B$ is a subgring: it's a subgroup (from group theory), and closed under multiplication because $(a_1+b_1)(a_2+b_2) = a_1a_2+a_1b_2+b_1(a_2+b_2) \in A+B$. B is an ideal in $A+B$ because $B \subseteq A+B$ and B is an ideal in R (so if any $b \in B$ and $r \in A+B$ then $br \in B$ because $r \in R$ and $rb \in B$ because $r \in R$). Then, from group theory, $f : A \to (A+B)/B$ ($a \mapsto a+B$) is onto and \$and has kernel $A \cap B$, so $A \cap B$ is an ideal in A, and we get the isomorphism $\frac{A}{A\cap B} \xrightarrow{\sim} \frac{A+B}{B}$ from the First Isom. Thm.

Theorem (Third Isomorphism Theorem): If I and J are ideal in R and $I \subseteq J$, then J/I is an ideal in R/I, and $\frac{R/I}{J/I} \cong R/J$.

Proof: Map $R/I \to R/J$. It's onto with kernel J/I. As in group theory.

Theorem (Fourth Isomomorphism Theorem): Let R be a ring and let I be an ideal in R. Then $\exists$ a bijection $\{$subrings of R than contain I$\} \to \{$subrings of $R/I\}$. Moreover, this preserves idealness and inclusion.
Proof: that a subgroup of R (under $+$) that contains I is a subring $\iff$ its counterpart in R/I is a subring is an exercise.