Algebra Notes

Sept. 16: Fields of Fractions and Homomorphisms

Geoffrey Scott

Today, we discuss two topics. The first topic is a way to *enlarge* a ring by introducing new elements that act as multiplicative inverses of non-units, just like making fractions of integers enlarges $\mathbb{Z}$ into $\mathbb{Q}$. The second topic will be the concept of a ring homomorphism, which is a map between rings that preserves the addition and multiplication operations.

Fields of Fractions

Most integers don't have integer inverses. This is annoying, because it means we can't even solve linear equations like $2x = 5$ in the ring $\mathbb{Z}$. One popular way to resolve this issue is to work in $\mathbb{Q}$ instead, where the solution is $x = 5/2$. Because $\mathbb{Q}$ is a field, we can solve any equation $ax = b$ with $a, b \in \mathbb{Q}$ and $a \neq 0$ by multiplying both sides of the equation by a^{-1} (guaranteed to exist because $\mathbb{Q}$ is a field), obtaining $a^{-1}b$ (often written a/b).

Now suppose we want to solve $ax = b$, but instead of a and b being integers, they are elements of some ring R. Can we always find a field that contains R so that we multiply both sides by a^{-1} (in other words, "divide" by a), thereby solving $ax = b$ in this larger field? To start, let's assume that R is a commutative ring with identity. If we try to enlarge R into a field in the most naive way possible, using as inspiration the way we enlarge $\mathbb{Z}$ into $\mathbb{Q}$, we might try the following definition.

Naive definition 1: Let R' be the ring whose elements are expressions of the form a/b, where $a, b \in R$. Addition is given by $a/b + c/d = (ad + bc)/bd$, and multiplication is given by $(a/b)(c/d) = ac/bd$.

Sad fact: This isn't even a ring because it fails to be a group under the addition operation: the additive identity element would need to be $0/1$, and there's no way to find an inverse for a/b (the element $(-a)/b$ is not its inverse because $a/b + (-a)/b = 0/(b^2)$).

Your reaction to the failure of this definition is probably "Oh, of course you need some condition saying that $0/(b^2)$ is the same as $0/1$. In $\mathbb{Q}$, two fractions a/b and c/d are the same number when $ad = bc$; let's modify our definition so that the elements are *equivalence classes* of fractions under this relation."

Naive definition 2: Let R' be the ring whose elements are equivalence classes of fractions a/b, where a/b is equivalent to c/d if $ad = bc$. Addition is given by $a/b + c/d = (ad + bc)/bd$, and multiplication is given by $(a/b)(c/d) = ac/bd$.

Sad fact: Under this equivalence relation, *everything* is equivalent to the fraction $0/0$, so R' only has a single element.

Again taking our inspiration from fractions of integers, we might decide to prohibit 0 from being a denominator.

Naive definition 3: Let R' be the ring whose elements are equivalence classes of fractions a/b, $b \neq 0$, where a/b is equivalent to c/d if $ad = bc$. Addition is given by $a/b + c/d = (ad + bc)/bd$, and multiplication is given by $(a/b)(c/d) = ac/bd$.

Sad fact: This won't (in general) be an enlargement of R, because it won't (in general) contain R as a subring. Suppose, for example, that R contains zero divisors, so $ab = 0$ for some nonzero a, b. Then $a/1 = 0/b$, and $0/b = 0/1$, so $a/1 = 0/1$. We were hoping that the elements $\{r/1 \mid r \in R\}$ would be a copy of R inside R' and we have failed, because $a/1 = 0/1$ for any zero divisor a.

Somehow, the presence of zero divisors in our ring prevents us from using this fraction construction. In retrospect, this sort of makes sense – in a field, you *never* have zero divisors. And when you "enlarge" a ring, the zero divisors will still be zero divisors in the enlarged ring. So we were naive to think we could ever enlarge a ring with zero divisors into a field. However, for integral domains (which don't have zero divisors), we can.

Definition: Let R be an integral domain. The **field of fractions of** R is the field $\mathcal{F}$ consisting of equivalence classes of pairs (a, b) of elements of R, $b \neq 0$, where $(a, b) \sim (c, d)$ if $ad = bc$. Normally, an equivalence class $[(a, b)]$ is written a/b. Addition and multiplication on $\mathcal{F}$ are defined by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \text{and} \qquad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}.$$

Remark: There is a lot to check in the above definition: the equivalence relation is indeed an equivalence relation, the addition and multiplication operations are well-defined and make $\mathcal{F}$ into a ring, and that the ring is indeed a field.

We constructed the field of fractions $\mathcal{F}$ as a way to "enlarge" a ring R into a field – indeed, $\mathcal{F}$ contains a copy of R as a subring, namely $\{\frac{r}{1} \mid r \in R\}$. When I say that this subring "is" a copy of R, I mean that there is a correspondence between elements of R and this subring (namely, the correspondence that associates r with $r/1$), and that the ring structure (i.e. the addition and multiplication tables) for the elements of R is the same as that of the corresponding elements of $\mathcal{F}$.

When we're comparing two different rings, it's helpful to study maps from the elements of one ring to elements of the other that "preserve the structure." This idea is made rigorous through the definition of a *ring homomorphism*.

Homomorphisms

Definition: A **ring homomorphism** φ from a ring R to a ring S is a mapping from the elements of R to the elements of S that preserves the addition and multiplication operations. That is, for all $a, b \in R$ it satisfies

$$\varphi(a + b) = \varphi(a) + \varphi(b) \text{ and}$$
$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

If φ is injective (one-to-one) and surjective (onto), it is an **isomorphism**. The **kernel** of φ is $\ker(\varphi) := \{r \in R \mid \varphi(r) = 0\}$, and the **image** of φ is $\text{im}(\varphi) := \varphi(R)$.

In the definition above, the expressions $a + b$ and $a \cdot b$ use the addition and multiplication operations from R, while the expressions $\varphi(a) + \varphi(b)$ and $\varphi(a) \cdot \varphi(b)$ use the operations from S.

Remark: Just like in group theory, a ring homomorphism φ is injective if and only if $\ker(\varphi) = \{0\}$. This follows from the fact that every ring homomorphism is also a group homomorphism of the underlying abelian group, so the same proof from group theory carries over to the context of ring homomorphisms.

Examples

Example 1: Let $\varphi : \mathbb{R} \to \mathbb{R}[x]$ send a number a to the constant polynomial a.

Example 2: Let $\varphi : C(\mathbb{R}) \to \mathbb{R}$ send a function f to the number $f(5)$.

Example 3: Let $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ send a to the coset $[a]$.

Example 4: Let R be a ring with identity, and let $\varphi : \mathbb{Z} \to R$ send k to $1 + 1 + \cdots + 1$ (where there are k copies of "1" added together).

Example 5: (from topology). Let $\psi : X \to Y$ be a continuous map of topological spaces, and let $C(X), C(Y)$ be the rings of continuous functions on X and Y respectively. Define $\varphi : C(Y) \to C(X)$ by $f \mapsto f \circ \psi$.

Non-examples: The following are *not* examples of ring homomorphisms. Explain why.

- Define $\varphi : \mathbb{Z} \to 2\mathbb{Z}$ by $\varphi(a) = 2a$.
- Define $\varphi : \mathbb{Z} \to \mathbb{Z}$ by $\varphi(a) = a^2$.
- Let $C^\infty(\mathbb{R})$ be the set of functions on $\mathbb{R}$ which are infinitely-many times differentiable. Then define $\varphi : C^\infty(\mathbb{R}) \to C^\infty(\mathbb{R})$ by $\varphi(f) = \frac{df}{dx}$.

Kernels and Images are Subrings

Recall from linear algebra that the kernel and image of a linear transformation are subspaces of the domain and codomain of the linear transformation. In group theory, the kernel and image of a group homomorphism are subgroups of the domain and codomain of the group homomorphism. Following this trend, we prove that the kernel and image of a ring homomorphism are subrings of the domain and codomain of the ring homomorphism.

Proposition: If $\varphi : R \to S$ is a ring homomorphism, then $\ker(\varphi)$ is a subring of R, and $\mathrm{Im}(\varphi)$ is a subring of S.

Proof: We must show that $\ker(\varphi)$ and $\mathrm{im}(\varphi)$ are closed under addition, additive inverses, and multiplication. Because ring homomorphisms are group homomorphisms of the underlying abelian group, we know from group theory that $\ker(\varphi)$ and $\mathrm{im}(\varphi)$ are subgroups. Therefore, they are closed under addition and additive inverses. Then for $a, b \in \ker(\varphi)$,

$$\varphi(ab) = \varphi(a)\varphi(b) = 0$$

proves that $\ker(\varphi)$ is closed under multiplication. Now, suppose $a, b \in \mathrm{im}(\varphi)$. This means that there exists $a', b' \in R$ for which $\varphi(a') = a$ and $\varphi(b') = b$. Then

$$a'b' = \varphi(a)\varphi(b) = \varphi(ab),$$

so $a'b' \in \mathrm{im}(\varphi)$, proving that $\mathrm{im}(\varphi)$ is closed under multiplication.