Section 18: Ring Homomorphisms

Let's make it official:

Def: A function φ from one ring R to another S is a ring homomorphism iff it respects the ring operations: For all $a, b \in R$,

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

Because a ring homomorphism is first an additive group homomorphism, we have $\varphi(0_R) = 0_S$ and for n in $\mathbb{Z}$ and a in R, $\varphi(na) = n\varphi(a)$. And it is also true that $\varphi(a^n) = \varphi(a)^n$ for any <u>positive</u> integer n. But weird things can happen with unities, if they exist at all. Note first that, if R is a ring with unity and $\varphi : R \to S$ is a ring homomorphism for which $\varphi(1_R) = 0_S$, then for all r in R, $\varphi(r) = \varphi(r1_R) = \varphi(r)\varphi(1_R) = \varphi(r)0_S = 0_S$, so φ is the constant function 0.

Ex: Consider the function $\varphi : \mathbb{R} \to M_{2\times 2}(\mathbb{R}) : r \mapsto \begin{pmatrix} r & 0 \\ 0 & 0 \end{pmatrix}$. This is a ring homomorphism, and both rings have unities, 1 and $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ respectively, but the homomorphism doesn't take the unity of $\mathbb{R}$ to the unity of $M_{2\times 2}(\mathbb{R})$.

Exs: • For any positive integer n, the function $\mathbb{Z} \to \mathbb{Z}_n : x \mapsto x \mod n$ is not just a homomorphism of additive groups; it is also a ring homomorphism.

• "Complex conjugation", sending each complex number $z = x + yi$ (where $x, y \in \mathbb{R}$) to its complex conjugate $\overline{z} = x - yi$, turns out to be a ring automorphism of $\mathbb{C}$. Similarly, in the ring $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$, the function $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ is an automorphism of $\mathbb{Z}[\sqrt{2}]$.

• If R, S are rings and $R \times S$ is the direct product of rings, with coordinatewise operations, the projection onto the first coordinate $R \times S \to R : (r, s) \mapsto r$ is a ring epimorphism — as is the projecton onto the second coordinate S. The inclusion as the first coordinate $R \to R \times S : r \mapsto (r, 0)$ is a ring monomorphism, as the inclusion as the second coordinate. If R, S have unities, then $R \times S$ has unity $(1_R, 1_S)$ and the projections take unity to unity; but the inclusions don't do that.

• If a is a fixed element of the set X and $\mathcal{F}(X)$ is the family of all functions $X \to \mathbb{R}$,with pointwise operations, then the evaluation function $\varepsilon_a : \mathcal{F}(X) \to \mathbb{R} : f \mapsto f(a)$ is a ring epimorphism. Similarly, on the set $\mathbb{R}[x]$ of polynomials in the variable x with real coefficients, if a is a fixed real number, the evaluation function (which I will again denote ε_a) $\mathbb{R}[x] \to \mathbb{R} : p(x) \mapsto p(a)$ is a ring homomorphism — the definitions of addition and multiplication of polynomials, which look weird in the abstract [ask a struggling high school algebra student], were chosen to make that work.

• On the set $\mathbb{R}[x]$ of polynomials in the variable x with real coefficients, differentiation is a homomorphism of additive groups, but it is <u>not</u> a ring homomorphism, because the product rule is not $D(fg) = D(f)D(g)$.

• On the set $M_{2\times 2}(\mathbb{R})$ of 2×2 matrices with real entries, the determinant function (onto $\mathbb{R}$) respects multiplication but not addition, so it is not a ring homomorphism. And the trace function $M_{2\times 2}(\mathbb{R}) \to \mathbb{R}$ (which we don't usually mention in our Math 214 — it's just the sum of the main diagonal entries) respects addition but not multiplication, so it is not a ring homomorphism, either.

• Consider the functions $\mathbb{Z}_n \to \mathbb{Z}_n$ given by $x \mapsto ax$, where a is a fixed element of $\mathbb{Z}_n$ and the last multiplication is mod n. They are all additive group homomorphisms; they are epimorphisms, and hence automorphisms, exactly when a is a generator of $\mathbb{Z}_n$, i.e., relatively prime to n. Usually, though, they are not ring homomorphisms, because they don't respect the multiplication. They only do that, i.e., they are only ring homomorphisms, if a is an idempotent ($a^2 = a$). We always have the idempotents 0 and 1, of course, giving the zero function and the identity function on $\mathbb{Z}_n$; others are 3 or 4 in $\mathbb{Z}_6$, 4 or 9 in $\mathbb{Z}_{12}$, etc. To get an idempotent other than 0 or 1 in $\mathbb{Z}_n$, we need n to divide $a(a-1)$ for some a between 2 and $n-1$.

Theorem 18.2 says that, if R, S are rings with unity and $\varphi : R \to S$ is a ring homomorphism for which $\varphi(1_R) \neq 0_S$, then $\varphi(1_R) = 1_S$ provided S is either a division ring or an integral domain. The two cases fall into a single one: $\varphi(1_R) = 1_S$ provided S has no nonzero zero-divisors. Part (i) of the same theorem, 18.2, can be stated a bit more strongly: If R has a unity and $\varphi : R \to S$ is an epimorphism, then $\varphi(1_R)$ is a unity for S.

Let's collect the basic facts about ring homomorphisms:

Prop: Let $\varphi : R \to S$ be a ring homomorphism.

- If A is a subring of R, then $\varphi(A)$ is a subring of S. If A is an ideal in R <u>and</u> φ is onto S, then $\varphi(A)$ is an ideal in S.
- If B is a subring of S, then $\varphi^{-1}(B)$ is a subring of R. If B is an ideal in S, then $\varphi^{-1}(B)$ is an ideal in R.
- If $\psi : S \to T$ is another ring homomorphism, then $\psi \circ \varphi : R \to T$ is a ring homomorphism.
- If φ is a ring isomorphism, then so is φ^{-1}.
- The kernel $A = \{r \in R : \varphi(r) = 0_S\}$ of φ is an ideal in R, and the canonical group homomorphism $R \to R/A$ is a ring epimorphism.
- (Fundamental Theorem of Ring Homomorphisms) Again, let $A = \ker(\varphi)$. The group isomorphism $\overline{\varphi} : R/A \to \varphi(R) : Ar \mapsto \varphi(r)$ is also a ring isomorphism.

All of this is easy to check. Let's just give a quick example to show why we need "onto" for the image of an ideal to be an ideal: The set $2\mathbb{Z}$ of even integers is an ideal in $\mathbb{Z}$, and the inclusion function $\mathbb{Z} \to \mathbb{Q} : x \mapsto x$ is a ring homomorphism, but in $\mathbb{Q}$, $2\mathbb{Z}$ no longer captures multiplication: $\frac{1}{2} \cdot 2 = 1 \notin 2\mathbb{Z}$.

Cor: Let R, S be rings with unity and $\varphi : R \to S$ be a ring homomorphism for which $\varphi(1_R) \neq 0_S$. Then:

(a) For every unit u in R, $\varphi(u) \neq 0_S$. In particular, any ring homomorphism from a division ring (or field) to some other ring either takes every element to 0_S or is a monomorphism.

(b) If r, s in R satisfy $rs = 0_R$ and $\varphi(r)$ is a unit in S, then $\varphi(s) = 0_S$.

Pf: (a) $\varphi(u)\varphi(u^{-1}) = \varphi(1_R) \neq 0_S$, so $\varphi(u) \neq 0_S$.
(b) $\varphi(s) = \varphi(r)^{-1}\varphi(r)\varphi(s) = \varphi^{-1}\varphi(rs) = \varphi(r)^{-1}0_S = 0_S$. //

Prop and Def: Let R be a ring with unity.

(a) The function $\varphi : \mathbb{Z} \to R : n \mapsto n1_R$ is a ring homomorphism; the image $\varphi(\mathbb{Z})$ is in the center of R (the set of elements that commute with every element of R) and is called the *prime subring* of R; the nonnegative generator of the kernel of φ is the *characteristic* of R.

(b) If R has no nonzero zerodivisors, then the additive order of 1_R (which is the characteristic if the characteristic is nonzero and infinite if the characteristic is 0) is also the additive order of every nonzero element of R, and if it is finite, then it is a prime number p, so that $\varphi(\mathbb{Z}) \cong \mathbb{Z}_p$, a field.

(c) Suppose R is a division ring; if it has finite characteristic, we have just seen that it contains a copy of some $\mathbb{Z}_p$. If it has characteristic 0, then φ is a monomorphism of $\mathbb{Z}$ into R, and $\{(m1_R)(n1_R)^{-1} : m, n \in \mathbb{Z},\ n \neq 0\} \cong \mathbb{Q}$ is a subfield in the center of R. The subfield congruent $\mathbb{Z}_p$ or $\mathbb{Q}$ (depending on the characteristic) is called the *prime subfield* of R.

Pf: (a) The elements $n1_R$, as integer multiples of 1_R, must commute with every element of R, so they are in $Z(R)$. It is easy to check that φ is a ring homomorphism. The rest of part (a) is definitions.

(b) Let r be a nonzero element of R, and suppose $nr = 0_R$ for some positive integer. Then $r(n1_R) = 0_R$, and because R has no nonzero zerodivisors, $n1_R = 0_R$. Conversely if $n1_R = 0_R$, then it is easy to see that $nr = 0_R$ for all r in R. So the additive orders of all the nonzero elements of R are equal. Now suppose that order is finite but not prime, say it is mn where m, n are integers greater than 1. Then $0 = (mn)1_R = (m1_R)(n1_R)$, and because R has no nonzero zerodivisors, one of $m1_R, n1_R$ must be 0; but that means the additive order of 1_R is less than mn, the desired contradiction. So $\varphi(\mathbb{Z})$ is isomorphic to $\mathbb{Z}_p$ for some prime p.

(c) In characteristic 0: Because $\varphi(\mathbb{Z}) \subseteq Z(R)$, the reciprocals of its nonzero elements are also in $Z(R)$. So $\{(m1_R)(n1_R)^{-1} : m, n \in \mathbb{Z},\ n \neq 0\}$ is in $Z(R)$ and is a field isomorphic in the obvious way to $\mathbb{Q}$. The rest of part (c) is definitions. //

The text proves in some detail the following fact:

Prop and Def: Let R be an integral domain. Then there is a field F, called the *field of fractions* of R, which contains (an isomorphic copy of) R and such that every element of F can be written in the form ab^{-1} where $a, b \in R$ and $b \neq 0$.

It is only a bit messier, and actually clearer, to prove a more general result:

Prop and Def: Let R be a commutative ring and S be a subset of R that is closed under multiplication; for simplicity, assume R has unity and $1_R \in S$. Then there is a ring $S^{-1}R$ with unity, called the *ring of fractions of R with respect to S*, such that

(i) there is a ring homomorphism $\varphi : R \to S^{-1}R$ (that takes 1_R to the unity of $S^{-1}R$),

(ii) for all s in S, $\varphi(s)$ is a unit in $S^{-1}R$, and

(iii) every element of $S^{-1}R$ has the form $\varphi(r)\varphi(s)^{-1}$.

The kernel of φ consists of the elements r of R for which $sr = 0$ for some s in S.

Pf: On the set $R \times S$, define the relation $\mathcal{R}$ by $(a, s)\mathcal{R}(b, t)$ iff there is an element u of S for which $atu = bsu$. (If S contains no zerodivisors, then we don't have to bother with the extra u, and the φ we get will be a monomorphism.)

(R) $as1_R = as1_R$, so $(a,s)\mathcal{R}(a,s)$ for all (a,s) in $R \times S$.

(S) If $(a,s)\mathcal{R}(b,t)$, then $atu = bsu$, so $bsu = atu$, so $(b,t)\mathcal{R}(a,s)$.

(T) If $(a,s)\mathcal{R}(b,t)$ and $(b,t)\mathcal{R}(c,v)$, then $atu = bsu$ and $bvw = ctw$ for some u, w in S, so

$$(av)(tuw) = (atu)vw = (bsu)vw = (bvw)su = (ctw)su = (cs)(tuw) ,$$

and $tuw \in S$ because S is closed under multiplication, so $(a,s)\mathcal{R}(c,v)$

So $\mathcal{R}$ is an equivalence relation on $R \times S$; denote the equivalence class of (a,s) by $[a,s]$, and the set of all such equivalence classes by $S^{-1}R$. (Think of $[a,s]$ as a/s, and the following definitions will make sense.)

Define the operations of addition and multiplication on these equivalence classes:

$$[a,s] + [b,t] = [at + bs, st] \qquad \text{and} \qquad [a,s][b,t] = [ab, st] \ .$$

Of course, we need to check that these operations are well-defined: If $[a,s] = [a', s']$ and $[b,t] = [b', t']$, say $as'u = a'su$ and $bt'v = b'tv$, then

$$(at + bs)(s't')uv = (as'u)tt'v + (bt'v)ss'u = (a'su)tt'v + (b'tv)ss'u = (a't' + b's')(st)uv$$

and

$$(ab)(s't')uv = (at'u)(bs'v) = (a'tu)(b'sv) = (a'b')(st)uv$$

where $uv \in S$, so $[at + bs, st] = [a't' + b's', s't']$ and $[ab, st] = [a'b', s't']$. Therefore, the operations are well-defined.

We can check that this addition is commutative, associative and distributive over the multiplication, that multiplication is associative and commutative, that $[0_R, 1_R]$ is a zero and $[-a, s]$ is a negative for $[a,s]$, and that $[1_R, 1_R]$ is a unity and $[1_r, s]$ is a multiplicative inverse for $[s, 1_R]$.

Finally, we need to define the homomorphism $\varphi : R \to S^{-1}R$. Set $\varphi(r) = [r, 1_R]$. Then we can check that φ is a ring homomorphism. We have seen that, for each s in S, $\varphi(s) = [s, 1_R]$ is a unit in $S^{-1}R$. An element r of R is in the kernel of φ iff $[r, 1_R] = [0_R, 1_R]$, i.e., iff there is an element s of S for which $r(1_R)s = 0_R(1_R)s$, i.e., iff $rs = 0_R$ for some s in S. //

The text makes the point that the field of fractions of an integral domain R is the unique smallest field that contains R. In the same way, if R is a commutative ring and S is a subset of R closed under multiplication, and if T is a commutative ring with unity for which there is a ring homomorphism $\psi : R \to T$ with the property that $\psi(s)$ is a unit in T for every s in S, then there is a ring homomorphism $\overline{\psi} : S^{-1}R \to T$, defined by $\overline{\psi}[a,s] = \psi(a)\psi(s)^{-1}$, for which the $\overline{\psi} \circ \varphi = \psi$, i.e., the following diagram is commutative:

$$\begin{tikzcd}
R \arrow[r, "\Psi"] \arrow[d] & T \\
S^{-1}R \arrow[ur, "\overline{\Psi}"] &
\end{tikzcd}$$

This $S^{-1}R$ may seem very artificial, but it is used a great deal in commutative algebra. For example, if P is a prime ideal in a commutative ring R with unity, then $R - P$ is closed under multiplication, so we can form the ring $(R - P)^{-1}R$, which is usually denoted R_P and called the "localization of R at P." The set $PR_P = \{[a, s] : a \in P, s \in R - P\}$ is the only maximal ideal in R_P, and every element outside it is a unit. In the case $R = \mathbb{Z}$ and $P = p\mathbb{Z}$ where p is a prime integer, this ring would be the set of rational numbers where the denominator is not divisible by p. In the case $R = \mathbb{R}[x, y]$ and P is the set of polynomials that take the value 0 at a point (a, b) in the plane, R_P is the set of rational functions (quotients of two polynomials) that are defined in a neighborhood of (a, b) (the neighborhood varies with the function). Etc. On the other hand, if we have an element s of a commutative ring R with unity, and we want to see what happens if we give s a reciprocal, then of course we are also making units of all the powers of s, so we form the ring $\{s^n : n \in \mathbb{Z}^+\}^{-1}R$.