Abstract Algebra. Math 6310. Bertram/Utah 2022-23.

Ideals and Quotients and Isomorphism Theorems

Definition. A ring homomorphism $f : R \to S$ is an *isomorphism* if it has a two-sided inverse ring homomorphism $g : S \to R$.

Remark. A ring homomorphism is an isomorphism if and only if it is a bijection*, i.e. if and only if it has a two-sided inverse as a set mapping since the inverse set mapping is automatically a ring homomorphism.

First Isomorphism Theorem. If $f : R \to S$ is a ring homomorphism, then:

$$R/\ker(f) \text{ is isomorphic to the image ring } Q = f(R)$$

Proof. Let $I = \ker(f)$. We define a map $\overline{f} : R/I \to Q$ by:

$$\overline{f}(r + I) = f(r)$$

This is well-defined, since $r \sim r'$ implies $r - r' \in I$, so $f(r) - f(r') = f(r - r') = 0$. Moreover, it is surjective by construction and injective, since $f(r + I) = f(r' + I)$ if and only if $f(r) = f(r')$, if and only if $r - r' \in I$, if and only if $r + I = r' + I$. $\square$

If R is a commutative ring with 1, then there is an "ideal/quotient" bijection between the sets of ideals in R and quotient rings of R:

$$\{\text{ideals } I \subset R\} \xleftrightarrow{IQ} \{\text{quotients } q : R \to Q\}$$
$$(I \subset R) \mapsto (q : R \to R/I)$$
$$(q : R \to Q) \mapsto (I = q^{-1}(0) \subset R)$$

Remark. Some care needs to be taken in the meaning of the set of quotient rings. By the first isomorphism theorem, any pair of quotient rings with the same kernel I are isomorphic to R/I, and hence to each other. Thus, a quotient needs to be understood as an *equivalence class* of surjective homomorphisms $q : R \to Q$, where q is equivalent to $q' : R \to Q'$ if there is an isomorphism linking the two quotients:

$$\begin{array}{ccccc} & & R & & \\ & \swarrow q & & q' \searrow & \\ Q & & \stackrel{\sim}{\to} & & Q' \end{array}$$

Each equivalence class has a canonical element, namely the quotient $q : R \to R/I$. Interestingly, we don't need to take this care with ideals, which are subsets of R.

Next, we translate some properties of ideals into those of the quotient rings.

Our first property of a ring is a weakened version of multiplicative inverses.

Definition. R is an *(integral) domain* if for all $r \in R - \{0\}$,

$$rs = rs' \Rightarrow s = s'$$

i.e. non-zero elements of R can be cancelled from both sides of an equation.

Examples. Fields. $R[x], R[[x]], R((x))$ and all subrings of an integral domain R.

Nonexample. $\mathbb{Z}/n\mathbb{Z}$ when n is not a prime. Nontrivial product rings.

There is another way to think about this.

Definition. An element $r \in R$ is a *zero-divisor* if $rs = 0$ for some $s \neq 0$.

Clearly, $0 \in R$ is a zero-divisor. But:

Proposition 1. R is a domain if and only if $0 \in R$ is the only zero-divisor in R.

Proof. If R is not a domain, then $rs = rs'$ and r cannot be cancelled for some pair $s \neq s' \in R$ and non-zero r. Then $r(s - s') = 0$ so r is a zero divisor. Conversely, if $r \neq 0$ is a zero-divisor, then $rs = 0$ for some $s \neq 0$ and r cannot be cancelled from that equation, so R is not a domain. □

And now for the partner property of ideals.

Definition. An ideal $I \subset R$ is *prime* if $rs \in I$ implies $r \in I$ or $s \in I$.

Example. $n\mathbb{Z} \subset \mathbb{Z}$ is prime if and only if n is a prime number.

Proposition 2. Under the IQ correspondence,

$$\{\text{prime ideals } P \subset R\} \overset{IQ}{\longleftrightarrow} \{\text{quotient domains } q : R \to R/P\}$$

Note: This does not require R itself to be a domain!

Proof. Suppose I is not prime. Then $rs \in I$ for some $r, s \notin I$. Then:

$$(r + I)(s + I) = (rs + I) = 0 \in R/I \text{ but } (r + I), (s + I) \neq 0$$

so R/I is not a domain, and conversely. □

Corollary. R itself is a domain if and only if $\{0\} \subset R$ is a prime ideal.

Example. If p is a prime dividing n, then the ideal $\langle p + n\mathbb{Z}\rangle \subset \mathbb{Z}/n\mathbb{Z}$ is prime.

Primeness also has the nice property of being preserved under inverse images.

Proposition 3. Let $f : R \to S$ be a homomorphism of commutative rings with 1.

(a) If $I \subset S$ is an ideal, then $f^{-1}(I) \subset R$ is an ideal, and:

(b) If $P \subset S$ is a *prime* ideal, then $f^{-1}(P) \subset R$ is a prime ideal.

Proofs. We get (a) by observing that:

(a1) if $f(r_1), f(r_2) \in I$, then $f(r_1 + r_2) = f(r_1) + f(r_2) \in I$, and

(a2) if $f(r) \in I$ and $r' \in R$, then $f(r'r) = f(r')f(r) \in I$.

As for (b), we observe that if $r, r' \notin f^{-1}(P)$ if and only if $f(r), f(r') \notin P$. Thus if P is prime, then $f(r)f(r') = f(rr') \notin P$, so $rr' \notin f^{-1}(P)$ and $f^{-1}(P)$ is prime. □

Remark. It is possible for $f^{-1}(I)$ to be prime and I not to be prime. Consider:

$$\delta : R \to R \times R;\ \delta(r) = (r, r),\ \text{the diagonal homomorphism}$$

Then δ is injective, so $\delta^{-1}(0) = 0$. But if R is a domain, then $\delta^{-1}(0)$ is prime while $(1, 0) \cdot (0, 1) = 0$ in $R \times R$, so 0 is not a prime ideal in $R \times R$.

However, we do have the following refinement of Proposition 3.

Proposition 4. Suppose $q : R \to R/I$ is a quotient ring. Then the map:

$$\{\text{ideals in } R/I\} \to \{\text{nestled ideals } I \subset J \subset R\}$$

$$(K \subset R/I) \mapsto (I = q^{-1}(0) \subset J = q^{-1}(K) \subset R\}$$

is a bijection, restricting to a bijection of (nestled) prime ideals:

$$\{\text{prime ideals in } R/I\} \to \{\text{nestled prime ideals } I \subset P \subset R\}$$

Proof. The inverse set map is given by $(I \subset J) \mapsto K = J/I := \{j + I \mid j \in J\}$. It is left to the reader to show that J/I is an ideal, and that this inverts q^{-1}.

For the correspondence of *prime* ideals, we use Proposition 2 and the:

Third Isomorphism Theorem. In the context of Proposition 4,

$$(R/I)/(J/I) \text{ is isomorphic to } R/J$$

Proof. The map: $(r+I)+(J/I) \mapsto r+J$ is a bijective ring homomorphism. $\square$

The astute reader will have noticed that we have skipped an isomorphism theorem.

Second Isomorphism Theorem. If $S \subset R$ be a subring and $I \subset R$ an ideal then

(a) $S+I \subset R$ is a subring and $I \subset S+I$ and $S \cap I \subset S$ are ideals.

(b) $S/(S \cap I)$ is isomorphic to $(S+I)/I$.

The astute reader is invited to prove this.

Next, we turn to maximal ideals and quotient fields.

Definition. An ideal $I \subset R$ is *maximal* if no ideal nestles between I and R.

Example. The prime ideals $p\mathbb{Z} \subset \mathbb{Z}$ are maximal, but the other ideals are not.

Proposition 5. An ideal $\mathfrak{m} \subset R$ is maximal if and only if $R/\mathfrak{m}$ is a field.

Proof. Suppose $R/\mathfrak{m}$ is not a field. Then $r+\mathfrak{m}$ does not have an inverse, and so $\langle r+\mathfrak{m}\rangle \subset R/\mathfrak{m}$ is a nonzero ideal, which corresponds to a nestled ideal $\mathfrak{m} \subset J \subset R$ and $\mathfrak{m}$ is not maximal. Conversely, if $\mathfrak{m}$ is not maximal, then choose $r \in J - \mathfrak{m}$ for a nestled ideal. Then $r+\mathfrak{m}$ cannot be a unit in $R/\mathfrak{m}$. $\square$

Corollary. Every maximal ideal is, in particular, a prime ideal.

Example. Let k be an algebraically closed field, and consider the quotient fields:

$$ev_a : k[x_1, ..., x_n] \to k; \;\; a = (a_1, ..., a_n) \in k^n$$

of the polynomial ring given by evaluation at a point $a \in k^n$. The kernel is:

$$\mathfrak{m}_a := \langle x_1 - a_1, ..., x_n - a_n\rangle$$

which is therefore a maximal ideal of the polynomial ring. We will eventually prove the (weak) *Hilbert Nullstellensatz*, which says these are the **only** maximal ideals.

Definition. An ideal $I \subset R$ is *radical* if $s^n \in I$ for some $n \geq 1$ implies that $s \in I$.

Note. Among ideals, maximal implies prime implies radical (but not vice versa).

Example. $n\mathbb{Z}$ is radical if and only if n has no square prime factors.

Definition. An element $r \in R$ is *nilpotent* if $r^n = 0$ for some $n \geq 1$ and a ring Q is *reduced* if $0 \in Q$ is the only nilpotent.

Then it is easy to check that:

$$\{\text{radical ideals } J \subset R\} \overset{IQ}{\leftrightarrow} \{\text{nilpotent quotients } q : R \to Q\}$$

under the IQ correspondence. Moreover:

Proposition 6. Every ideal $I \subset R$ is (uniquely) *radicalized* by the ideal:

$$I \subset \sqrt{I} = \{s \in R \mid s^n \in I \text{ for some } n \geq 1\}$$

Proof. If $s^n \in I$ and $t^m \in I$, then $(s+t)^{n+m-1} \in I$ and $(rs)^n \in I$. $\square$

Corollary. Every ring R can be (uniquely) reduced to $q : R \to R_{\text{red}} = R/\sqrt{0}$.

Example. $\mathbb{Z}/n\mathbb{Z}$ reduces to $\mathbb{Z}/m\mathbb{Z}$ where m is the product of the primes dividing n.

Finally, we turn to the question of:

The Existence of (Radical, Prime, Maximal) Ideals.

(0) If R is a field if and only if 0 is the only ideal in R.

Note. If R is not a field, then 0 is not maximal, so R has other ideals!

(1) If R_{red} is a field, if and only if $\sqrt{0}$ is the only radical ideal in R.

Proof. By Proposition 4, nestled ideals $\sqrt{0} \subset J \subset R$ correspond to ideals of R_{red}, so if R_{red} is not a field, then R has radical ideals $\sqrt{J} \neq \sqrt{0}$ and vice versa.

Note. There are many "interesting" rings for which R_{red} **is** a field. For example, $R = \mathbb{Z}/p^n\mathbb{Z}$ or $R = k[x_1, ..., x_n]/I$ where I contains all monomials of some degree

The existence of prime and maximal ideals, however, is more indirect.

(2) There are maximal ideals (hence prime ideals) in any ring R.

Proof. This relies on:

Zorn's Lemma. Let Λ be a partially ordered set with the property that every nonempty chain (totally ordered subset) in Λ has an upper bound in Λ. Then Λ contains maximal elements.

Note. This is equivalent to the axiom of choice for the set Λ.

Let Λ be the set of ideals $I_\lambda \subset R$, partially ordered by inclusion. Then any chain $\Gamma \subset \Lambda$ indexes *nested* ideals with an upper bound, namely the **union** ideal:

$$I_\Gamma := \bigcup_{\gamma \in \Gamma} I_\gamma$$

and so Zorn's Lemma applies.

Remark. If I_γ is an arbitrary set of ideals, then:

$$\bigcap_{\gamma \in \Gamma} I_\gamma$$

is always an ideal. The *union* is generally not an ideal if the ideals fail to be nested.