M3P8 Algebra III

Lectured by Dr David Helm
Typeset by David Kurniadi Angdinata

Autumn 2018

Contents

Lecture 1
Friday
05/10/18

0 Introduction

This course is an introduction to ring theory. The topics covered will include ideals, factorisation, the theory of field extensions, finite fields, polynomial rings in several variables, and the theory of modules.

In addition to the lecture notes, the following will cover much of the material we will be studying.

1. M Artin, Algebra, 1991

Rings are contexts in which it makes sense to add and multiply. For example, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, polynomials, functions $\{0,1\} \to \mathbb{R}$, and $\mathbb{Z}/n\mathbb{Z}$ are rings. The goals of this course include:

1. unify arguments that apply in all of the above contexts, and
2. study relationships between different rings.

The applications of rings include:

1. number theory - studying extensions of $\mathbb{Z}$ in which particular Diophantine equations have solutions, for example $n = x^2 + y^2 = (x + iy)(x - iy)$ to study solutions in $\mathbb{Z}\{i\}$ and pass to result about $\mathbb{Z}$,
2. algebraic geometry - study of zero sets of polynomials in several variables via rings of functions, and
3. topology - cohomology classes of topological space form a ring.

1 Basic definitions and examples

1.1 Rings

Recall the definition of a commmutative ring.

Definition 1.1. A **commutative ring with identity** R is a set together with two binary operations $+_R, \cdot_R : R \times R \to R$, addition and multiplication, and two distinguished elements 0_R and 1_R such that:

1. The operation $+_R$ makes R into an abelian group with identity 0_R:
   (a) for all $r \in R$, $0_R +_R r = r +_R 0_R = 0_R$ (additive identity),
   (b) for all $r, s, t \in R$, $(r +_R s) +_R t = r +_R (s +_R t)$ (associativity of $+_R$),
   (c) for all $r, s \in R$, $r +_R s = s +_R r$ (commutativity of $+_R$), and
   (d) for all $r \in R$, there exists $-r \in R$ such that $r +_R (-r) = (-r) +_R r = 0_R$ (additive inverses).
2. The operation $\cdot_R$ is associative and commutative with identity 1_R:
   (a) for all $r \in R$, $1_R \cdot_R r = r \cdot_R 1_R = 1_R$ (multiplicative identity),
   (b) for all $r, s, t \in R$, $(r \cdot_R s) \cdot_R t = r \cdot_R (s \cdot_R t)$ (associativity of $\cdot_R$), and
   (c) for all $r, s \in R$, $r \cdot_R s = s \cdot_R r$ (commutativity of $\cdot_R$).
3. Multiplication distributes over addition: for all $r, s, t \in R$, $r \cdot_R (s +_R t) = r \cdot_R s +_R r \cdot_R t$ and $(s +_R t) \cdot_R r = s \cdot_R r +_R t \cdot_R r$.

There is some redundancy here, of course. I have written things this way so that one obtains the definition of a noncommutative ring simply by removing the condition that multiplication is commutative. In this course, however, all rings will be commutative.

Proposition 1.2. Let R be a ring. Then for all $r \in R$, $r \cdot_R 0_R = 0_R$.

Proof. $r \cdot_R 0_R = r \cdot_R (0_R +_R 0_R) = r \cdot_R 0_R +_R r \cdot_R 0_R$. Thus $0_R = -(r \cdot_R 0_R) +_R (r \cdot_R 0_R) = -(r \cdot_R 0_R) +_R (r \cdot_R 0_R +_R r \cdot_R 0_R) = r \cdot_R 0_R$. □

Some people require $0_R \neq 1_R$ in R.

Proposition 1.3. If $0_R = 1_R$, then $R = \{0_R\}$.

Proof. $0_R = r \cdot_R 0_R = r \cdot_R 1_R = r$. □

When it is clear from the context what ring we are working with, we will write 0_R and 1_R as 0 and 1, $a +_R b$ as $a + b$ and $a \cdot_R b$ as ab.

Definition 1.4. A ring R is a **field** if $R \neq \{0_R\}$ and every nonzero element of R has a multiplicative inverse, that is for every $r \in R \setminus \{0_R\}$ there exists $r^{-1} \in R$ such that $rr^{-1} = r^{-1}r = 1_R$.

We do not consider the zero ring $\{0_R\}$ to be a field. We have seen many examples of rings at this point. The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all rings with their usual notion of addition and multiplication. All of them but $\mathbb{Z}$ are in fact fields. As another example, we have the ring $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n. Let $n \in \mathbb{Z}_{>0}$, and recall that a and b are said to be **congruent modulo** n if $a - b$ is divisible by n. It is easy to check that this is an equivalence relation on $\mathbb{Z}$. Moreover, since any $a \in \mathbb{Z}$ can uniquely be written as $qn + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < n$, the set $\{[0]_n, \ldots, [n-1]_n\}$ is a complete list of the equivalence classes under this relation, where $[a]_n$ denotes the set of all integers congruent to $a \mod n$. We denote this n-element set by $\mathbb{Z}/n\mathbb{Z}$, and we can define addition and multiplication in $\mathbb{Z}/n\mathbb{Z}$ by setting $[a]_n + [b]_n = [a+b]_n$ and $[a]_n [b]_n = [ab]_n$. This defines a ring structure on $\mathbb{Z}/n\mathbb{Z}$ once one checks that it is well-defined. This is the first example of a general construction of the quotient of a ring by an ideal we will define later.

Lecture 2
Monday
08/10/18

1.2 Polynomial rings

A very important class of rings that we will study are the polynomial rings. Let R be any ring. Then we can form a new ring $R[X]$, called the **ring of polynomials in X with coefficients in R**. Informally, a polynomial in $R[X]$ is a finite sum of the form $r_0 + \cdots + r_n X^n$ for some $n \in \mathbb{Z}_{\geq 0}$ and $r_i \in R$. If $n > m$, we consider $r_0 + \cdots + r_n X^n$ to represent the same polynomial of $R[X]$ as $s_0 + \cdots + s_m X^m$ if $r_i = s_i$ for $i \leq m$ and $r_i = 0_R$ for $i > m$. That is, you can pad out a polynomial with terms of the form $0_R X^i$ without changing it. From a formal standpoint, it is better to define a polynomial to be an infinite sum $\sum_{n=0}^{\infty} r_i X^i$ for $r_i \in R$ in which all but finitely many r_i are zero. This makes it easier to define addition and multiplication. The **degree** of such an expression is the largest i such that r_i is nonzero. We add and multiply in $R[X]$ just as we would any other polynomials, by

$$\left(\sum_{i=0}^{\infty} r_i X^i\right) +_{R[X]} \left(\sum_{i=0}^{\infty} s_i X^i\right) = \sum_{i=0}^{\infty} (r_i +_R s_i) X^i,$$

$$\left(\sum_{i=0}^{\infty} r_i X^i\right) \cdot_{R[X]} \left(\sum_{i=0}^{\infty} s_i X^i\right) = \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} (r_j \cdot_R s_{i-j})\right) X^i.$$

What about polynomial rings in more than one variable? Since the construction of polynomial rings takes an arbitrary ring as input, one can iterate it. Start with a ring R, and consider first the ring $R[X]$ and then the ring $(R[X])[Y]$. An polynomial of this has the form $\sum_{i=0}^{\infty} \left(\sum_{j=0}^{\infty} r_{ij} X^j\right) Y^i$ for $r_{ij} \in R$. On the other hand, we can consider the ring $(R[Y])[X]$, whose polynomials have the form $\sum_{i=0}^{\infty} \left(\sum_{j=0}^{\infty} s_{ij} Y^j\right) X^i$ for $s_{ij} \in R$. Alternatively, we could consider the ring $R[X, Y]$ whose polynomials are formal expressions of the form $\sum_{i=0}^{\infty} \left(\sum_{i=0}^{\infty} r_{ij} X^i\right) Y^j$ with only finitely many nonzero coefficients r_{ij} and define addition and multiplication in the usual way. It is not hard to see that all three approaches yield the same ring. There is a bijection between these expressions. We will therefore primarily use notation like $R[X, Y]$ for polynomial rings in multiple variables, but we will occasionally need to know that this is the same as $(R[X])[Y]$ or $(R[Y])[X]$. The identification we have made here is an example of an isomorphism of rings, a notion we will make precise later.

1.3 Subrings and extensions

Definition 1.5. Let R be a ring. A subset S of R is a **subring** of R if

1. $0_R, 1_R, -1_R \in S$.
2. S is closed under $+_R$ and $\cdot_R$, so if $r, s \in S$, then so are $r +_R s$ and $r \cdot_R s$.

Subrings inherit the additive and multiplicative structures from the ring that contains them, and are thus themselves rings.

Example. $\mathbb{Z}$ is a subring of $\mathbb{R}$, which is itself a subring of $\mathbb{C}$.

It is easy to see that the intersection of two subrings of R, or even an arbitrary collection of subrings of R, is also a subring of R.

Definition 1.6. Let $S \subseteq R$ be a subring of a ring R, and let α be an element of R. We can then form a subring $S[\alpha]$ of R, called the **subring of R generated by α over S**, consisting of all elements of R that can be expressed as $r_0 + \cdots + r_n\alpha^n$ for some $n \in \mathbb{Z}^*$, and $r_i \in S$.

This operation is known as **adjoining** the element α to the ring S. An alternative way of defining the ring $S[\alpha]$ is to note that it is the smallest subring of R containing S and α. In one direction, any such subring contains every expression of the form $r_0 + \cdots + r_n\alpha^n$, with $r_i \in S$, so any subring of R containing S and α contains $S[\alpha]$. One can thus construct $S[\alpha]$ as the intersection of every subring of R containing S and α. Since the intersection of any collection of subrings of R is a subring of R it is clear that this intersection is equal to $S[\alpha]$ as defined above.

Example. Let i denote a square root of -1 in $\mathbb{C}$. $\mathbb{Z} \subseteq \mathbb{C}$ and i form $\mathbb{Z}[i]$. Note $-1 = i^2 = i^6 = i + i^3 + i^{10}$.

Proposition 1.7. Every element of $\mathbb{Z}[i]$ can be uniquely expressed as $a + bi$ for $a, b \in \mathbb{Z}$.

Example. Given $\sum_{n=0}^{\infty} a_n i^n$ with only finitely many a_n nonzero, set $a = a_0 - a_2 + \ldots$ and $b = a_1 - a_3 + \ldots$. Then $\sum_{n=0}^{\infty} a_n i^n = a + bi$. For uniqueness, if $a + bi = c + di$ in $\mathbb{C}$ for $a, b, c, d \in \mathbb{Z}$, then $a = c$ or $b = d$.

If α is more complicated then the elements of $R[\alpha]$ may well be harder to describe.

Example. If α is the real cube root of 2, then every element of $\mathbb{Z}[\alpha]$ can be uniquely expressed as $a + b\alpha + c\alpha^2$ for $a, b, c \in \mathbb{Z}$.

Example. In $\mathbb{Z}[\pi]$, any element has a unique expression in the form $\sum_{n=0}^{\infty} a_n \pi^n$ for all but finitely many a_n are zero. Suppose $\sum_{n=0}^{\infty} a_n \pi^n = \sum_{n=0}^{\infty} b_n \pi^n$, then $0 = \sum_{n=0}^{\infty} (a_n - b_n)\pi^n$. Since π is transcendental, this polynomial must be zero. Thus each $a_n = b_n$.

Example. The elements of $\mathbb{Z}\left[\frac{1}{2}\right]$ can be expressed uniquely as a/b, where b is a power of 2 and a is odd unless $b = 1$.

Example. Let α be a root of $x^2 - \frac{1}{2}x + 1$. Then $\alpha^2 \in \mathbb{Z}[\alpha]$ and $\alpha^2 = \alpha/2 - 1$. Can show that every element of $\mathbb{Z}[\alpha]$ can be expressed as $a + b\alpha$ for $a, b \in \mathbb{Z}\left[\frac{1}{2}\right]$, but not every $a + b\alpha$ arises $a, b \in \mathbb{Z}\left[\frac{1}{2}\right]$.

Lecture 3
Wednesday
10/10/18

1.4 Integral domains and rings of fractions

Definition 1.8. A **zero divisor** in a ring R is a nonzero element r of R such that there exists a nonzero $s \in R$ with $rs = 0$. A ring R in which there are no zero divisors is called an **integral domain**.

Example. $\mathbb{Z}$ is an integral domain and any subring of a field is an integral domain, but $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain, as $[2]\,[3]$ is zero modulo 6 even though neither $[2]$ nor $[3]$ is zero modulo 6.

If R is an integral domain, then we can form the field of fractions of R in analogy to the way we build $\mathbb{Q}$ from $\mathbb{Z}$.

Definition 1.9. Let R be an integral domain. The **field of fractions** $K(R)$ is the set of equivalence classes of expressions of the form a/b for $a, b \in R$, $b \neq 0$, where $a/b \sim a'/b'$ iff $ab' = a'b$. We add and multiply elements of $K(R)$ just as we do for fractions, by

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}, \qquad \frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}, \qquad 0_{K(R)} = \frac{0_R}{1_R}, \qquad 1_{K(R)} = \frac{1_R}{1_R}.$$

If $a \neq 0$ in R, then $b/a \in K(R)$, so $(a/b) \cdot (b/a) = ab/ba \sim 1/1$.

Then $K(R)$ is a field, and it contains R in a natural way as a subring if we identify r with $r/1_R \in K(R)$. The field $K(R)$ is in some sense the smallest field containing R as a subring. When we talk about homomorphisms and isomorphisms, we will be able to state this more precisely. More generally, a subset S of R is a **multiplicative system** if $1 \in S$ and $0 \notin S$, and S is closed under multiplication, that is if a, b are in S then so is ab. For any integral domain R and any multiplicative system S, we can define $S^{-1}R \subseteq K(R)$ consisting of all fractions of the form a/b with $b \in S$. It is easy to see that his is closed under addition and multiplication, and defines a ring in between R and $K(R)$.

Example. If $R = \mathbb{Z}$ and S is the set of powers of 2, then $S^{-1}R = \mathbb{Z}\left[\frac{1}{2}\right]$. On the other hand, if S is the set of odd integers, then $S^{-1}R$ is the set of all rational numbers of the form a/b with b odd.

In general $S^{-1}R$ is the smallest subring of $K(R)$ containing R in which every element of S has a multiplicative inverse, that is $b^{-1} \in S$ for all $b \in S$. The process of obtaining $S^{-1}R$ from R is called **localisation** and is an extremely powerful tool. One can even make sense of it when R is not an integral domain, but one has to be more careful. The equivalence relation on fractions is tricker, for example. We will not discuss this in this course but it will be quite useful in future courses.

2 Homomorphisms, ideals, and quotients

2.1 Homomorphisms

Let R and S be rings. A ring homomorphism from R to S is, roughly, a way of interpreting elements of R as elements of S, in a way that is compatible with the addition and multiplication laws on R and S. More precisely is the following.

Definition 2.1. A function $f : R \to S$ is a **ring homomorphism** if

1. $f(1_R) = 1_S$,
2. for all $r, r' \in R$, $f(r +_R r') = f(r) +_S f(r')$, and
3. for all $r, r' \in R$, $f(r \cdot_R r') = f(r) \cdot_S f(r')$.

Note. If f is a homomorphism then $f(0_R) = f(0_R + 0_R) = f(0_R) +_S f(0_R)$ gives $f(0_R) = 0_S$. Thus we do not need to require this as an axiom. On the other hand we do need to require $f(1_R) = 1_S$. For certain R, S one can construct examples of maps $f : R \to S$ that satisfy properties 2 and 3 of the definition without satisfying property 1.

Example. If R is a subring of S, then the inclusion of R into S, such as $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, is a homomorphism. This is just a fancy way of saying that the addition and multiplication on R are induced from the corresponding operations on S.

Example. The composition of two homomorphisms is a homomorphism, as is easily checked from the definitions.

Example. The map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ that takes an integer m into its congruence class modulo n is also a homomorphism. In fact, this is a special case of the following construction.

Proposition 2.2. Let R be any ring. Then there is a unique ring homomorphism $f : \mathbb{Z} \to R$ such that

$$f(n) = \begin{cases} 1_R + \cdots + 1_R & n > 0 \\ -(1_R + \cdots + 1_R) & n < 0 \\ 0_R & n = 0 \end{cases}.$$

Proof. Let $f : \mathbb{Z} \to R$ be a homomorphism. Then, directly from the definition, we have $f(0) = 0_R$ and $f(1) = 1_R$. In particular for all $n > 0$, $f(n) = f(1 + \cdots + 1) = 1_R +_R \cdots +_R 1_R$, where there are n copies of 1_R in the sum. Moreover, $0_R = f(n + (-n)) = f(n) + f(-n)$, so $f(-n) = -(1_R +_R \cdots +_R 1_R)$. Thus $f(n)$ is determined, for all n, completely by the fact that f is a homomorphism. In the converse direction, it is not hard to check that the map defined above is in fact a homomorphism. □

Thus, for any ring R, we can regard an integer as an element of R via this homomorphism.

Definition 2.3. A bijective homomorphism $f : R \to S$ is called an **isomorphism**. Write $S \cong R$ for S is isomorphic to R.

In this case one verifies easily that the inverse map $f^{-1} : S \to R$ is also a bijective homomorphism.

2.2 Evaluation homomorphisms

Let R be a ring, and consider the ring $R[X]$ of polynomials in X with coefficients in R. If s is an element of R, then we can define a homomorphism $R[X] \to R$ by **evaluation at** s. More precisely, given an element of $R[X]$ of the form $P(X) = r_0 + \cdots + r_n X^n$ for some n and $r_i \in R$. Then $P(s)$ for $s \in R$ is defined to be $P(s) = r_0 + \cdots + r_n s^n \in R$. Consider the map $\phi_s : R[X] \to R$ that sends $\phi_s(P)$ to $P(s)$. In effect, it substitutes s for X. It is easy to check that this is in fact a ring homomorphism. More generally, if R and S are rings and $f : R \to S$ is a homomorphism, and s is an element of S, then we can define a map

$$\phi_{s,f} : R[X] \to S,$$

by setting

$$\phi_{s,f}(r_0 + \cdots + r_n X^n) = f(r_0) + \cdots + f(r_n) s^n.$$

That is, by appling f to the coefficients and substituting s for X. Again, this is clearly a homomorphism. The evaluation homomorphisms $\phi_{s,f}$ are a fundamental property of polynomial rings. In some sense, they are the reason polynomial rings are worth studying. In fact, the ring $R[X]$ is uniquely characterised by the fact that homomorphisms from $R[X]$ to S are in bijection with pairs (s, f), where $f : R \to S$ is a homomorphism and s is an element of S.

2.3 Images, kernels, and ideals

Definition 2.4. Let $f : R \to S$ be a homomorphism. The **image** of f is the subset $Im(f) = \{f(r) \mid r \in R\} \subseteq S$. The **kernel** of f is the subset $Ker(f) = \{r \in R \mid f(r) = 0\} \subseteq R$.

The image of a homomorphism $f : R \to S$ is easily seen to be a subring of S.

Example. If R is a subring of S, $f : R \to S$ is the inclusion and s lies in S, then the image of the map $\phi_{s,f} : R[X] \to S$ is precisely the subring $R[s]$ of S.

By contrast, the kernel of a homomorphism f is almost never a subring of R. For instance, subrings contain the identity. However, it is an ideal of R.

Lecture 4
Friday
12/10/18

Definition 2.5. A nonempty subset I of R is an **ideal** of R if I is closed under addition, that is for all $i, j \in I$, $i + j \in I$, and for all $i \in I$, $r \in R$, $ri \in I$.

Then one can verify, directly from the definition, that the kernel of any homomorphism $f : R \to S$ is an ideal of R.

Note. Any ideal of R contains 0_R, and conversely the subset $\{0_R\}$ of R is an ideal, called the **zero ideal**. A homomorphism $f : R \to S$ is injective if and only if its kernel is the zero ideal. Forward direction is easy. Conversely, if $f(x) = f(y)$, $f(x-y) = 0$, so $x - y \in Ker(f)$. If $Ker(f) = \{0\}$, $x = y$.

The kernel of the homomorphism $\mathbb{Z} \to R$ is either the zero ideal, or the ideal of multiples of n in $\mathbb{Z}$ for some positive n. We say that R has characteristic zero or characteristic n, respectively. If not zero, the characteristic of R is the smallest n such that the sum of n copies of 1_R is equal to zero.

2.4 Ideals: examples and basic operations

If r is an element of R, then any ideal containing R contains any multiple sr of R, for any r in S. Conversely, one checks easily that the set $\{sr \mid s \in R\}$ is an ideal of R. It is known as the **ideal of R generated by r**, and denoted $\langle r \rangle$. An ideal generated by one element in this way is called a **principal ideal**.

Note. The ideal generated by 1_R, or more generally by any element of R with a multiplicative inverse, is all of R. This ideal is called the **unit ideal** of R.

Proposition 2.6. R is a **field** iff the only ideals of R are the zero ideal $\{0\}$ and the unit ideal R.

Proof. If R is a field, let $I \subseteq R$ be a nonzero ideal. There exists $r \in I \neq 0$. Then for all $s \in R$, $\left(sr^{-1}\right)(r) \in I$, so $s \in I$ for all $s \in R$. Conversely, if R has only zero ideal, unit ideal, let $r \in R \neq 0$, let $I\{sr \mid s \in R\}$. This is an ideal not zero ideal, so it is all of R. In particular, $1 \in I$, so there exists $s \in R$ such that $sr = 1$. □

More generally is the following.

Definition 2.7. If S is a subset of elements of R, then any ideal containing S consists of all elements of R the form $r_0 s_0 + \cdots + r_n s_n$ for some $n \in \mathbb{Z}_{\geq 0}$, $r_i \in R$, and $s_i \in S$. The intersection of all these ideals is an ideal of R, known as the **ideal of R generated by S**, and denoted $\langle S \rangle$. It is also the smallest ideal of R containing S.

If S has one element, $\langle S \rangle$ is a principal ideal. We will show soon that any ideal of $\mathbb{Z}$ is a principal ideal, as is any ideal of the ring $k[X]$ for any field k. On the other hand, there are rings in which not every ideal is principal.

Example. The ideal $\langle X, Y \rangle$ of $k[X, Y]$ is not a principal ideal.

Given ideals I and J there are several ways to create new ideals.

1. If I, J are ideals, then the intersection $I \cap J$ is an ideal. If I and J are given by generators, it might be hard to find generators for the intersection. Certainly it is not enough to intersect the generating sets.
2. The union of ideals is not usually an ideal. Taking $R = \mathbb{Z}$, $\langle 3 \rangle \cup \langle 5 \rangle$ contains $3, 5$ but not $3 + 5$.
3. If I, J are ideals, then the sum $I + J$ is an ideal, which are all expressions of the form $i + j$ for $i \in I$, $j \in J$. It is the smallest ideal containing both I and J, and also the ideal generated by $I \cup J$.
4. If I, J are ideals, the product $I \cdot J$ or IJ is the ideal generated by elements of the form ij for $i \in I$, $j \in J$. This may be strictly larger than the set of such products.

Example. Consider the product of the ideals $I = \langle X, Y \rangle$ and $J = \langle Z, W \rangle$ in $R = k[X, Y, Z, W]$ for k a field. The product $IJ = \langle XZ, XW, YZ, YW \rangle$ contains $XZ + YW$, but the latter is not a product of an element in I with an element in J.

Note. Let I, J be general ideals. The product of I and J is always contained in the intersection of I and J, but the two need not be equal, even in simple rings like $\mathbb{Z}$. $\langle 3 \rangle \cdot \langle 3 \rangle = \langle 9 \rangle \subseteq \mathbb{Z}$ and $\langle 3 \rangle \cap \langle 3 \rangle = \langle 3 \rangle$.

2.5 Quotients

Let R be a ring and let I be an ideal of R. If x, y are elements of R, we say that x is **congruent to** y **modulo** I if $x-y$ is in I. This is an equivalence relation on R. We denote the equivalence class of r by $r+I$, or the alternative notations $[r]_I$, $\overline{r}$. It is the set $\{r+s \mid s \in I\}$. Let R/I denote the set of equivalence classes on R modulo I. This set has the natural structure of a ring. The additive and multiplicative identities are 0_R+I and 1_R+I, respectively, and addition and multiplication are defined by $(r+I)+(s+I)=(r+s)+I$ and $(r+I)\cdot(s+I)=(rs+I)$ respectively. One has to check that these are well-defined, but this is not difficult. The ring R/I is called the **quotient** of R by the ideal I.

Example. If $R=\mathbb{Z}$ and I is the ideal generated by n, then R/I is the ring $\mathbb{Z}/n\mathbb{Z}$ that we have already seen.

Note. There is a **reduction modulo** I or **natural quotient** homomorphism $R \to R/I$ defined by taking r to $r+I$. This homomorphism is surjective with kernel I.

We then have the following.

Proposition 2.8. Let $I \subseteq R$ be an ideal and let $f : R \to S$ be a homomorphism, and suppose that the kernel of f contains I. Then there is a unique homomorphism $\overline{f} : R/I \to S$ such that for all $r \in R$, $\overline{f}(r+I)=f(r)$.

This is called the **universal property of the quotient**.

Proof. $\overline{f}$ is necessarily unique, as every element of R/I has the form $r+I$ for some r. It thus suffices to show that it is well-defined and gives a homomorphism. If $r+I=r'+I$, then $r-r' \in I$, so $f(r-r')=0$ gives $f(r)=f(r')$. Thus $\overline{f}$ is well-defined. Checking that it is a homomorphism follows from f is a homomorphism. □

Note. The kernel of $\overline{f}$ in the above proposition is just the image of the kernel of f in R/I. If the kernel of f is equal to I, this image is the zero ideal and $\overline{f}$ is injective. In particular, any homomorphism of R to S can be thought of as an isomorphism of some quotient of R with a subring of S.

Example. Let $R \subseteq S$ be a subring, $\alpha \in S$, and $\iota : R \to S$ be the inclusion map. Recall that we have an evaluation at α by $\phi_{\iota,\alpha} : R[X] \to S$. Image of this is $R[\alpha]$. Let $I = Ker(\phi_{\iota,\alpha})$. Then $\phi_{\iota,\alpha}$ descends to a map $\phi_{\iota,\alpha} : R[\alpha]/I \to S$ that is injective with image $R[\alpha]$. So $R[\alpha]$ is isomorphic to a quotient of $R[X]$.