MSM203a: Polynomials and rings
Chapter 2: Quotients, ideals and homomorphisms

Richard Kaye

Autumn 2013*

Note: These printed handouts are summary sheets and are intended to supplement the material provided in lectures. They are not sufficient on their own.

1 Equivalence relations and partitions

Definition 1.1. Let X be a nonempty set. An equivalence relation $\sim$ on X is a relation on X (i.e. a set of pairs $\sim \subseteq X \times X$) satisfying the axioms of reflexivity, symmetry and transitivity.

Rather than writing $(x, y) \in \sim$ we write $x \sim y$.

Instead of a relation being a 'rule' it is defined as a set. This is more precise and more general than talking about 'rules'. Notice also that the equivalence relation $\sim$ on the set X depends just as much on what the set X is as what $\sim$ is. If you change X everything changes, and we no longer have the same equivalence relation.

Example 1.2. Let X be any set. Then the equality relation $=$ on X is an equivalence relation on X.

The key example of an equivalence relation is the next one.

Example 1.3. Suppose we have a function $f\colon X \to Y$ and we define $x \sim y$ to mean $f(x) = f(y)$. Then $\sim$ is an equivalence relation on X. For $y \in Y$ in the image of f, we define the set $f^{-1}\{y\}$ by

$$f^{-1}\{y\} := \{x : f(x) = y\}.$$

$f^{-1}\{y\}$ is called a *fibre* of f (or *the fibre of* f *above* y or *at* y).

Example 1.4. Let $X = \mathbb{Z}$ and define $\sim$ on X by $x \sim y$ if and only if $x - y$ is divisible by 5. This is an equivalence relation on $\mathbb{Z}$.

Definition 1.5. Let X be a nonempty set and $\sim$ an equivalence relation on X. We denote by $[x]$ (or by $x/\!\sim$ or $[x]_\sim$) the *equivalence class* of $x \in X$, i.e. the set

$$[x] := \{y \in X : x \sim y\}.$$

Example 1.6. For equivalence modulo 5 on $\mathbb{Z}$ the equivalence classes are

$$[0] = \{\ldots, -5, 0, 5, 10, \ldots\},\ [1] = \{\ldots, -4, 1, 6, 11, \ldots\},\ [2] = \{\ldots, -3, 2, 7, 12, \ldots\},$$
$$[3] = \{\ldots, -2, 3, 8, 13, \ldots\},\ [4] = \{\ldots, -1, 4, 9, 14, \ldots\}.$$

The notation $[x]$ is useful when it is easily understood from context which equivalence relation is being considered. The notations $x/\!\sim$ or $[x]_\sim$ are better if there is more than one possible equivalence relation and we need to specify which we mean. You may use any of these, but you may need to avoid ambiguity if you use $[x]$.

*Version 2.1 of 2011-10-12

Definition 1.7. If $\sim$ is an equivalence relation on X, then $X/\sim$ denotes the set of equivalence classes, i.e.

$$X/\sim := \{[x] : x \in X\}.$$

Proposition 1.8. Let X be a nonempty set and $\sim$ an equivalence relation on X. Then for $x, y \in X$ we have:

(a) $x \in [x]$;

(b) if $[x] \cap [y] \neq \varnothing$ then $[x] = [y]$;

(c) $[x] = [y]$ if and only if $x \sim y$.

Definition 1.9. Let X be a nonempty set. A *partition* of X is a set Q of subsets of X such that

(a) Each $A \in Q$ is nonempty.

(b) Each $x \in X$ is a member of exactly one $A \in Q$.

Thus if $\sim$ is an equivalence relation on X then the set of equivalence classes $X/\sim$ is a partition of X. Partitions and equivalence relations are essentially the same thing: one can turn an equivalence relation $\sim$ into a partition $X/\sim$. Conversely one can turn a partition Q of X into an equivalence relation by saying $x \sim_Q y$ holds if and only if x and y are in exactly the same sets $A \in Q$.

Exercise 1.10. Let Q be a partition of X. Show that $x \sim_Q y$ as just defined is an equivalence relation. Show that the $\sim_Q$-equivalence classes are precisely the sets in Q.

An equivalence relation is a bit like a weak form of equality $=$. Many equivalence relations are derived from equality as we saw in Example 1.3. In fact we can now prove that *every* equivalence relation can be derived in this way using a suitable function.

Proposition 1.11. Let $\sim$ be an equivalence relation on a set X. Then there is a set Y and a function $f\colon X \to Y$ such that $x \sim y \Leftrightarrow f(x) = f(y)$ for all $x, y \in X$.

Proof. Let $\sim$ be an equivalence on X, and let $Y = X/\sim$. Define $f\colon X \to Y$ by $f(x) = [x] \in Y$. Then $x \sim y$ if and only if $[x] = [y]$, that is $f(x) = f(y)$. □

To summarise: given X and an equivalence relation $\sim$ on X we have *partitioned* the set X into subsets called $\sim$-*equivalence classes*. Then we defined a function $f\colon X \to X/\sim$ in the only sensible way possible, by $f(x) := [x]$, and observed that the $\sim$-equivalence classes are the *fibres* $f^{-1}\{y\} = \{x : f(x) = y\}$ of f.

In simpler language, the elements of X are *shared* around the different equivalence classes. This 'sharing' *really is* 'division'. Such divisions and quotients appear a lot in ring theory.

There is one further important but mildly tricky aspect of equivalence classes that we need. Suppose X is a set, $\sim$ is an equivalence on X and $Y = X/\sim$. We often want to define an operation on Y, that is a function $f\colon Y \to Y$. Suppose we already have an operation $F\colon X \to X$ on X and want to define

$$f(x/\sim) := (F(x))/\sim$$

or if you prefer $f([x]) := [F(x)]$. *This might not work.* The problem is that it might be the case that two distinct $x, y \in X$ are equivalent (so $x/\sim = y/\sim$, that is $x \sim y$) but $F(x)$ and $F(y)$ are not equivalent (i.e. $F(x)/\sim \neq F(y)/\sim$, that is $F(x) \not\sim F(y)$). Why is this a problem? Well, our recipe above says to put $f(x/\sim) = (F(x))/\sim$ and also $f(y/\sim) = (F(y))/\sim$. But $x/\sim = y/\sim$ are the same equivalence class, so we had better have $f(x/\sim) = f(y/\sim)$ since f is a function. On the other hand $F(x)/\sim \neq F(y)/\sim$ so these values are *not* the same. Functions must assign a unique value to each element on the domain.

But this is the only obstruction, and the following is true.

Proposition 1.12. Suppose X is a set, $\sim$ is an equivalence on X and $Y = X/\sim$. Suppose $F\colon X \to X$. Then

$$f(x/\sim) := (F(x))/\sim$$

defines a function $f\colon Y \to Y$ if and only if

$$\text{for all } x, y \in X,\ x \sim y \text{ implies } F(x) \sim F(y).$$

A similar version of this works for binary operations.

Proposition 1.13. Suppose X is a set, $\sim$ is an equivalence on X and $Y = X/\sim$. Suppose $F\colon X \times X \to X$. Then

$$f(x_1/\sim, x_2/\sim) := (F(x_1, x_2))/\sim$$

defines a function $f\colon Y \times Y \to Y$ if and only if

$$\text{for all } x_1, y_1, x_2, y_2 \in X,\ x_1 \sim y_1 \text{ and } x_2 \sim y_2 \text{ implies } F(x_1, x_2) \sim F(y_1, y_2).$$

2 Homomorphisms

We now return to rings. The first objective is to compare two rings and say when they are 'similar' or even 'the same'. This is done with functions. This section looks at such functions between two rings. The link with equivalence classes will come later.

Definition 2.1. Let R, S be rings each with its own addition and multiplication. A *homomorphism* $f\colon R \to S$ is a function $f\colon R \to S$ that carries the addition and multiplication structure, in the following sense.

(a) $f(0) = 0$, that is f takes the zero in R to the zero of S.

(b) for all $x, y \in R$, $f(x + y) = f(x) + f(y)$. (Here $+$ on the left is addition in R and $+$ on the right is addition in S.)

(c) for all $x, y \in R$, $f(x \cdot y) = f(x) \cdot f(y)$. (Here $\cdot$ on the left is multiplication in R and $\cdot$ on the right is multiplication in S.)

This tells us how to recognise rings which are 'the same'.

Definition 2.2. A homomorphism $f\colon R \to S$ that is injective and surjective is called an *isomorphism*. If there is such an isomorphism then R, S are *isomorphic* rings and we write $R \cong S$.

Example 2.3. Let $R = \mathbb{Z}$, $S = \mathbb{Z}_6$ and define $f(n) := [n] \in \mathbb{Z}_6$ for $n \in \mathbb{Z}$. Then $f\colon \mathbb{Z} \to \mathbb{Z}_6$ is a homomorphism. Note that $\{n \in \mathbb{Z} : f(n) = 0\} = 6\mathbb{Z}$.

Example 2.4. Let $R = \mathbb{Z}[X]$ and $S = \mathbb{Z}[i]$. Define $f(p(X)) := p(i) \in \mathbb{Z}[i]$. Then $f\colon \mathbb{Z}[X] \to \mathbb{Z}[i]$ is a homomorphism. The set $I = \{p(X) \in \mathbb{Z}[X] : p(i) = 0\}$ can be identified as follows. Consider a general $p(X) \in I$. Since $p(i) = 0$ and $\mathbb{Z}[X]$ is an integral domain we must have that $p(X)$ is divisible by $(X - i)$. But $p(X) \in \mathbb{Z}[X]$ has only real coefficients so $p(X)$ is divisible by $(X - i)(X + i) = (X^2 + 1)$. The converse holds too, and is rather easier. So I consists of the polynomials $p(X) \in \mathbb{Z}[X]$ divisible by $X^2 + 1$.

Example 2.5. More generally, suppose R is a subring of S, $a \in S$ and define $f\colon R[X] \to S$ by $p(X) \mapsto p(a)$. Then this is a homomorphism.

The last example in the case $R = S$ says that 'evaluation of polynomials at $X = a$' is a homomorphism from $R[X]$ to R. This map takes a general polynomial and evaluates it. Polynomials behave as numbers here!

Example 2.6. Compare this with the map that evaluates a *particular* polynomial at a *general* element of the ring. For example, if $R = \mathbb{Z}$ and $p(X)$ is the polynomial $(X+1) \in \mathbb{Z}[X]$ then the map $v_p\colon \mathbb{Z} \to \mathbb{Z}$ given by $v_p(n) := p(n)$ is not a homomorphism.

Exercise 2.7. For which polynomials $p(X)$ in $\mathbb{Z}[X]$ is the function $v_p\colon \mathbb{Z} \to \mathbb{Z}$ a homomorphism?

A homomorphism $f\colon R \to S$ gives us some useful subrings of R, S to work with.

Proposition 2.8. Given a homomorphism $f\colon R \to S$ of rings, the set

$$\operatorname{im} f := \{s \in S : \exists r \in R\ s = f(r)\}$$

of elements in the image of f is a subring of S. Also, the kernel of f,

$$\ker f := \{r \in R : f(r) = 0\}$$

is a subring of R.

Definition 2.9. A ring homomorphism $f\colon R \to S$ is a surjection if and only if $\operatorname{im} f = S$.

Proposition 2.10. A ring homomorphism $f\colon R \to S$ is an injection if and only if $\ker f = \{0\}$.

Definition 2.11. An injective homomorphism is often called *monomorphism*. A surjective homomorphism is a *epimorphism*.

Given a ring homomorphism $f\colon R \to S$, it is natural to consider the equivalence relation

$$x \sim_f y :\Leftrightarrow f(x) = f(y).$$

This equivalence relation only depends on the kernel of f, and can be read off as follows.

Proposition 2.12. Given a ring homomorphism $f\colon R \to S$ and any $x, y \in R$ we have

$$f(x) = f(y) \Leftrightarrow x - y \in \ker f.$$

3 Ideals

Kernels have an extra property not always enjoyed by subrings in general.

Definition 3.1. A subset $I \subseteq R$ of a ring R with the properties

(a) for all $x, y \in I$, $x + y \in I$

(b) for all $x \in I$, $-x \in I$

(c) for all $x \in I$ and $y \in R$, both $xy, yx \in I$

is called a (two sided) ideal[1]. Part (c) is rather stronger than the closure of I under multiplication. We write $I \lhd R$ to mean I is an ideal of R.

Example 3.2. In the polynomial ring $R = \mathbb{Z}[X]$ over the integers, the set S of 'constant' polynomials $a + 0X + 0X^2 + \cdots$ is a subring isomorphic to $\mathbb{Z}$ (check closure!) but is not an ideal since $1 \cdot X = X$ is not in S even though $1 \in S$ and $X \in R$.

Example 3.3. Any ring R has ideals $\{0\}$ and R itself. These are called *improper* ideals.

Proposition 3.4. Given a homomorphism $f\colon R \to S$, the kernel $\ker f$ is an ideal of R.

Example 3.5. For any $n \in \mathbb{Z}$ the set $n\mathbb{Z} := \{nz : z \in \mathbb{Z}\}$ is an ideal of the ring $\mathbb{Z}$ with the usual addition and multiplication.

Exercise 3.6. If R is a ring with 1, every ideal $I \lhd R$ containing 1 is improper.

Proposition 3.7. Given $I \lhd R$, if R is a field then $I = \{0\}$ or $I = R$. In other words, a field has no proper ideals.

Ideals are considerably more complicated when the ring is not commutative. The next example is very important, and the version given here works in the commutative case only.

Example 3.8. If R is a *commutative* ring and $a \in R$, the set $\{ar : r \in R\}$ is an ideal of R. It is denoted by (a) or aR (or, since R is commutative, it could even be written Ra). This ideal is called the *principal ideal generated by* a.

Example 3.9. If $n \in \mathbb{Z}$ the ideal (n) of $\mathbb{Z}$ is $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$.

Proposition 3.10. If I, J are ideals of R so is $I + J := \{a + b : a \in I, b \in J\}$.

[1] All ideals in this course will be two-sided.

4 Quotients of rings

We now look at what happens when we divide R using the equivalence relation $\sim_f$, where $f\colon R \to S$ is a ring homomorphism. By Proposition 2.12 we can forget about f itself, and only need to consider $I = \ker f$.

Definition 4.1. Given an ideal $I \lhd R$ we say that $x, y \in R$ *are congruent modulo* I or $x \equiv y \bmod I$ if $x - y \in I$.

Proposition 4.2. For an ideal $I \lhd R$, congruence modulo I is an equivalence relation. (In fact the 'ideal' property is not needed here and it suffices that I is a subring of R.)

Example 4.3. For $R = \mathbb{Z}$ and $I = n\mathbb{Z}$, congruence modulo I is nothing else but the familiar congruence modulo n.

Proposition 4.4. Given $I \lhd R$ and $x \in R$, the equivalence class of x modulo I is the set $\{x + i : i \in I\}$.

Definition 4.5. Given $I \lhd R$, the equivalence class $\{x + i : i \in I\}$ of $x \in R$ is denoted $x + I$ and the set of all equivalence classes is denoted R/I. R/I is the *quotient of* R *by* I.

Proposition 4.6. Given $I \lhd R$, the binary operations of addition and multiplication on R/I given by

$$(x + I) + (y + I) := (x + y) + I$$

and

$$(x + I) \cdot (y + I) := (x \cdot y) + I$$

are well-defined. They make R/I into a ring.

It is precisely the last proposition that goes wrong when one tries to quotient out by an arbitrary subring rather than an ideal.

Example 4.7. Let $R = \mathbb{Z}[X]$ and let I be the *subring* $\mathbb{Z}$ of R. We want to define $(p(X) + I)(q(X) + I) = p(X)q(X) + I$. But this doesn't work. Let $p(X) = q(X) = X + 1$. Then $p(X)q(X) = x^2 + 2X + 1$ so $(p(X) + I)(q(X) + I)$ should be $X^2 + 2X + 1 + I$. But $p(X) \equiv X \bmod I$ since $P(X) - X = 1 \in \mathbb{Z}$. And $(X + I)(X + I)$ should be $X^2 + I$. So if all is well we would have to have $X^2 + 2X + 1 + I = X^2 + I$ or in other words $X^2 + 2X + 1 \equiv X^2 \bmod I$. But this is false since $X^2 + 2X + 1 - X^2 = 2X + 1 \notin \mathbb{Z}$.

The 'ideal' property is specially designed to ensure that problems like this do not happen and multiplication can be defined adequately on quotient rings.

Proposition 4.8. Given $I \lhd R$, if R is a commutative ring with 1 then so is R/I.

Example 4.9. Given $I \lhd R$, even if R is an integral domain, R/I need not be an integral domain. For example if $R = \mathbb{Z}$ with the usual addition and multiplication, and $I = 6\mathbb{Z}$ then $\mathbb{Z}/6\mathbb{Z}$ has zero divisors [2] and [3].

Example 4.10. Given a commutative ring R and a polynomial $p(X) \in R[X]$ we can form the principal ideal $(p(X)) \lhd R[X]$ and the quotient ring $R[X]/(p(X))$.

5 Isomorphism theorems

We are interested here in homomorphisms, quotients and general connections between the two.

Example 5.1. Given a ring R there are homomorphisms $i\colon R \to R$ given by $i(r) := r$ and $z\colon R \to R$ given by $z(r) := 0$. (For many rings there will be other homomorphisms besides these.) These have $\ker i = \operatorname{im} z = \{0\}$ and $\ker z = \operatorname{im} i = R$.

Exercise 5.2. Let R be a ring. Then the ring $R/\{0\}$ is isomorphic to R, and the ring R/R is isomorphic to $\{0\}$.

Next, we suppose we already have an ideal $I \lhd R$ of R.

Example 5.3. Given a ring R and an ideal $I \lhd R$ of R the map F defined by

$$F(r) := r + I$$

is well-defined and is a homomorphism from R to R/I which is onto. Also, $I = \ker F$.

Given a homomorphism $f\colon R \to S$ we want to try to relate the rings R, S to $\ker f$. There are versions of the theorem that does this for all sorts of algebraic structures (most notably groups and vector spaces) which you may see elsewhere. The following is the version for rings.

Theorem 5.4 (First isomorphism theorem)**.** Suppose $f\colon R \to S$ is a homomorphism of rings. Then

$$R/\ker f \cong \operatorname{im} f.$$

The proof is given in lectures. It is 100% 'natural' in the sense that, as long as you understand what the statement of the result says and what you need to do, there is only one way to define the isomorphism and prove it has the properties required.

Example 5.5. Given a ring R and an ideal $I \lhd R$ we have seen that there is a surjective homomorphism $R \to R/I$ given by $x \mapsto x + I$. The 'naturality' of the first isomorphism theorem says that all surjective homomorphisms look like this, i.e. if $F\colon R \to S$ is a surjective homomorphism then $S \cong R/I$ where $I = \ker F$ and also that the homomorphisms $F\colon R \to S$ and $R \to R/I$ 'look exactly the same'.[2]

There are other isomorphism theorems. For completeness' sake we state them all here, but the proofs, whilst not hard, are longer and slightly technical, and are not examinable in totality. (So you won't get an exam question like 'state and prove the second isomorphism theorem'. But you may be asked in a more directed way to prove parts of it.)

The second isomorphism theorem says $(S + I)/I \cong S/(S \cap I)$. That's how you remember it, but there are few extra parts that say the notation makes sense.

Theorem 5.6 (Second isomorphism theorem)**.** Let R be a ring, S a subring of R and I be an ideal of R. Then

(a) The sum $S + I = \{s + i : s \in S, i \in I\}$ is a subring of R

(b) The intersection $S \cap I$ is an ideal of S, and

(c) The quotient rings $(S + I)/I$ and $S/(S \cap I)$ are isomorphic.

The third isomorphism theorem says $(R/B)/(A/B) \cong R/A$, showing in a rather pretty way how the division notation works out nicely.

Theorem 5.7 (Third isomorphism theorem)**.** Let R be a ring. Let A and B be ideals of R, with $B \subseteq A \subseteq R$. Then

(a) The set A/B is an ideal of the quotient R/B, and

(b) The quotient ring $(R/B)/(A/B)$ is isomorphic to R/A.

The correspondence theorem is sometimes called 'the fourth isomorphism theorem' and describes intermediate subrings.

Theorem 5.8 (Correspondence theorem)**.** Let I be an ideal of a ring R. There is a bijection ϕ from the set of subrings of R containing I and the set of subrings of R/I. The bijection preserves inclusion ($S_1 \subseteq S_2 \Leftrightarrow \phi(S_1) \subseteq \phi(S_2)$), and ideals of R containing I correspond to ideals of R/I.

[2] In other words these homomorphisms are also 'isomorphic', though the definitions required to explain this go beyond the scope of this course and will not be given.