Modern Algebra Lecture Notes: Rings and fields set 2, revision 2

Kevin Broughan

University of Waikato, Hamilton, New Zealand

May 6, 2010

Ring homomorphism

Let R and S be rings, not necessarily distinct. A ring homomorphism is a function $f : R \to S$ such that for all $a, b \in R$ we have

$$f(a+b) = f(a) + f(b), \quad f(ab) = f(a)f(b),$$

where the operations on the left are those of R and on the right those of S.

Ring isomorphism

If a ring homomorphism is both one-to-one (injective) and onto (surjective) then we say the function is a ring isomorphism and that R and S are isomorphic rings.

Examples

(1) Define a function $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by the rule $x \to [x]$. Then this is a homomorphism which is onto but not injective.

(2) The function $g : \mathbb{C} \to \mathbb{C}$ defined by $x + iy \to x - iy$ is a ring isomorphism of the complex numbers.

(3) If R is a commutative ring with $\mathrm{char}\ R = 2$ then the map $x \to x^2$ is a ring homomorphism of R.

(4) The additive groups $\mathbb{Z}$ and $3\mathbb{Z}$ are isomorphic via $x \to 3x$ which is injective and surjective, but not isomorphic as rings, **since Z has an identity but $3\mathbb{Z}$ does not**.

Definition of a kernel

Let $f : R \to S$ be a homomorphism of rings. Define

$$\text{Ker } f = \{x \in R : f(x) = 0\}.$$

Theorem 7

The kernel K of f is an **ideal** of R. Conversely if I is an ideal in R the natural map $f : R \to R/I$ is a **homomorphism** with kernel I

Proof of Theorem 7

If $x, y \in K$ then $f(x+y) = f(x) + f(y) = 0 + 0 = 0$ so $x + y \in K$.

If $x \in K$ and $r \in R$ then $f(r.x) = f(r).f(x) = f(r).0 = 0$ and similarly, $f(x.r) = 0$ so $r.x \in K$ and $x.r \in K$.

Therefore K is an ideal of R.

Conversely we have $f(r) = [r] = r + I$ for each $r \in R$. Then $r \in I$ if and only if $r + I = I = 0 + I = [0]$. Therefore I is the kernel of f.

Isomorphism Theorem for rings

Theorem 8

Let $f : R \to S$ be any ring homomorphism. Then $f(R) \subset S$ is a subring. Let K be the kernel of f. Then the mapping

$$g : R/K \to f(R)$$

defined by $x + K \to f(x)$ is a ring isomorphism.

Proof of Theorem 8

If $u, v \in f(R)$ then $\exists x, y \in R$ so $u = f(x),\ v = f(y)$ and then $u + v = f(x) + f(y) = f(x + y) \in f(R)$. Similarly $u.v \in f(R)$ so $f(R)$ is a subring.

Let $x - y \in K$ so $[x] = [y]$. Then $g([x]) = g([y])$ iff $f(x) = f(y)$ iff $f(x - y) = 0$ iff $x - y \in K$ iff $[x] = [y]$. Therefore g is well defined. And the part of this from "Then" shows that g is one-to-one or injective.

Since the image of g coincides with that of f, namely $f(R)$, g is an isomorphism

$$R/K \approx f(R).$$

Note:

A homomorphism $f : R \to S$ is injective $\iff \operatorname{Ker} f = \{0\}$.

Theorem 9

Let R be a ring with identity 1. Then the function $f : \mathbb{Z} \to R$ defined by $n \to n.1$ (1 or -1 added to itself n times, or if $n = 0$, just the 0 of the ring) is a ring homomorphism.

Proof

If $n, m \geq 1$ then $f(n+m) = (n+m).1$ which is the sum of $n+m$ copies of 1, which can be written as the sum of n copies of 1 followed by m copies of 1, which is just $f(n) + f(m)$. Therefore $f(n+m) = f(n) + f(m)$ in this case. Similarly $f(nm) = f(n).f(m)$.

If $n = 0, m > 0$ then $f(n+m) = f(m)$ which is m copies of 1 added in R which is $0 + f(m)$.

If $n < 0$ we note that $f(n) = -1 - 1 - \cdots - 1 = -(1 + 1 + \cdots + 1) = -f(-n)$ and we can use this when n or m are negative.

Theorem 10

Let R be a ring with identity 1 and characteristic $n > 0$. Then R contains a subring isomorphic to $\mathbb{Z}/nZ$. If R has characteristic 0 it contains a subring isomorphic to $\mathbb{Z}$.

Proof

Use the map $f(m) = m.1$ defined in Theorem 9. Let $K = \mathrm{Ker}\ f$. We see that

$$m \in K \iff f(m) = 0 \iff m.1 = 0 \iff n \mid m \iff m \in n\mathbb{Z}.$$

Hence, by Theorem 8, $\mathbb{Z}/n\mathbb{Z} \approx f(\mathbb{Z}) \subset R$, which is a subring. Hence R contains a subring isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

Characteristic Zero

In this case $f(n) = n.1$ is an ismorphism $\mathbb{Z} \approx f(\mathbb{Z})$ since $f(n) = 0 \implies n = 0$.

Theorem 11

Any field contains a copy of one of $\mathbb{Z}/p\mathbb{Z}$ (p a prime) or $\mathbb{Q}$.

Proof

Let F be a field. Then F is a commutative ring with a 1 which is such that every non-zero element has a multiplicative inverse.

So let $ab = 0$ in F and suppose $a \neq 0$. Then $b = a^{-1}.a.b = a^{-1}.0 = 0$, so F is always an integral domain.

Therefore, by Theorem 3, its characteristic is either a prime p or is zero. Therefore, by Theorem 10, it contains a subring isomorphic to $\mathbb{Z}/p\mathbb{Z}$ or to $\mathbb{Z}$ respectively.

Proof of Theorem 11 in characteristic zero

Statement

Any field F of characteristic zero contains a copy of $\mathbb{Q}$.

Define a mapping $\theta : \mathbb{Q} \to F$ by

$$\theta\left(\frac{m}{n}\right) := (m.1)(n.1)^{-1}.$$

We need to show that θ is well defined, that it is a ring homomorphism, and that it is injective.

θ is well defined:

$$\begin{aligned} \theta(m/n) &= \theta(m'/n') \iff (m.1)(n.1)^{-1} = (m'.1)(n'.1)^{-1} \\ &\iff (m.1)(n'.1) = (m'.1)(n.1) \iff (mn'.1) = (nm'.1) \\ &\iff mn' = nm' \iff \frac{m}{n} = \frac{m'}{n'}. \end{aligned}$$

θ is a homomorphism:

$$\begin{aligned}
\theta\left(\frac{m}{n}+\frac{r}{s}\right) &= \theta\left(\frac{ms+nr}{ns}\right) \\
&= ((ms+nr).1)(ns.1)^{-1} \\
&= ((ms.1)+(nr.1))(ns.1)^{-1} \\
&= (ms.1)(ns.1)^{-1}+(nr.1)(ns.1)^{-1} \\
&= (m.1)(s.1)((n.1)(s.1))^{-1}+(n.1)(r.1)((n.1)(s.1))^{-1} \\
&= \cdots = \theta\left(\frac{m}{n}\right)+\theta\left(\frac{r}{s}\right).
\end{aligned}$$

θ is injective:

$\theta(\frac{m}{n}) = 0 \iff (m.1)(n.1)^{-1} = 0 \iff (m.1) = 0 \iff m = 0.$

Theorem 12

Let R be an integral domain, commutative with 1. then R is isomorphic to a subring of a field F, namely the so called field of quotients of R.

Proof

Define a set $S = \{(x, y) : x, y \in R,\ y \neq 0\}$ and a relation $\sim$ on S by $(x, y) \sim (x', y') \iff xy' = yx'$ in R.

Then $\sim$ is reflexive, symmetric and transitive, i.e. an equivalence relation. Let the set of equivalence classes $[(x, y)]$ be denoted by $F = S/\sim$.

Then we can define natural operations $+$ and . on F making it a field, and the mapping

$$\theta : R \to F \text{ defined by } \theta(x) := [(x, 1)]$$

is an injective homomorphism. Thus R is isomorphic to a subring of F.

Some details for Theorem 12

The algebraic operations

Define $[(x,y)]+[(u,v)] := [(xv+yu, yv)]$ and $[(x,y)].[(u,v)] := [(xu,yv)]$.

These are well defined

We need to show they are independent of the representatives: for "."
Let $(x,y) \sim (x',y')$ and $(u,v) \sim (u',v')$. Then

$$\begin{aligned} xy' &= yx',\ uv' = vu' \\ xy'uv' &= yx'vu' \implies xuy'v' = yvx'u' \\ \implies & \quad (xu,yv) \sim (x'u', y'v') \implies [(xu,yv)] = [(x'u', y'v')] \end{aligned}$$

θ is injective:

In F, $0 = [(0,1)]$, so

$$\theta(x) = 0 \implies [(x,1)] = [(0,1)] \implies x.1 = 1.0 = 0$$

so $x = 0$ in R.