Lecture 5 — Homomorphisms

Dr. D. Bernhard

In this lecture: homomorphisms — isomorphisms — automorphisms and their group — application to groups, rings and fields

Learning outcomes. After this lecture and revision, you should be able to:

- Define homomorphisms and isomorphisms and give examples.
- Check, for simple examples, whether two structures are isomorphic and find an isomorphism if they are.
- Determine the isomorphism class of finite Abelian groups.
- Find integers with given remainders modulo different coprime moduli.
- Compute the Frobenius map in a ring and the inverse of an element in a finite field.

5 Homomorphisms

Imagine you're trying to solve a sudoku puzzle. Halfway through, you take out your laptop and open a sudoku solver program to check whether one of your guesses is correct. Except — this sudoku is in a paper that tries to be special and uses the letters A–I instead of the numbers 1–9, but your sudoku solver only accepts numbers as input. Does this make any difference? Of course not: you can map the letters to numbers, for example A=1, B=2 etc., then solve the numeric sudoku and map back again: if the program says that a certain field is a 3, you can write a C in the original sudoku there.

The moral of this story is that you have a mapping that respects the structure of a sudoku: you not only map the elements (letters) to other elements (numbers) and back again but any statement that you can make about the original "in the language of sudokus" maps to a statement about the numeric version and back again too. For example, "the remaining field in row one of the top left square must be an A or a B" is a statement that translates to the numeric version by replacing A and B with 1 and 2. Such a mapping lets us say that the two versions of the sudoku are "essentially the same, just written differently"; mathematicians would say the two are isomorphic.

Apart from isomorphisms, there are more general structure-respecting mappings that are not reversible: these are called homomorphisms.

5.1 Group homomorphisms

A homomorphism from a group $(G, +_G)$ to a group $(H, +_H)$ is a map from G to H that preserves the structure or language or groups. The language of groups revolves around the noun "neutral" and the verbs "add" and "invert". Note that to be pedantic, we are using different symbols for addition in the two groups.

Definition 5.1 (group homomorphism). A function $f : G \to H$ is a group homomorphism between the groups $(G, +_G)$ and $(H, +_H)$ if it satisfies these three conditions.

- It preserves neutral elements: if 0_G is the neutral element of $(G, +_G)$ and 0_H is the neutral element of $(H, +_H)$ then $f(0_G) = 0_H$.
- It preserves addition. For any two elements a, b of G we have $f(a +_G b) = f(a) +_H f(b)$.
- It preserves inverses: for any element a of G with inverse $-a$, $f(-a)$ is the inverse of $f(a)$.

We have discussed one particular group homomorphism a lot: for any positive integer n, the map $[\,]$ from $(\mathbb{Z}, +)$ to $(\mathbb{Z}_n, +_n)$ is a homomorphism. Indeed, $[0] = 0$, $[a+b] = [a] +_n [b]$ and $[a] +_n [-a] = 0$ so $[-a]$ is the inverse of $[a]$. This is one of the times when it really pays off to be pedantic with the addition symbol. The statement $[a+b] = [a]+_n[b]$ is the same as $[a + b] = [[a] + [b]]$ which we stated as a rule in lecture 1; it would be wrong to write $[a + b] = [a] + [b]$ for the usual addition in $\mathbb{Z}$ however. (Exercise: find a counter-example.)

Exercise. ($\star$) *Trivial homomorphisms.*

- For any $n > 0$, describe the group homomorphisms between $(\mathbb{Z}_n, +)$ and $(\{0\}, +_0)$ in both directions, where $0 +_0 0 = 0$.
- Check that for any groups $(G, +_G)$ and $(H, +_H)$ the map $f : G \to H$ that sends every element of G to the neutral element of $(H, +_H)$ is a group homomorphism.
- Which other trivial homomorphism is there from any group $(G, +)$ to itself?

Exercise. ($\star\star$) *Group homomorphisms and orders.*

- Explain why there are no non-trivial homomorphisms (that do not send everything to the neutral element) from $(\mathbb{Z}_2, +_2)$ to $(\mathbb{Z}_3, +_3)$ or back again.

- What about $(\mathbb{Z}_2, +_2)$ to $(\mathbb{Z}_4, +_4)$ (and back again)?
- Consider the following situation. $(G, +_G)$ and $(H, +_H)$ are groups and $g \in G$ is an element of finite order $n > 0$, in particular $\underbrace{g +_G \ldots +_G g}_{n \text{ times}} = 0_G$. Show that if $f : G \to H$ is a homomorphism between these groups and $h = f(g)$ then $\underbrace{h +_H \ldots +_H h}_{n \text{ times}} = 0_H$.
- Show that group homomorphisms do not have to preserve the order of elements: find an example of two groups as above, an element $g \in G$ and a group homomorphism f such that the order of $f(a)$ is not the same as the order of a.

($\star\star\star$) The precise rule is that if $(G, +_G)$ and $(H, +_H)$ are groups and $f : G \to H$ is a group homomorphism between them then the order of $f(g)$ divides the order of g for any $g \in G$. Prove this.

5.2 Isomorphisms

A homomorphism allows you to translate statements one way but not back. For example, the statement "adding any element to itself gives 0" holds in the group $(\mathbb{Z}_2, +_2)$ but not in $(\mathbb{Z}, +)$ so there is no way to translate all possible statements in group-language back again. If a homomorphism does have an inverse, it is called an isomorphism.

Definition 5.2 (isomorphism). A homomorphism f from $\mathbb{G} = (G, +_G)$ to $\mathbb{H} = (H, +_H)$ is called an isomorphism if there is a homomorphism s from $\mathbb{H}$ to $\mathbb{G}$ such that f and s are inverses, i.e. for any $g \in G$ we have $s(f(g)) = g$ and for any $h \in H$ we have $f(s(h)) = h$.

Two groups are called isomorphic if there is an isomorphism between them (being isomorphic is an equivalence relation).

For example, consider the following three groups.

$\mathbb{G} = (\{0, 1, 2, 3\}, +)$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\mathbb{H} = (\{A, B, C, D\}, \oplus)$

$\oplus$	A	B	C	D
A	A	B	C	D
B	B	C	D	A
C	C	D	A	B
D	D	A	B	C

$\mathbb{I} = (\{0, 1, 2, 3\}, \boxplus)$

$\boxplus$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

The groups $\mathbb{G}$ and $\mathbb{H}$ are isomorphic: the isomorphism from $\mathbb{G}$ to $\mathbb{H}$ is the function f with $f(0) = \mathsf{A}, f(1) = \mathsf{B}, f(2) = \mathsf{C}, f(3) = \mathsf{D}$. However, $\mathbb{G}$ and $\mathbb{I}$ are not isomorphic. For example, adding any element to itself in $\mathbb{I}$ gives the neutral element but this is not true in $\mathbb{G}$, so there cannot be any function f from $\mathbb{I}$ to $\mathbb{G}$ that preserves neutral elements and addition.

The notion of isomorphism is very general and powerful in mathematics. The way we gave our definition, there is nothing specific to groups so once we know what a ring or field homomorphism is, we have got a definition of ring and field isomorphisms for free. The same idea could be carried over to other kinds of structure but we would have to give a more abstract definition of what it means for two homomorphisms to be inverses (since they are no longer necessarily functions on sets) which we can happily leave to professional mathematicians.

5.3 Group isomorphisms

There are only two "really different" groups with four elements, both of which we have just seen: one which is "essentially" $(\mathbb{Z}_4, +_4)$ and one in which every element added to itself is zero. The notion of isomorphism allows us to make clear what we mean by this statement: there are only two groups of order 4 "up to isomorphism". To define this formally, let $\sim$ be the equivalence relation "is isomorphic to" for groups. (Exercise: check that this really is an equivalence relation.) Then there are exactly two different equivalence classes that contain groups of order 4. Two groups of different orders cannot be isomorphic so these two classes contain only groups of order 4.

For prime numbers the classification is even simpler:

> **Proposition 5.3.** For any prime number p, there is only one group of order p up to isomorphism.

Another way of putting this is that if we have any two groups of order p where p is a prime then they are automatically isomorphic. Sensibly, one chooses $(\mathbb{Z}_p, +_p)$ as the representative element of this class of group.

We can extend this classification to all finite groups but we need to introduce one more concept to do this.

Exercise. $(\star\star)$ *Isomorphisms preserve group orders.* Show that if $(G, +_G)$ and $(H, +_H)$ are groups and $f : G \to H$ is an isomorphism then for every element $g \in G$, the order of g is the same as the order of $f(g)$.

Exercise. ($\star\star$) *Isomorphisms between additive and multiplicative groups.*

- Start with the group $(\mathbb{Z}_7^\times, \cdot)$ and consider the subgroup $\langle 2 \rangle$. This subgroup has 3 elements; find an isomorphism between this group and $(\mathbb{Z}_3, +)$.
- Find the other isomorphism between the above two groups (there are exactly two).
- There is one isomorphism f from $(\mathbb{Z}_{10}, +)$ to the subgroup $\langle 2 \rangle$ of $(\mathbb{Z}_{11}^\times, \cdot)$ that has $f(1) = 2$. First, find it. Secondly, what is the obvious formula for this isomorphism?

5.4 Products of groups

If $\mathbb{G} = (G, +_G)$ and $\mathbb{H} = (H, +_H)$ are two groups we can form a further group by taking all the pairs of elements (g, h) with $g \in G$ and $h \in H$ and adding component-wise, i.e. the sum of (g, h) and (g', h') is $(g +_G g', h +_H h')$. Since the set of elements of this group is $G \times H$, we call this group $\mathbb{G} \times \mathbb{H}$, the product of groups $\mathbb{G}$ and $\mathbb{H}$.

Definition 5.4 (product of groups). For a finite list of groups $\mathbb{G}_1, \ldots, \mathbb{G}_n$, the product group $\mathbb{G}_1 \times \ldots \times \mathbb{G}_n$ is the group whose elements are tuples of n elements where the i-th element is in $\mathbb{G}_i$, with component-wise addition. For the n-fold product of a group with itself we also write $\mathbb{G}^n$.

By now, we should all be able to find the formulas for the neutral element and the inverse of elements in product groups. Products of rings and fields (and when we introduce them, vector spaces) work in much the same manner.

5.5 Classification of finite Abelian groups

Product groups let us describe all finite Abelian groups:

Theorem 5.5 (classification of finite Abelian groups). Every finite Abelian group $\mathbb{G}$ is isomorphic to exactly one group of the form $\mathbb{Z}_{p_1^{m_1}} \times \ldots \times \mathbb{Z}_{p_k^{m_k}}$ where the p_i are primes and the m_i positive integers.

For a group of order n, we have $n = p_1^{m_1} \cdot \ldots \cdot p_k^{m_k}$ in this decomposition. Groups of the same order can still differ in whether prime powers are inside or outside the subscripts: the two non-isomorphic groups of order 4 are $\mathbb{Z}_{2^2} = \mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 = (\mathbb{Z}_2)^2$.

By this theorem, a cyclic group of composite order — say, $(\mathbb{Z}_{15}, +)$ — should be isomorphic to a product group $\mathbb{Z}_3 \times \mathbb{Z}_5$. Indeed, if we take any element x of $\mathbb{Z}_{15}$, we can write it as the pair $(x \pmod 3, x \pmod 5)$ to get an element of $\mathbb{Z}_3 \times \mathbb{Z}_5$ and for any such pair, there is exactly one element in $\mathbb{Z}_{15}$ with the given decomposition, as in the table below.

0	(0, 0)	5	(2, 0)	10	(1, 0)
1	(1, 1)	6	(0, 1)	11	(2, 1)
2	(2, 2)	7	(1, 2)	12	(0, 2)
3	(0, 3)	8	(2, 3)	13	(1, 3)
4	(1, 4)	9	(0, 4)	14	(2, 4)

Exercise. ($\star\star$) *Another decomposition.* Decompose $(\mathbb{Z}_{12}, +)$ into $\mathbb{Z}_4 \times \mathbb{Z}_3$.

5.6 The group of automorphisms

Isomorphism is an equivalence relation. In particular, if f is an isomorphism from $\mathbb{G}$ to $\mathbb{H}$ and g is an isomorphism from $\mathbb{H}$ to $\mathbb{K}$ then the composition gf (as a function on the underlying sets, i.e. for each element x of $\mathbb{G}$ we have $gf(x) := g(f(x))$, an element of $\mathbb{K}$). Since we can compose and invert isomorphisms, can we make them into a group? Not necessarily — we cannot compose any two isomorphisms, only ones with compatible domains. If $f : \mathbb{G} \to \mathbb{H}$ and $k : \mathbb{K} \to \mathbb{L}$ then we cannot compose f and k. We can always compose isomorphisms if they start and end at the same object though:

Definition 5.6 (automorphism). An isomorphism from a group (or ring, field) $\mathbb{G}$ to itself is called an automorphism of $\mathbb{G}$. The automorphisms of any object $\mathbb{G}$ form a group called $\mathrm{Aut}(\mathbb{G})$ with composition as the operation.

$\mathrm{Aut}(\mathbb{G})$ is a group because function composition is associative, the identity map that sends every element of $\mathbb{G}$ to itself is an automorphism and forms the neutral element of $\mathrm{Aut}(\mathbb{G})$ and isomorphisms are invertible by definition.

The definition of an automorphism group applies equally to rings, fields and many other structures; the automorphisms themselves always form a group, whichever structure one looks at.

Exercise. ($\star\star$) *Group automorphisms.*

- There is exactly one nontrivial automorphism from $(\mathbb{Z}_3, +)$ to itself (that is neither the identity map nor sends everything to the neutral element). Find it.
- Find the automorphism groups of $(\mathbb{Z}_5, +)$ and $(\mathbb{Z}_6, +)$ as well. Hint: automorphisms preserve orders of elements, so they must preserve generators of finite groups as well.
- Find the automorphism group of $\mathbb{Z}_2 \times \mathbb{Z}_2$.

5.7 Ring homomorphisms

To adapt the notion of homomorphism to rings, we just have to take care of multiplication as well.

Definition 5.7 (ring homomorphism). Let $\mathcal{R} = (R, +, \cdot)$ and $\mathcal{S} = (S, \oplus, \odot)$ be two rings. A function $f : R \to S$ is a ring homomorphism if f is a group homomorphism from $(R, +)$ to $(S, \oplus)$ and these two conditions hold:

- For any $a, b \in R$ we have $f(a \cdot b) = f(a) \odot f(b)$.
- We have $f(1_R) = 1_S$ where 1_R is the one (neutral element of multiplication) of $\mathcal{R}$ and 1_S is the one of $\mathcal{S}$.

If we look at a ring homomorphism from a ring $\mathcal{R}$ to itself, there is very little freedom. We know that for such a f, for all r, s we have $f(r+s) = f(r)+f(s)$ and $f(rs) = f(r)f(s)$ along with $f(1) = 1$. So for any $k \in \mathbb{Z}$ and for the ring element

$$r := \underbrace{1 + 1 + \ldots + 1}_{k \text{ times}}$$

we have $f(r) = f(1) + \ldots + f(1) = 1 + \ldots + 1 = r$, so ring homomorphisms from a ring to itself cannot change multiples of 1. For example, in $\mathbb{Z}$, the identity function is the only ring homomorphism.

WARNING: A ring homomorphism is not the same as a linear function (which we will introduce later). A linear function must satisfy $f(ax) = af(x)$ rather than $f(ax) = f(a)f(x)$, which gives it a lot more freedom.

In polynomial rings over finite fields, the interesting part of a ring homomorphism f is therefore what it does to X (which is not a multiple of 1). Since $f(X^2) = f(X) \cdot f(X)$ and so on, the behaviour of a ring homomorphism on such a polynomial ring is determined

by its behaviour on X, since we will see in a moment that all non-zero field elements are multiples of 1.

Let's look at multiples of 1 in a ring again. We can construct a function $m : \mathbb{N} \to \mathcal{R}$ for any ring $\mathcal{R}$ that takes n to

$$m(n) := \underbrace{1 + \ldots + 1}_{n \text{ times}}$$

where 1 is the one of the ring. For 0, we set $m(0) := 0$, that is evaluating m at the number zero gives the zero of the ring. We can extend this function to $\mathbb{Z}$ by setting $m(a) := -m(-a)$ for negative a, i.e. to evaulate on a negative integer you invert the integer to get a positive one, compute m on that and then invert back again in the ring. This function m is now a ring homomorphism $\mathbb{Z} \to \mathcal{R}$. If $\mathcal{R} = \mathbb{Z}$ then this m-function is the identity. In fact,

Proposition 5.8. For any ring $\mathcal{R}$, there is exactly one ring homomorphism from $\mathbb{Z}$ to $\mathcal{R}$ and it is the map

$$m(z) := \begin{cases} \underbrace{1_R + \ldots + 1_R}_{z \text{ times}} & z > 0 \\ 0_R & z = 0 \\ -m(-z) & z < 0 \end{cases}$$

where 1_R and 0_R are the one and zero elements of the ring.

With this homomorphism in place, we can define the characteristic of a ring. It is a similarly important number for rings as the order is for groups, although it does not always count elements.

Definition 5.9 (characteristic). The characteristic $\mathsf{char}(\mathcal{R})$ of a ring $\mathcal{R}$ is the smallest positive integer z for which $m(z) = 0$, the zero of the ring. If no such integer exists, the characteristic is 0 (the zero of $\mathbb{Z}$).

For example, $\mathsf{char}(\mathbb{Z}) = 0$ and $\mathsf{char}(\mathbb{Z}_n) = n$. But, $\mathsf{char}(\mathbb{Z}_n[X]) = n$ too, so the characteristic does not "count" elements that are not multiples of 1.

If p is a prime number and $\mathcal{R}$ is a commutative ring of characteristic p, the map $\phi : \mathcal{R} \to \mathcal{R}, x \mapsto x^p$ has the property that $\phi(a)\phi(b) = \phi(ab)$ — this is just the usual formula $a^p b^p = (ab)^p$ that holds in any commutative ring. But if we write out the expansion of $\phi(a + b) = a^p + b^p$, all intermediate terms gain a factor p and vanish: we get $(a + b)^p = a^p + b^p$.

Proposition 5.10 (Frobenius map). In a commutative ring $\mathcal{R}$ with prime characteristic p, the map $\phi : x \mapsto x^p$ is a ring homomorphism, called the Frobenius map.

5.8 Field homomorphisms

A field is a ring and all the information we need to make a field homomorphism is contained in the ring structure already.

Definition 5.11 (field homomorphism). Let $\mathbb{F} = (F, +, \cdot)$ and $\mathbb{K} = (K, \oplus, \odot)$ be fields. A function $f : F \to K$ is a field homomorphism if it is a ring homomorphism.

Don't we have to check that, for example, $f(a/b) = f(a) \oslash f(b)$? This comes for free: since $f(a/b \cdot b) = f(a)$ and know that $f(a/b) \odot f(b) = f(a)$, we can conclude that $f(a/b) = f(a) \oslash f(b)$.

Like for groups, we can use isomorphisms to classify finite fields. We will do this in the next lecture; for now we find a few more properties of field homomorphisms.

Proposition 5.12. In a finite field of characteristic p for a prime p, the Frobenius map $\phi : x \mapsto x^p$ is an isomorphism (and therefore an automorphism).

Further, such a field has p^n elements for some positive integer n and applying ϕ in sequence n times gives the identity map, i.e. for any field element x we have $x^{(p^n)} = x$.

We will see in the next lecture that all finite fields are of this form. A useful formula to remember in finite fields is that the Frobenius map can be used to invert elements: since $x^{p^n-1} = 1$, we must have $x^{p^n-2} = 1/x$. The fact that all finite field elements become one when raised to a certain power is also interesting to study field homomorphisms.

Definition 5.13 (root of unity). A field element x is called a k-th root of unity if $x^k = 1$ in the field, for a positive integer k. If $x^k = 1$ and $x^m \neq 1$ for all $1 \leq m < k$, we say that x is a primitive root of unity. (In this case, k is the order of x in the multiplicative group $(\mathbb{F} \setminus \{0\}, \cdot)$ of the field.)

In finite fields, all elements are roots of unity. But, by the same reasoning that we know over the reals why a non-zero polynomial of degree n cannot have more than n

roots, we know that in a finite field there cannot be more than n elements that are n-th roots of unity, i.e. roots of the polynomial $X^n - 1$. This tells us a lot about the orders of elements in finite fields.

The important fact that we need to take away to investigate finite fields is that field homomorphisms preserve roots of unity: if $x^k = 1$ then for any field homomorphism f we have $f(x^k) = f(x)^k$ so $f(x)$ is still a k-th root of unity. Isomorphisms are even better:

Proposition 5.14. If $\mathbb{F}, \mathbb{K}$ are fields and $f : \mathbb{F} \to \mathbb{K}$ is a field isomorphism then f preserves element orders, specifically $f(x)^k = 1$ if and only if $x^k = 1$.

So if we introduce an equivalence relation on a field where two elements are equivalent if they have the same multiplicative order, any field automorphism can only permute elements around within the classes but never move an element between classes.

Exercise. ($\star\star$) *Finite field inversion.* Let $p = 1033$, this is a prime number. The exercise is to compute $1/3$ in the finite field $\mathbb{F}_p$ — without a computer (so don't just program a loop that tries all possibilities), though you may use a calculator that supports the modulo operation. Hint: 1031 is 0100 0000 0111 in binary.

5.9 ◇ More on finite Abelian groups

◇ The formula $\mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_5$ is just a special case of a theorem that is supposed to have originated in ancient China.

Theorem 5.15 (Chinese remainder theorem). Let $n_1, \ldots, n_k$ be positive integers such that no two of these have a factor in common. Then for any integers $a_1, \ldots, a_k$ with $0 \leq a_i \leq n_i$ for all i there is exactly one integer x satisfying all the equations $x = a_i \pmod{n_i}$.

◇ The classification theorem for finite Abelian groups can be generalised to finitely generated Abelian groups, where there is a finite set of elements $x_1, \ldots, x_n$ such that $g = \langle x_1, \ldots, x_n \rangle$. In this case, every such group is isomorphic to the direct product of a finite Abelian group as above and a group $\mathbb{Z}^r$ for a unique value of r, which is called the rank of the group.

◇ One can also give a classification theorem for all finite groups, dropping the Abelian requirement. A theorem by Jordan and Hölder states that all finite groups are composed of finite simple groups (the "primes" of the group world, where every subgroup of a certain form has to be trivial). It remains to classify all finite simple groups — the result is one of the masterpieces of Algebra, completed for the first time (assuming no mistakes) in 2008. A revised version of the proof is being edited for publication and is expected to run to several thousand pages.