MT316A – GROUPS

Fiacre Ó Cairbre

Lecture 1

Chapter 1 – Definition and Examples.

Section 1.1 – A little bit of history of group theory.

Galois is considered the founder of group theory around 1832. The ideas in group theory have turned out to be very powerful in solving many important problems in mathematics, science and other areas.

Section 1.2 – Definition of a Group.

Remark 1. We will motivate the definition of a group by looking at two examples first.

Example 1. Consider the set of integers: $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3\ldots\}$.

Note the following four facts:

(i) $a + b \in \mathbb{Z}, \quad \forall \quad a, b \in \mathbb{Z}$

(ii) $a + 0 = a, \quad \forall \quad a \in \mathbb{Z}$

(iii) For every $a \in \mathbb{Z}$, there exists $b \in \mathbb{Z}$ such that $a + b = 0$

(iv) $a + (b + c) = (a + b) + c, \quad \forall \quad a, b, c \in \mathbb{Z}$

Example 2.

Consider the set of non–zero real numbers: $P = \{x \in \mathbb{R} : x \neq 0\}$.

Note the following four facts:

(i) $ab \in P, \quad \forall \quad a, b \in P$

(ii) $a1 = a, \quad \forall \quad a \in P$

(iii) For every $a \in P$, there exists $b \in P$ such that $ab = 1$

(iv) $a(bc) = (ab)c, \quad \forall \quad a, b, c \in P$

Definition 1.

Suppose we have a set S with an operation $*$ which acts on pairs of elements $a, b \in S$ to create $a * b$. We say that S is closed under $*$ if

$$a * b \in S, \quad \forall \quad a, b \in S$$

Remark 2.

Fact (i) in example 1 shows that $\mathbb{Z}$ is closed under addition. Fact (i) in example 2 shows that P is closed under multiplication.

Example 3.

Give an example of a set K (where K is a subset of $\mathbb{Z}$) such that $a+b \notin K$, for some $a, b \in K$.

Solution.

We can take $K = \{x \in \mathbb{Z} : 1 \leq x \leq 10\}$ and see that $3 + 8 \notin K$, with $3, 8 \in K$. This example shows that K is not closed under addition.

Definition 2.

Suppose S is a set. Then, $S \times S = \{(a, b) : a, b \in S\}$.

Definition 3.

Suppose S is a set and f is a function such that $f : S \times S \to S$. Then f is called a binary operation on S.

Example 4.

From example 1 we see that addition is a binary operation on $\mathbb{Z}$ because

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$

$$(a, b) \to a + b$$

Similarly, from example 2(i) we see that multiplication is a binary operation on P. From example 3 we see that addition is not a binary operation on K.

Remark 3.

Note that by using definitions 1 and 3 we see that S is closed under the operation $* \iff *$ is a binary operation on S.

Remark 4.

Suppose S is a set and $*$ is an operation. Then, the notation $(S, *)$ means that we consider S with the operation $*$. The reason for this notation $(S, *)$ is because when we define a group later, it will be important to know what operation we are considering.

Definition 4.

Suppose S is a set that is closed under the operation $*$. If there exists $e \in S$ such that

$$a * e = a = e * a, \quad \forall \quad a \in S$$

then e is called an identity element of $(S, *)$.

Remark 5.

In definition 4 it's important to know which operation we are considering because an element of a set S may be an identity under one operation but not under a different operation. For example, 0 is an identity of $(\mathbb{Z}, +)$ because $0 + a = a = a + 0, \quad \forall \quad a \in \mathbb{Z}$, but 0 is not an identity of $(\mathbb{Z}, \times)$, where $\times$ denotes the usual multiplication operation on $\mathbb{Z}$, because $0 \times 1 \neq 1$.

Definition 5.

Suppose S is closed under $*$ and suppose e is an identity element of $(S, *)$. Suppose $a \in S$. If there exists $b \in S$ such that

$$a * b = e = b * a$$

then b is called an inverse of a.

Definition 6 – Definition of a Group.

Suppose S is a non–empty set. Then $(S, *)$ is called a group if the following conditions are satisfied:

(i) $a * b \in S, \quad \forall \quad a, b \in S$

(ii) There exists $e \in S$ such that $a * e = a = e * a, \quad \forall \quad a \in S$.

(iii) If $a \in S$, then there exists $b \in S$ such that $a * b = e = b * a$.

(iv) $(a * b) * c = a * (b * c), \quad \forall \quad a, b, c \in S$.

MT316A – GROUPS

Fiacre Ó Cairbre

Example 5.

We see that $(\mathbb{Z}, +)$ is a group from example 1 where $+$ denotes the usual addition in $\mathbb{Z}$, because conditions (i), (ii), (iii) and (iv) in example 1 give us conditions (i), (ii), (iii) and (iv) in definition 6.

Similarly, $(P, \times)$ is a group from example 2 where $\times$ denotes the usual multiplication in the reals,

Remark 6.

In definition 6, (i) means that S is closed under $*$, (ii) means that there exists an identity e of $(S, *)$ and (iii) means that b is an inverse of a. We say that the operation $*$ is associative if condition (iv) in definition 6 is satisifed.

Example 6.

Is $(\mathbb{Z}, \times)$ a group where $\times$ denotes the usual multiplication in $\mathbb{Z}$?

Solution.

No, and here is a proof. First note that 1 is an identity element of $(\mathbb{Z}, \times)$ because $1 \times a = a = a \times 1$, for all $a \in \mathbb{Z}$. Now, 2 has no inverse because there is no $b \in \mathbb{Z}$ such that $2 \times b = 1$. So, condition (iii) in definition 6 is not satisfied and hence $(\mathbb{Z}, \times)$ is not a group.

Remark 7.

Notice that $(\mathbb{Z}, +)$ is a group but $(\mathbb{Z}, \times)$ is not a group.

Definition 7.

A group $(G, *)$ is called abelian if $a * b = b * a, \quad \forall \quad a,\ b \in G$. If a group is not abelian, then we call it non–abelian.

Example 7: $\mathbb{Z}_m$, the set of integers modulo m.

Suppose m is an integer and $m \geq 2$. Recall the set of integers modulo m denoted by $\mathbb{Z}_m$.

For us here we will think of $\mathbb{Z}_m$ as the set

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$$

with the operation of addition (mod m), denoted by $*$, which means that if $a, b \in \mathbb{Z}_m$, then $a * b$ is defined to be the remainder when the usual sum of a and b is divided by m. So, $a * b \in \mathbb{Z}_m$.

It's important to note that the elements of $\mathbb{Z}_m$ are not ordinary integers because, for example, in $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ we have that $2 * 4 = 1$ because 1 is the remainder when the

usual sum of 2 and 4 is divided by 5. Notice also that addition (mod 5) in $\mathbb{Z}_5$ is different from the usual addition in $\mathbb{Z}$ because again $2 * 4 = 1$ in $\mathbb{Z}_5$.

One can show that $(\mathbb{Z}_m, *)$ is a group, for $m \geq 2$, as follows:

(i) $a * b \in \mathbb{Z}_m, \quad \forall \quad a, b \in \mathbb{Z}_m$, as mentioned above.

(ii) 0 is an identity element in $(\mathbb{Z}_m, *)$, because $0 * a = a = a * 0, \quad \forall \quad a \in \mathbb{Z}_m$

(iii) If $a \in \mathbb{Z}_m$ and $a \neq 0$, then $m - a \in \mathbb{Z}_m$ is an inverse of a because $a * (m - a) = 0 = (m - a) * a$. Note that 0 is an inverse of 0.

(iv) One can check that

$$(a * b) * c = a * (b * c), \quad \forall \quad a, b, c \in \mathbb{Z}_m$$

So, the 4 conditions in definition 6 are satisfied and hence $(\mathbb{Z}_m, *)$ is a group for $m \geq 2$.

Note that $*$ above, for addition (mod m) on $\mathbb{Z}_m$, is usually just written as $+$ as long as there is no confusion with ordinary addition in $\mathbb{Z}$. So, we can now write that $2 + 4 = 1$ in $\mathbb{Z}_5$ and also say that $(\mathbb{Z}_m, +)$ is a group for $m \geq 2$. We will assume the operation on $\mathbb{Z}_m$ is addition (mod m) unless otherwise stated.

Remark 8.

Suppose $(G, *)$ is a group and $x, y \in G$. For convenience of notation we will often write $x * y$ as xy.

Furthermore, for convenience of notation, we will often just say 'suppose G is a group' instead of saying ' suppose $(G, *)$ is a group'. However, it should always be clear what operation we are considering when we are working with a group.

Lemma 1.

Suppose G is a group. Then G has a unique identity element.

Proof.

Suppose that e and f are identity elements of G. Then, $ef = e$ and $ef = f$ and so $e = f$ and we are done.

Lemma 2.

Suppose G is a group and $x \in G$. Then x has a unique inverse. The unique inverse of x is denoted by x^{-1}.

Proof.

Suppose that y and z are inverses of x. Also, suppose e is the identity element of G. Then

$$xy = e = yx \quad \text{and} \quad xz = e = zx$$

Now, $(zx)y = z(xy) = ze = z$. Also, $(zx)y = ey = y$. Hence, $z = y$ and we are done.

Example 8.

$2^{-1} = 3$ in $\mathbb{Z}_5$ because $2 + 3 = 0$ in $\mathbb{Z}_5$.

Remark 9.

We will introduce some notation here. Suppose G is a group with identity element e. Suppose $a \in G$. We can write the element aa as a^2. Similarly, we can write a^2a as a^3. In the same way, for a positive integer n, we can write $aaa \dots a$ (where a appears n times here) as a^n. Note that this also means that $a^1 = a$.

We define a^0 to be e.

Also, if $t \in \mathbb{Z}$ and $t < 0$, we define a^t to be the inverse of a^{-t} which makes sense because $-t$ is a positive integer. Thus a^t is defined to be $(a^{-t})^{-1}$.

In this way, we have now defined a^r where r is any integer.

Definition 8.

Suppose G is a group with identity element e. Suppose $a \in G$. The order of a is the least positive integer k such that $a^k = e$. If there is no positive integer r such that $a^r = e$, then we say that the order of a is infinity (denoted by ∞). We denote the order of a by $o(a)$.

Example 9.

Find the order of each element in $\mathbb{Z}_6$.

Solution.

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ and 0 is the identity in $\mathbb{Z}_6$.

Note that $0^1 = 0$ so $o(0) = 1$.

Note that if $a \in \mathbb{Z}_6$ and n is a positive integer, then from remark 9, a^n means $a + a + a + \dots + a$, where a is added (mod 6) to itself n times here.

Now $o(2) = 3$ because

$$2^1 = 2 \neq 0, \quad 2^2 = 2 + 2 = 4 \neq 0, \quad 2^3 = 2 + 2 + 2 = 0$$

So, 3 is the least positive integer k such that $2^k = 0$ and so $o(2) = 3$.

Similarly, $o(3) = 2$ because

$$3^1 = 3 \neq 0, \quad 3^2 = 3 + 3 = 0$$

So, 2 is the least positive integer k such that $3^k = 0$ and so $o(3) = 2$.

Similarly, $o(4) = 3$, $o(5) = 6$ and $o(1) = 6$ and we are done.

MT316A – GROUPS

Fiacre Ó Cairbre

Lecture 3

Example 10.

Consider the group $\mathbb{Z}$ with the operation of usual addition and consider $2 \in \mathbb{Z}$. Then $o(2) = \infty$, because there is no positive integer r such that $2^r = 0$. Note that 2^r here means $2 + 2 + 2 + \cdots + 2$, where 2 is added to itself r times.

Definition 9.

Suppose G is a group. Then the order of G is defined to be the number of elements in G and is denoted by $|G|$.

Example 11.

(i) $|\mathbb{Z}_m| = m$, for $m \geq 2$.

(ii) $|\mathbb{Z}| = \infty$.

Example 12.

For $n \geq 2$, suppose T_n denotes that set of invertible $n \times n$ matrices with real entries. We will now prove that T_n (with the operation of usual matrix multiplication) is a group, for $n \geq 2$. This group T_n is also denoted by $GL(n)$.

Proof.

First note that T_n is non–empty because the identity $n \times n$ matrix, I_n, is an element of T_n. Recall that I_n is the $n \times n$ matrix with 1 everywhere on the main diagonal and zero everyewhere else.

(i) $AB \in T_n$, for all $A, B \in T_n$, because the product of two invertible matrices is an invertible matrix. So, conditon (i) in definition 6 is satisfied.

(ii) $I_n A = A = A I_n$, for all $A \in T_n$ and so condition (ii) in definition 6 is satisfied.

(iii) Recall from linear algebra that if $A \in T_n$, then A has a (matrix) inverse denoted by A^{-1} such that $AA^{-1} = I_n = A^{-1}A$. Note that $A^{-1} \in T_n$ and so condition (iii) in definition 6 is satisfied.

(iv) $(AB)C = A(BC)$, for all $A, B, C \in T_n$ and so condition (iv) in definition 6 is satisfied.

So, all four conditions in definition 6 are satisfied and hence T_n is a group for $n \geq 2$.

Example 13.

$GL(2)$ is a non–abelian group.

Proof.

Consider the two matrices, $A, B \in GL(2)$ where

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Then,

$$AB = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \qquad BA = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$$

So, $AB \neq BA$ and hence $GL(2)$ is a non–abelian group.

Remark 10.

Suppose G is a group and $x \in G$. Then, $x^{r+s} = x^r x^s$, for any integers, r, s. Also, $(x^r)^s = x^{rs}$, for any integers, r, s.

Lemma 3.

Suppose G is a group with identity element e and suppose $x \in G$. Suppose $o(x) = k$, where k is finite, and suppose $x^n = e$. Then $n = rk$, for some integer r.

Proof.

If we divide k into n, then we will get that

$$n = qk + s, \quad \text{where} \quad q, s \in \mathbb{Z} \quad \text{with} \quad 0 \leq s < k$$

Now,

$$x^n = x^{qk+s} = x^{qk} x^s = (x^k)^q x^s = e^q x^s = e x^s = x^s$$

So, $x^s = e$ and hence $s = 0$ because k is the least positive integer such that $x^k = e$. So, we have $n = qk$, for some integer q and we are done.

Lemma 4.

Suppose G is a group and $x \in G$ with $o(x) = k$, where k is finite. Then,

$$o(x^m) = \frac{k}{gcd(k, m)}$$

where $m \in \mathbb{Z}$ and $m > 0$ and $gcd(k, m)$ denotes the greatest common divisor of k and m.

Example 14.

Consider $0 \in \mathbb{Z}$ and let $S = \{0\}$. Then, S is a group with the usual addition.

Consider $1 \in \mathbb{Z}$ and let $L = \{1\}$. Then, L is a group with the usual multiplication.

Note that both groups L and S contain exactly one element each. It turns out that all groups which contain exactly one element can be considered essentially to be the same because if $(\{y\}, *)$ is any group that contains exactly one element y, then we have

$$y * y = y, \qquad y \text{ is the identity element in the group} \qquad \text{and} \quad y^{-1} = y$$

Any group that contains exactly one element is called the trivial group. Also, if a group contains more than one element, then it's called a non–trivial group.

Section 1.2 – Subgroups.

Definition 10.

Suppose $(G, *)$ is a group and H is a subset of G. Then, we say that H is a subgroup of G if $(H, *)$ is a group. Note that here the operation on H is the same as the operation on G.

Example 15.

$(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$, where $\mathbb{R}$ denotes the set of real numbers and $+$ is usual addition.

Remark 11.

From now on, when we consider $\mathbb{Z}$ as a group, we wll always be using the operation of usual addition, unless otherwise stated.

Example 16.

Consider the group $\mathbb{Z}_6$.

(a) Is $H = \{0, 3\}$ a subgroup of $\mathbb{Z}_6$?

(b) Is $W = \{0, 1, 3\}$ a subgroup of $\mathbb{Z}_6$?

Solution.

(a) Yes, and here is a proof: H is non–empty and:

(i) $a + b \in H$, for all $a, b \in H$.

(ii) $0 + a = a = a + 0$, for all $a \in H$.

(iii) If $a \in H$, then there exists $b \in H$ such that $a + b = 0 = b + a$.

(iv) $(a + b) + c = a + (b + c)$, for all $a, b, c \in H$.

So, all the conditions in defintion 6 are satisfied and hence H (with the operation $+$) is a group and so H is a subgroup of $\mathbb{Z}_6$.

(b) No, and here is a proof: Condition (i) in definition 6 is not satisfied because $1 + 3 \notin W$ with $1, 3 \in W$. Hence, W is not a group (with the operation $+$) and so W is not a subgroup of $\mathbb{Z}_6$.

Example 17.

Suppose $(G, *)$ is a group with identity element e. Then $(G, *)$ itself is a subgroup of $(G, *)$. Also, the trivial group $(\{e\}, *)$ is a subgroup of $(G, *)$.

MT316A – GROUPS

Fiacre Ó Cairbre

Lecture 4

Proposition 1.

A non–empty subset H of a group G is a subgroup of $G \iff ab^{-1} \in H$, for all $a, b \in H$.

Proof.

We first prove the $\Rightarrow$ part: H is a group and so $b^{-1} \in H$ and hence $ab^{-1} \in H$ and so we have proved the $\Rightarrow$ part:

We next prove the $\Leftarrow$ part: Our aim is to show that H is a group and we will do that by showing that the four conditions of definition 6 are satisfied for H. Suppose e is the identity element of G. Suppose $x \in H$. Then, $xx^{-1} \in H$ and so $e \in H$. Hence, H has an identity element and condition (ii) in definition 6 is satisfied.

Next, suppose $y \in H$. Then, $ey^{-1} \in H$ and so $y^{-1} \in H$. Hence, condition (iii) in definition 6 is satisfied. Now, suppose $v, w \in H$. Then

$$w^{-1} \in H \ \Rightarrow \ v(w^{-1})^{-1} \in H \ \Rightarrow \ vw \in H$$

and so condition (i) in definition 6 is satisfied.

Finally, $(xy)z = x(yz)$, for all $x, y, z \in H$ and so condition (iv) in definition 6 is satisfied. So, overall H is a group and hence H is a subgroup of G. So, we have proved the $\Leftarrow$ part and we are done.

Example 18.

Consider the group $\mathbb{Z}$. Suppose H is the set of even integers. Then, H is a subset of $\mathbb{Z}$. Is H a subgroup of $\mathbb{Z}$?

Solution.

Yes, and here is a proof: Note that if $a, b \in H$, then $ab^{-1} = a - b \in H$ and so by proposition 1 we get that H is a subgroup of $\mathbb{Z}$.

Theorem 1.

Denote the set of positive integers (or natural numbers) by $\mathbb{N}$ and so $\mathbb{N} = \{1, 2, 3, \ldots\}$. Then, the non–trivial subgroups of $\mathbb{Z}$ are $n\mathbb{Z}$, for $n \in \mathbb{N}$, where $n\mathbb{Z}$ is the set of integer multiples of n, i.e.

$$n\mathbb{Z} = \{\ldots, -2n, -n, 0, n, 2n, 3n, \ldots\}$$

Proof.

Suppose H is a non–trivial subgroup of $\mathbb{Z}$. Then, H must contain a smallest positive number t. Now, $t\mathbb{Z}$ is a subset of H. We will prove that H is a subset of $t\mathbb{Z}$ and hence we will have that $H = t\mathbb{Z}$ and we will be done.

Consider $m \in H$. Then, if we divide t into m we get that

$$m = kt + r, \quad \text{where} \quad k,\ r \in \mathbb{Z} \quad \text{with} \quad 0 \leq r < t$$

Now, $r = m - kt \in H$ and so $r = 0$ because t is the least positive number in H. Thus, $m = kt$ and so H is a subset of $t\mathbb{Z}$. Hence $H = t\mathbb{Z}$ and we are done.

CHAPTER 2 – Permutation Groups.

Section 2.1 – Definition and Examples.

Definition 1.

(i) Suppose X and Y are sets and $f : X \to Y$ is a function. Then, f is called $1 - 1$ if

$$a \neq b \ \Rightarrow \ f(a) \neq f(b), \quad \text{for} \ \ a,\ b \in X$$

(ii) Suppose X and Y are sets and $f : X \to Y$ is a function. Then, f is called onto if

$$z \in Y \ \Rightarrow \ z = f(w), \quad \text{for some} \ \ w \in X$$

Definition 2.

Suppose X and Y are sets and $f : X \to Y$ is a function. Then, f is called a bijection if f is $1 - 1$ and onto.

Definition 3.

Suppose V is a non–empty set and $f : V \to V$ is a bijection. Then, we call f a permutation of V. Denote the set of all permutations of V by $\mathrm{Sym}(V)$.

Theorem 1.

Suppose W is a non–empty set. Then, $\mathrm{Sym}(W)$ (with the operation of composition of functions) is a group.

Proof.

First note that $\mathrm{Sym}(W)$ is non–empty because $I \in \mathrm{Sym}(W)$ where I is the function

$$I : W \to W$$

$$x \to x$$

Suppose $f, g \in \mathrm{Sym}(W)$. Denote the composition f after g by $f \circ g$. This means that $(f \circ g)(x) = f(g(x))$, for $x \in W$. Note that $f \circ g \in \mathrm{Sym}(W)$, for all $f, g \in \mathrm{Sym}(W)$ and so condition (i) in definition 6 in chapter 1 is satisfied.

Note that I above will be an identity element of $\mathrm{Sym}(W)$ because $I \circ f = f = f \circ I$, for all $f \in \mathrm{Sym}(W)$ and so condition (ii) in definition 6 is satisfied.

MT316A – GROUPS

Fiacre Ó Cairbre

Lecture 5

Continuation of the proof of Theorem 1.

If $f \in \text{Sym}(W)$, then the inverse function f^{-1} is an element of $\text{Sym}(W)$ and we have $f \circ f^{-1} = I = f^{-1} \circ f$. So, condition (iii) in definition 6 is satisfied.

Finally, we have that

$$(f \circ g) \circ h = f \circ (g \circ h), \quad \text{for all} \quad f,\ g,\ h, \in \text{Sym}(W)$$

and so condition (iv) in definition 6 is satisfied. Hence, $\text{Sym}(W)$ (with the operation of composition of functions) is a group.

Definition 4.

Suppose $n \in \mathbb{N}$. The symmetric group (on n symbols) is denoted by S_n and is defined by:

$$S_n = \text{Sym}(W), \quad \text{where} \quad W = \{1, 2, 3, \ldots, n\}$$

Remark 1.

Note that the elements of S_n are the permutations of $\{1, 2, 3, \ldots, n\}$.

Remark 2.

We will now discuss some notation. Consider the function

$$\alpha : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$$

where $\alpha(1) = 4,\ \alpha(2) = 3,\ \alpha(3) = 1,\ \alpha(4) = 2$.

Then, $\alpha \in \text{Sym}(W)$, where $W = \{1, 2, 3, 4\}$ and so $\alpha \in S_4$. For convenience of notation, we denote the permutation α by

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \qquad (*)$$

where this notation means that α takes a number in the top row to the corresponding number directly below it in the bottom row. It's important to note that the notation in $(*)$ above does not correspond to a matrix. Another example of this notation in $(*)$ is

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

which means that β is the permutation in S_4 given by

$$\beta : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$$

where $\beta(1) = 3,\ \beta(2) = 4,\ \beta(3) = 2,\ \beta(4) = 1$.

In the same way, we can represent any permutation in S_4 using the same type of notation as $(*)$.

Example 1.

Suppose

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \text{ and } \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \text{ in } S_4$$

Then,

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \qquad (*)$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

Remark 3.

From now on we will omit the $\circ$ symbol in $(*)$ in example 1 and so

$$\alpha\beta = \alpha \circ \beta \text{ and } \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

Example 2.

Suppose $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ in S_4. Find α^{-1}.

$$\alpha^{-1} = \begin{pmatrix} 4 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \qquad (*)$$

Remark 4.

We will now discuss some notation. Suppose $k_1, k_2, \ldots, k_m \in \{1, 2, 3, \ldots, n\}$, with $k_i \neq k_j$ for $i \neq j$. Then, $(k_1 k_2 \ldots k_m)$ denotes the permutation in S_n that maps k_1 to k_2, k_2 to k_3, k_3 to k_4 ..... k_{m-1} to k_m and finally maps k_m to k_1 and all other elements of $\{1, 2, 3, \ldots, n\}$ are mapped to themselves.

Definition 5.

(i) $(k_1 k_2 \ldots k_m)$ in remark 4, is called a cycle. The length of a cycle is the number of elements in the cycle and so $(k_1 k_2 \ldots k_m)$ has length m.

(ii) An m–cycle is a cycle of length m.

Example 3.

In S_4 the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$

can be expressed as the cycle (134). Note that (134) is a 3–cycle.

Also, $(134)(12) = (1234)$ and $(134)^{-1} = (143)$.

Note that $(134) = (341) = (413)$.

Example 4.

(i) $S_2 = \{I, (12)\}$, where I is the identity in S_2 from Theorem 1. Note that S_2 is abelian.

(ii)

$$S_3 = \{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\}$$

$$= \{I, (12), (13), (23), (123), (132)\}$$

where I is the identity in S_3 from Theorem 1. Note that $|S_3| = 6$. Also, S_3 is non–abelian because

$$(12)(13) = (132) \quad \text{but} \quad (13)(12) = (123)$$

and so

$$(12)(13) \neq (13)(12)$$

MT316A – GROUPS

Fiacre Ó Cairbre

Lecture 6

Theorem 2.

S_n is non–abelian for $n \geq 3$.

Proof.

Consider $(12),\ (13) \in S_n$ for $n \geq 3$. Then, as in example 4 we have that $(12)(13) \neq (13)(12)$ and so S_n is non–abelian.

Theorem 3.

$|S_n| = n!$, for $n \geq 2$.

Proof.

The different elements of S_n correspond to the different ways of filling in the bottom row of

$$\begin{pmatrix} 1 & 2 & 3 & 4 & . & . & . & n \\ . & . & . & . & . & . & . & . \end{pmatrix}$$

So, there are $n(n-1)(n-2)\ldots.3.2.1 = n!$ different elements in S_n.

Definition 6.

Two cycles are called disjoint if they have no elements in common.

Example 5.

(134) and (25) are disjoint cycles in S_5. (134) and (12) are not disjoint cycles in S_5.

Example 6.

We know from theorem 3 that there are 24 elements in S_4 and here they are:

$$I, (12), (13), (14), (23), (24), (34), (123), (132), (124), (142), (134), (143), (234),$$

$$(243), (1234), (1243), (1324), (1342), (1423), (1432), (12)(34), (13)(24), (14)(23)$$

where I is the identity element in S_4 from Theorem 1.

Example 7.

Suppose $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$ in S_5. Express α as the product (composition) of two disjoint cycles.

Solution.

$\alpha = (143)(25)$, where (143) and (25) are disjoint cycles.

Theorem 4.

Every $\alpha \in S_n$ can be expressed as a cycle or as a product (composition) of disjoint cycles.

Corollary 1.

Up to the ordering of cycles, there is only one way to express a permutation as a product (composition) of disjoint cycles.

Example 8.

Consider the permutation α from example 7. Then, $\alpha = (143)(25)$. Also, $\alpha = (25)(143)$ and there is no other way to express α as a product of disjoint cycles.

Definition 7.

Suppose G is a group and $x, y \in G$. Then, we say that x and y commute in G if $xy = yx$.

Theorem 5.

Suppose α, β are disjoint cycles in S_n. Then α and β commute in S_n, i.e. $\alpha\beta = \beta\alpha$.

Proof.

The elements in α and β come from disjoint subsets of $\{1, 2, 3, \ldots, n\}$.

Example 9.

In S_6, we have $(12)(45) = (45)(12)$.

Lemma 1.

Suppose α is a k–cycle in S_n. Then, $o(\alpha) = k$.

Proof.

Suppose $\alpha = (b_1 b_2 \ldots . b_k)$. Then $\alpha^k = I$, where I is the identity element in S_n. Also, k is the least positive integer such that $\alpha^k = I$. Hence, $o(\alpha) = k$.

Example 10.

Suppose $\alpha = (2351)$ in S_6. Then, $o(\alpha) = 4$.

Theorem 6.

Suppose $\alpha = \beta_1 \beta_2 \ldots \beta_t$, where β_i and β_j are disjoint cycles for $i \neq j$. Suppose $o(\beta_i) = m_i$, for $1 \leq i \leq t$. Then, $o(\alpha) =$ lcm $\{m_1, m_2, \ldots, m_t\}$.

Example 11.

Suppose $\alpha = (12)(45)(367)$ in S_7. Then, $o(\alpha) =$ lcm $\{2, 2, 3\} = 6$.

MT316A – GROUPS

Fiacre Ó Cairbre

Lecture 7

Remark 5.

A 2–cycle is also called a transposition.

Theorem 7.

Suppose $\alpha \in S_n$ with $n \geq 2$. Then, α can be expressed as a product (composition) of transpositions.

Proof.

We know from theorem 4 that α can be expressed as a cycle or product of disjoint cycles. Now, any cycle $(b_1 b_2 \dots b_t)$ can be expressed as the following product of transpositions: $(b_1 b_t)(b_1 b_{t-1}) \dots (b_1 b_3)(b_1 b_2)$. Consequently, α can be expressed as a product of transpositions.

Example 12.

Express $\alpha = (124)(356)$ in S_6 as a product of transpositions.

Solution.

(i) $(124)(356) = (14)(12)(36)(35)$.

Theorem 8.

Suppose $\alpha \in S_n$. Suppose $\alpha = \beta_1 \beta_2 \dots \beta_m$ and $\alpha = \sigma_1 \sigma_2 \dots \sigma_k$, where all the β_i and σ_j are transpositions for $1 \leq i \leq m$, $1 \leq j \leq k$. Then, m and k are either both even or both odd.

Example 13.

Note that $\alpha = (124)(356)$ in S_6 in example 12 can also be expressed as the following product of transpositions: $(14)(13)(13)(12)(36)(35)$ because $(13)(13) = I$, where I is the identity in S_6. So, α can be expressed as the product of four transpositions (as in example 12) and also as the product of six transpositions.

Definition 8.

(i) $\alpha \in S_n$ is called an even permutation if it can be expressed as a product of an even number of transpositions.

(ii) $\alpha \in S_n$ is called an odd permutation if it can be expressed as a product of an odd number of transpositions.

Example 14.

Suppose $\alpha = (1245)(352)$ in S_6. Then, $\alpha = (15)(14)(12)(32)(35)$ and so α is an odd permutation.

Remark 6.

(i) Suppose G is group with identity e. If $x \in G$ with $x \neq e$, then we say that x is a non–identity element.

(ii) If G is a group and $|G|$ is finite, then we say that G is a finite group. If $|G| = \infty$, then we say that G is an infinite group.

Theorem 9.

Suppose $A_n = \{\alpha \in S_n : \alpha \text{ is even}\}$ for $n \geq 2$. Then, A_n is a subgroup of S_n and we call A_n the alternating group.

Proof.

Suppose I is the identity in S_n. Then $I = (12)(12)$ and so $I \in A_n$ and hence A_n is non–empty.

Suppose $\alpha, \beta \in A_n$. Then, $\alpha = \sigma_1\sigma_2 \ldots \sigma_k$, where k is even and the σ_i are transpositions for $1 \leq i \leq k$ and also $\beta = \gamma_1\gamma_2 \ldots \gamma_m$, where m is even and the γ_i are transpositions for $1 \leq i \leq m$.

Now note that

$$\beta^{-1} = \gamma_m^{-1}\gamma_{m-1}^{-1} \ldots \gamma_2^{-1}\gamma_1^{-1} = \gamma_m\gamma_{m-1} \ldots \gamma_2\gamma_1$$

and so

$$\alpha\beta^{-1} = \sigma_1\sigma_2 \ldots \sigma_k\gamma_m\gamma_{m-1} \ldots \gamma_2\gamma_1$$

which means that $\alpha\beta^{-1} \in A_n$. So, by proposition 1 in lecture 4, we get that A_n is a subgroup of S_n.

Theorem 10.

$|A_n| = \dfrac{n!}{2}$, for $n \geq 2$.

Proof.

Suppose $\alpha, \beta \in A_n$ with $\alpha \neq \beta$. Then, $(12)\alpha \neq (12)\beta$ with $(12)\alpha$ and $(12)\beta$ both odd permutations.

Also, suppose γ, σ are odd permutations in S_n with $\gamma \neq \sigma$. Then, $(12)\gamma \neq (12)\sigma$ with $(12)\gamma$ and $(12)\sigma$ both even permutations.

Thus, the number of odd permutations in S_n is equal to the number of even permutations in S_n and so $|A_n| = \dfrac{|S_n|}{2} = \dfrac{n!}{2}$

Example 15.

$|A_4| = 12$.

Example 16.

(i) $A_3 = \{I, (123), (132)\}$, where I is the identity in S_3. Notice that A_3 is abelian.

(ii) Notice that A_4 is non–abelian because $(123), (124) \in A_4$ and $(123)(124) \neq (124)(123)$.

Chapter 3 – Cyclic Groups.

Definition 1.

Suppose G is a group and L is a non–empty subset of G. Then, we say that L is a generating set for G if

$$G = \{x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} : x_i \in L,\ \alpha_i = \pm 1 \ \text{ for } \ 1 \leq i \leq n, \ \text{ and } \ n \ \text{ is any positive integer}\}$$

We also say that G is generated by L.

Remark 1.

Suppose L is a non–empty subset of a group G. Let $\underline{L} = \{x^{-1} : x \in L\}$. Then, definition 1 is essentially saying that L generates G if every element of G can be expressed as a product of elements from $L \cup \underline{L}$, where $\cup$ here denotes the union of two sets.

Example 1.

$\{1\}$ is a generating set for $\mathbb{Z}$ and $\{2, 3\}$ is a generating set for $\mathbb{Z}$.

Example 2.

$\{2\}$ is not a generating set for $\mathbb{Z}$.

Definition 2.

Suppose X is a generating set for a group G. Then, X is called a minimal generating set for G if, by removing any element of X, the resulting set is not a generating set for G.

Example 3.

$\{1\}$ is a minimal generating set for $\mathbb{Z}$ and $\{2, 3\}$ is a minimal generating set for $\mathbb{Z}$.

Example 4.

$\{1, 2, 3\}$ is not a minimal generating set for $\mathbb{Z}$.

Definition 3.

Suppose G is a group and suppose theres exists an $x \in G$ such that $\{x\}$ is a generating set for G. Then, G is called a cyclic group. We also say that G is generated by x and that x is a generator for G.

MT316A – GROUPS

Fiacre Ó Cairbre

Lecture 8

Example 5.

$\mathbb{Z}$ is a cyclic group because $\{1\}$ is a generating set for $\mathbb{Z}$. Also, 1 is a generator for $\mathbb{Z}$.

Example 6.

$\mathbb{Z}_4$ is a cyclic group because $1 \in \mathbb{Z}_4$ is a generator for $\mathbb{Z}_4$. Note also that $3 \in \mathbb{Z}_4$ is a generator for $\mathbb{Z}_4$. However, $2 \in \mathbb{Z}_4$ is a not generator for $\mathbb{Z}_4$.

Remark 2.

If G is a cyclic group and x is a generator for G, then $G = \{x^k : k \in \mathbb{Z}\}$. Consequently, every cyclic group is abelian.

Example 7.

Is S_3 a cyclic group?

Solution.

No, because we know S_3 is non–abelian and hence by remark 2, S_3 is not cyclic.

Definition 4.

Suppose G_1 and G_2 are groups. The product group is denoted by $G_1 \times G_2$ and is defined as the set

$$G_1 \times G_2 = \{(x, y) : x \in G_1,\ y \in G_2\}$$

with the operation defined as

$$(x, y)(a, b) = (xa, yb), \quad \text{for all } \ (x, y),\ (a, b) \in G_1 \times G_2$$

Remark 3.

One can check that $G_1 \times G_2$ (in definition 4) forms a group under the given operation. Note that the identity in $G_1 \times G_2$ is (e_1, e_2) where e_1 is the identity in G_1 and e_2 is the identity in G_2. The inverse of (x, y) in $G_1 \times G_2$ is (x^{-1}, y^{-1}).

Example 8.

Suppose the groups G_1 and G_2 in definition 4 are both $\mathbb{Z}$. Then, we have the product group $\mathbb{Z} \times \mathbb{Z}$. Recall that the operation on $\mathbb{Z}$ is the usual addition which we will denote by $+$. For convenience we will also denote the operation on $\mathbb{Z} \times \mathbb{Z}$ by $+$ and so we have

$$(x, y) + (a, b) = (x + a, y + b), \quad \text{for all} \quad (x, y),\ (a, b) \in \mathbb{Z} \times \mathbb{Z} \qquad (*)$$

Note that the + on the right hand side of = in $(*)$ denotes the usual addition in $\mathbb{Z}$ whereas the + on the left hand side of = in $(*)$ denotes the operation on $\mathbb{Z} \times \mathbb{Z}$.

For example,

$$(3, -2) + (4, 1) = (3 + 4, -2 + 1) = (7, -1)$$

Example 9.

$\mathbb{Z} \times \mathbb{Z}$ (from example 8) is an abelian group.

Example 10.

$\mathbb{Z} \times \mathbb{Z}$ is not a cyclic group.

Proof.

We will prove this by contradiction. So, suppose $\mathbb{Z} \times \mathbb{Z}$ is a cyclic group. Then (a, b) is a generator for $\mathbb{Z} \times \mathbb{Z}$ for some $(a, b) \in \mathbb{Z} \times \mathbb{Z}$.

Hence, by remark 2, $\mathbb{Z} \times \mathbb{Z} = \{(a, b)^k : k \in \mathbb{Z}\}$. Now, for convenience, we will write $(a, b)^k$ as $k(a, b)$ because the operation on $\mathbb{Z} \times \mathbb{Z}$ is the + operation in example 8. For example, $(3, -4)^2 = (3, -4) + (3, -4) = 2(3, -4)$.

Now, $(1, 0) = k(a, b) = (ka, kb)$, for some $k \in \mathbb{Z}$. Hence, $1 = ka$ and $0 = kb$. So, $b = 0$. Now, we also have $(0, 1) = q(a, b)$, for some $q \in \mathbb{Z}$, which implies $1 = qb = 0$ which is impossible.

So, our supposition that $\mathbb{Z} \times \mathbb{Z}$ is a cyclic group is false and thus $\mathbb{Z} \times \mathbb{Z}$ is not a cyclic group.

Example 11.

Note that $X = \{(1, 0), (0, 1)\}$ is a generating set for $\mathbb{Z} \times \mathbb{Z}$ because if $(a, b) \in \mathbb{Z} \times \mathbb{Z}$, then

$$(a, b) = a(1, 0) + b(0, 1) = (1, 0)^a (0, 1)^b$$

Also, X is a minimal generating set for $\mathbb{Z} \times \mathbb{Z}$ because $\{(1, 0)\}$ is not a generating set for $\mathbb{Z} \times \mathbb{Z}$ and $\{(0, 1)\}$ is not a generating for $\mathbb{Z} \times \mathbb{Z}$.

Example 12.

In $\mathbb{Z} \times \mathbb{Z}_4$ we have $o(0, 1) = 4$ and $o(1, 0) = \infty$.

Lemma 1.

(i) Suppose G_1 and G_2 are both finite groups. Then, $|G_1 \times G_2| = |G_1||G_2|$.

(ii) Suppose at least one of the groups G_1, G_2 is an infinite group. Then, $G_1 \times G_2$ is an infinite group.

Example 13.

$|A_4 \times \mathbb{Z}_5| = 60$ and $A_4 \times \mathbb{Z}$ is an infinite group.

Remark 4.

Suppose G is a group and suppose $x_i \in G$ for $1 \leq i \leq n$. Let $X = \{x_1, x_2, \ldots, x_n\}$. Then, the subgroup generated by X is denoted by $< x_1, x_2, \ldots, x_n >$ and so

$$< x_1, x_2, \ldots, x_n >= \{z_1^{\alpha_1} z_2^{\alpha_2} \ldots z_t^{\alpha_t} : z_i \in X,\ \alpha_i = \pm 1,\ \text{for}\ 1 \leq i \leq t\ \text{and}\ t\ \text{any positive integer}\}$$

Remark 5.

(i) One can check that $< x_1, x_2, \ldots, x_n >$ in remark 4 is a subgroup of G.

(ii) If G is a cyclic group that is generated by an element x, then we can now write $G =< x >$.

Example 14.

$\mathbb{Z} =< 1 >$.

Example 15.

In $\mathbb{Z} \times \mathbb{Z}$ we have $< (1, 0) >= \mathbb{Z} \times \{0\}$

Chapter 4 – Lagrange's Theorem.

Definition 1.

Suppose H is a subgroup of a group G and suppose $x \in G$. We define the set xH as follows:

$$xH = \{xy : y \in H\}$$

This set xH is a subset of G and is called a left coset of H in G. The set of all left cosets of H in G is denoted by $\frac{G}{H}$.

We also define the set Hx as follows:

$$Hx = \{yx : y \in H\}$$

This set Hx is a subset of G and is called a right coset of H in G.

Example 1.

Consider the group $\mathbb{Z}_{12}$ and suppose $H = \{0, 3, 6, 9\}$. Then, one can show that H is a subgroup of $\mathbb{Z}_{12}$. We have the following left cosets of H in $\mathbb{Z}_{12}$:

MT316A – GROUPS

Fiacre Ó Cairbre

Lecture 9

Example 1 continued

$$0H = H, \quad 2H = \{2, 5, 8, 11\}, \quad 3H = H$$

Notice that $xH = Hx$, for all $x \in \mathbb{Z}_{12}$ because $\mathbb{Z}_{12}$ is abelian.

Note that since the operation on $\mathbb{Z}_{12}$ is addition (mod 12), then we can write $x + y$ for xy, where $x, y \in \mathbb{Z}_{12}$ and so we can write $2 + H$ for $2H$ and get that $2 + H = \{2, 5, 8, 11\}$.

Example 2.

Consider the subgroup A_3 of the group S_3. Then we have the following left cosets of A_3 in S_3:

$$IA_3 = A_3, \quad (12)A_3 = \{(12), (23), (13)\}, \quad (123)A_3 = A_3$$

where I is the identity in S_3.

Lemma 1.

Suppose H is a subgroup of a group G and suppose $x \in G$. Then, $xH = H \iff x \in H$.

Proof.

Proof of $\Rightarrow$: Suppose e is the identity in G. Then, $e \in H$. Now, $x = xe \in xH = H$ and so $x \in H$ and we are done.

Proof of $\Leftarrow$: xH is a subset of H. Also, if $z \in H$, then $z = xx^{-1}z \in xH$ and so H is a subset of xH. Hence, $xH = H$ and we are done.

Definition 2.

Suppose X is a subset of a group G. Then, the number of elements in X is denoted by $|X|$.

Lemma 2.

Suppose H is a subgroup of the group G. Then, $|xH| = |yH|$, for all $x, y \in G$.

Proof.

It suffices to prove that $|xH| = |H|$, for all $x \in G$. Now, note that

$$f \quad : \quad H \to xH$$

$$k \to xk$$

is a bijection and so $|H| = |xH|$ and we are done.

Lemma 3.

Suppose H is a subgroup of a group G and suppose $x, y \in G$. Then, either $xH = yH$ or $xH \cap yH = \phi$.

Theorem 1 – Lagrange's Theorem.

Suppose H is a subgroup of a finite group G. Then, $|H|$ divides $|G|$.

Proof.

First note that $G = \bigcup_{y \in G} yH$. Then, apply lemma 3 to get that there are elements $x_1, x_2, \ldots, x_n$ in G for some positive integer n such that

$$G = x_1H \cup x_2H \cup \cdots \cup x_nH$$

where $x_iH \cap x_jH = \phi$, for $i \neq j$.

Hence,

$$|G| = |x_1H| + |x_2H| + \cdots + |x_nH|$$

$$= |H| + |H| + \cdots + |H|, \quad \text{where } |H| \text{ appears } n \text{ times here}$$

.

$$\Rightarrow |H| \text{ divides } |G|$$

and we are done.

Example 3.

$\mathbb{Z}_{11}$ has no subgroups except the trivial subgroup and the group $\mathbb{Z}_{11}$ itself.

Proof.

If H is a subgroup of $\mathbb{Z}_{11}$, then by Lagrange's theorem we have that $|H|$ divides 11. Hence, $|H| = 1$ or 11 and we are done.

Example 4.

S_4 has no subgroup of order 5.

Proof.

If H is a subgroup of S_4, then by Lagrange's theorem we have that $|H|$ divides 24. Hence, $|H| \neq 5$ and we are done.

Lemma 4.

Suppose G is a group and $x \in G$. Suppose H is the cyclic subgroup of G that is generated by x, i.e. $H =< x >$. Then, $|H| = o(x)$.

Proof.

Suppose e is the identity in G. There are two cases to consider. The first is where G is a finite group and the second is where G is an infinite group.

Case 1 – Suppose G is a finite group. Then H is a finite group. Now, $H = \{x^k : k \in \mathbb{Z}\}$ and so there exists integers r, s such that $x^r = x^s$ with $r > s$. Hence $x^{r-s} = e$ and so $o(x)$ is finite. Suppose $o(x) = t$, where $t \in \mathbb{N}$. Then, $H = \{e, x, x^2, \ldots, x^{t-1}\}$ and so $|H| = t = o(x)$ and we are done.

Case 2 – Suppose G is an infinite group. Then, either $o(x)$ is finite or infinite. If $o(x)$ is finite, say $o(x) = t$, where $t \in \mathbb{N}$, then $H = \{e, x, x^2, \ldots, x^{t-1}\}$ and so $|H| = t = o(x)$ and we are done. Otherwise, $o(x)$ is infinite and then $H = \{x^k : k \in \mathbb{Z}\}$ has infinitely many different elements in it and so $|H| = \infty = o(x)$ and we are done.

Theorem 2.

Suppose G is a finite group and $x \in G$. Then, $o(x)$ divides $|G|$.

Proof. Proceed as in case 1 in the proof of lemma 4 to get that $H =< x >$ is a subgroup of G with $|H| = o(x)$. Now, by Lagrange's theorem, we have that $|H|$ divides $|G|$ and so $o(x)$ divides $|G|$ and we are done.

Example 5.

$\mathbb{Z}_{11}$ has no element with order 5 because 5 does not divide 11.

MT316A – GROUPS

Fiacre Ó Cairbre

Lecture 1

Chapter 1 – Definition and Examples.

Section 1.1 – A little bit of history of group theory.

Galois is considered the founder of group theory around 1832. The ideas in group theory have turned out to be very powerful in solving many important problems in mathematics, science and other areas.

Section 1.2 – Definition of a Group.

Remark 1. We will motivate the definition of a group by looking at two examples first.

Example 1. Consider the set of integers: $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3\ldots\}$.

Note the following four facts:

(i) $a + b \in \mathbb{Z}, \quad \forall \quad a, b \in \mathbb{Z}$

(ii) $a + 0 = a, \quad \forall \quad a \in \mathbb{Z}$

(iii) For every $a \in \mathbb{Z}$, there exists $b \in \mathbb{Z}$ such that $a + b = 0$

(iv) $a + (b + c) = (a + b) + c, \quad \forall \quad a, b, c \in \mathbb{Z}$

Example 2.

Consider the set of non–zero real numbers: $P = \{x \in \mathbb{R} : x \neq 0\}$.

Note the following four facts:

(i) $ab \in P, \quad \forall \quad a, b \in P$

(ii) $a1 = a, \quad \forall \quad a \in P$

(iii) For every $a \in P$, there exists $b \in P$ such that $ab = 1$

(iv) $a(bc) = (ab)c, \quad \forall \quad a, b, c \in P$

Definition 1.

Suppose we have a set S with an operation $*$ which acts on pairs of elements $a, b \in S$ to create $a * b$. We say that S is closed under $*$ if

$$a * b \in S, \quad \forall \quad a, b \in S$$

Remark 2.

Fact (i) in example 1 shows that $\mathbb{Z}$ is closed under addition. Fact (i) in example 2 shows that P is closed under multiplication.

Example 3.

Give an example of a set K (where K is a subset of $\mathbb{Z}$) such that $a+b \notin K$, for some $a, b \in K$.

Solution.

We can take $K = \{x \in \mathbb{Z} : 1 \leq x \leq 10\}$ and see that $3 + 8 \notin K$, with $3, 8 \in K$. This example shows that K is not closed under addition.

Definition 2.

Suppose S is a set. Then, $S \times S = \{(a, b) : a, b \in S\}$.

Definition 3.

Suppose S is a set and f is a function such that $f : S \times S \to S$. Then f is called a binary operation on S.

Example 4.

From example 1 we see that addition is a binary operation on $\mathbb{Z}$ because

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$

$$(a, b) \to a + b$$

Similarly, from example 2(i) we see that multiplication is a binary operation on P. From example 3 we see that addition is not a binary operation on K.

Remark 3.

Note that by using definitions 1 and 3 we see that S is closed under the operation $* \iff *$ is a binary operation on S.

Remark 4.

Suppose S is a set and $*$ is an operation. Then, the notation $(S, *)$ means that we consider S with the operation $*$. The reason for this notation $(S, *)$ is because when we define a group later, it will be important to know what operation we are considering.

Definition 4.

Suppose S is a set that is closed under the operation $*$. If there exists $e \in S$ such that

$$a * e = a = e * a, \quad \forall \quad a \in S$$

then e is called an identity element of $(S, *)$.

Remark 5.

In definition 4 it's important to know which operation we are considering because an element of a set S may be an identity under one operation but not under a different operation. For example, 0 is an identity of $(\mathbb{Z}, +)$ because $0 + a = a = a + 0, \quad \forall \quad a \in \mathbb{Z}$, but 0 is not an identity of $(\mathbb{Z}, \times)$, where $\times$ denotes the usual multiplication operation on $\mathbb{Z}$, because $0 \times 1 \neq 1$.

Definition 5.

Suppose S is closed under $*$ and suppose e is an identity element of $(S, *)$. Suppose $a \in S$. If there exists $b \in S$ such that

$$a * b = e = b * a$$

then b is called an inverse of a.

Definition 6 – Definition of a Group.

Suppose S is a non–empty set. Then $(S, *)$ is called a group if the following conditions are satisfied:

(i) $a * b \in S, \quad \forall \quad a, b \in S$

(ii) There exists $e \in S$ such that $a * e = a = e * a, \quad \forall \quad a \in S$.

(iii) If $a \in S$, then there exists $b \in S$ such that $a * b = e = b * a$.

(iv) $(a * b) * c = a * (b * c), \quad \forall \quad a, b, c \in S$.

MT316A – GROUPS

Fiacre Ó Cairbre

Example 5.

We see that $(\mathbb{Z}, +)$ is a group from example 1 where $+$ denotes the usual addition in $\mathbb{Z}$, because conditions (i), (ii), (iii) and (iv) in example 1 give us conditions (i), (ii), (iii) and (iv) in definition 6.

Similarly, $(P, \times)$ is a group from example 2 where $\times$ denotes the usual multiplication in the reals,

Remark 6.

In definition 6, (i) means that S is closed under $*$, (ii) means that there exists an identity e of $(S, *)$ and (iii) means that b is an inverse of a. We say that the operation $*$ is associative if condition (iv) in definition 6 is satisifed.

Example 6.

Is $(\mathbb{Z}, \times)$ a group where $\times$ denotes the usual multiplication in $\mathbb{Z}$?

Solution.

No, and here is a proof. First note that 1 is an identity element of $(\mathbb{Z}, \times)$ because $1 \times a = a = a \times 1$, for all $a \in \mathbb{Z}$. Now, 2 has no inverse because there is no $b \in \mathbb{Z}$ such that $2 \times b = 1$. So, condition (iii) in definition 6 is not satisfied and hence $(\mathbb{Z}, \times)$ is not a group.

Remark 7.

Notice that $(\mathbb{Z}, +)$ is a group but $(\mathbb{Z}, \times)$ is not a group.

Definition 7.

A group $(G, *)$ is called abelian if $a * b = b * a, \quad \forall \quad a,\ b \in G$. If a group is not abelian, then we call it non–abelian.

Example 7: $\mathbb{Z}_m$, the set of integers modulo m.

Suppose m is an integer and $m \geq 2$. Recall the set of integers modulo m denoted by $\mathbb{Z}_m$.

For us here we will think of $\mathbb{Z}_m$ as the set

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$$

with the operation of addition (mod m), denoted by $*$, which means that if $a, b \in \mathbb{Z}_m$, then $a * b$ is defined to be the remainder when the usual sum of a and b is divided by m. So, $a * b \in \mathbb{Z}_m$.

It's important to note that the elements of $\mathbb{Z}_m$ are not ordinary integers because, for example, in $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ we have that $2 * 4 = 1$ because 1 is the remainder when the

usual sum of 2 and 4 is divided by 5. Notice also that addition (mod 5) in $\mathbb{Z}_5$ is different from the usual addition in $\mathbb{Z}$ because again $2 * 4 = 1$ in $\mathbb{Z}_5$.

One can show that $(\mathbb{Z}_m, *)$ is a group, for $m \geq 2$, as follows:

(i) $a * b \in \mathbb{Z}_m, \quad \forall \quad a, b \in \mathbb{Z}_m$, as mentioned above.

(ii) 0 is an identity element in $(\mathbb{Z}_m, *)$, because $0 * a = a = a * 0, \quad \forall \quad a \in \mathbb{Z}_m$

(iii) If $a \in \mathbb{Z}_m$ and $a \neq 0$, then $m - a \in \mathbb{Z}_m$ is an inverse of a because $a * (m - a) = 0 = (m - a) * a$. Note that 0 is an inverse of 0.

(iv) One can check that

$$(a * b) * c = a * (b * c), \quad \forall \quad a, b, c \in \mathbb{Z}_m$$

So, the 4 conditions in definition 6 are satisfied and hence $(\mathbb{Z}_m, *)$ is a group for $m \geq 2$.

Note that $*$ above, for addition (mod m) on $\mathbb{Z}_m$, is usually just written as $+$ as long as there is no confusion with ordinary addition in $\mathbb{Z}$. So, we can now write that $2 + 4 = 1$ in $\mathbb{Z}_5$ and also say that $(\mathbb{Z}_m, +)$ is a group for $m \geq 2$. We will assume the operation on $\mathbb{Z}_m$ is addition (mod m) unless otherwise stated.

Remark 8.

Suppose $(G, *)$ is a group and $x, y \in G$. For convenience of notation we will often write $x * y$ as xy.

Furthermore, for convenience of notation, we will often just say 'suppose G is a group' instead of saying ' suppose $(G, *)$ is a group'. However, it should always be clear what operation we are considering when we are working with a group.

Lemma 1.

Suppose G is a group. Then G has a unique identity element.

Proof.

Suppose that e and f are identity elements of G. Then, $ef = e$ and $ef = f$ and so $e = f$ and we are done.

Lemma 2.

Suppose G is a group and $x \in G$. Then x has a unique inverse. The unique inverse of x is denoted by x^{-1}.

Proof.

Suppose that y and z are inverses of x. Also, suppose e is the identity element of G. Then

$$xy = e = yx \quad \text{and} \quad xz = e = zx$$

Now, $(zx)y = z(xy) = ze = z$. Also, $(zx)y = ey = y$. Hence, $z = y$ and we are done.

Example 8.

$2^{-1} = 3$ in $\mathbb{Z}_5$ because $2 + 3 = 0$ in $\mathbb{Z}_5$.

Remark 9.

We will introduce some notation here. Suppose G is a group with identity element e. Suppose $a \in G$. We can write the element aa as a^2. Similarly, we can write a^2a as a^3. In the same way, for a positive integer n, we can write $aaa \dots a$ (where a appears n times here) as a^n. Note that this also means that $a^1 = a$.

We define a^0 to be e.

Also, if $t \in \mathbb{Z}$ and $t < 0$, we define a^t to be the inverse of a^{-t} which makes sense because $-t$ is a positive integer. Thus a^t is defined to be $(a^{-t})^{-1}$.

In this way, we have now defined a^r where r is any integer.

Definition 8.

Suppose G is a group with identity element e. Suppose $a \in G$. The order of a is the least positive integer k such that $a^k = e$. If there is no positive integer r such that $a^r = e$, then we say that the order of a is infinity (denoted by ∞). We denote the order of a by $o(a)$.

Example 9.

Find the order of each element in $\mathbb{Z}_6$.

Solution.

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ and 0 is the identity in $\mathbb{Z}_6$.

Note that $0^1 = 0$ so $o(0) = 1$.

Note that if $a \in \mathbb{Z}_6$ and n is a positive integer, then from remark 9, a^n means $a + a + a + \dots + a$, where a is added (mod 6) to itself n times here.

Now $o(2) = 3$ because

$$2^1 = 2 \neq 0, \quad 2^2 = 2 + 2 = 4 \neq 0, \quad 2^3 = 2 + 2 + 2 = 0$$

So, 3 is the least positive integer k such that $2^k = 0$ and so $o(2) = 3$.

Similarly, $o(3) = 2$ because

$$3^1 = 3 \neq 0, \quad 3^2 = 3 + 3 = 0$$

So, 2 is the least positive integer k such that $3^k = 0$ and so $o(3) = 2$.

Similarly, $o(4) = 3$, $o(5) = 6$ and $o(1) = 6$ and we are done.

MT316A – GROUPS

Fiacre Ó Cairbre

Lecture 3

Example 10.

Consider the group $\mathbb{Z}$ with the operation of usual addition and consider $2 \in \mathbb{Z}$. Then $o(2) = \infty$, because there is no positive integer r such that $2^r = 0$. Note that 2^r here means $2 + 2 + 2 + \cdots + 2$, where 2 is added to itself r times.

Definition 9.

Suppose G is a group. Then the order of G is defined to be the number of elements in G and is denoted by $|G|$.

Example 11.

(i) $|\mathbb{Z}_m| = m$, for $m \geq 2$.

(ii) $|\mathbb{Z}| = \infty$.

Example 12.

For $n \geq 2$, suppose T_n denotes that set of invertible $n \times n$ matrices with real entries. We will now prove that T_n (with the operation of usual matrix multiplication) is a group, for $n \geq 2$. This group T_n is also denoted by $GL(n)$.

Proof.

First note that T_n is non–empty because the identity $n \times n$ matrix, I_n, is an element of T_n. Recall that I_n is the $n \times n$ matrix with 1 everywhere on the main diagonal and zero everyewhere else.

(i) $AB \in T_n$, for all $A, B \in T_n$, because the product of two invertible matrices is an invertible matrix. So, conditon (i) in definition 6 is satisfied.

(ii) $I_n A = A = A I_n$, for all $A \in T_n$ and so condition (ii) in definition 6 is satisfied.

(iii) Recall from linear algebra that if $A \in T_n$, then A has a (matrix) inverse denoted by A^{-1} such that $AA^{-1} = I_n = A^{-1}A$. Note that $A^{-1} \in T_n$ and so condition (iii) in definition 6 is satisfied.

(iv) $(AB)C = A(BC)$, for all $A, B, C \in T_n$ and so condition (iv) in definition 6 is satisfied.

So, all four conditions in definition 6 are satisfied and hence T_n is a group for $n \geq 2$.

Example 13.

$GL(2)$ is a non–abelian group.

Proof.

Consider the two matrices, $A, B \in GL(2)$ where

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Then,

$$AB = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \qquad BA = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$$

So, $AB \neq BA$ and hence $GL(2)$ is a non–abelian group.

Remark 10.

Suppose G is a group and $x \in G$. Then, $x^{r+s} = x^r x^s$, for any integers, r, s. Also, $(x^r)^s = x^{rs}$, for any integers, r, s.

Lemma 3.

Suppose G is a group with identity element e and suppose $x \in G$. Suppose $o(x) = k$, where k is finite, and suppose $x^n = e$. Then $n = rk$, for some integer r.

Proof.

If we divide k into n, then we will get that

$$n = qk + s, \quad \text{where} \quad q, s \in \mathbb{Z} \quad \text{with} \quad 0 \leq s < k$$

Now,

$$x^n = x^{qk+s} = x^{qk} x^s = (x^k)^q x^s = e^q x^s = e x^s = x^s$$

So, $x^s = e$ and hence $s = 0$ because k is the least positive integer such that $x^k = e$. So, we have $n = qk$, for some integer q and we are done.

Lemma 4.

Suppose G is a group and $x \in G$ with $o(x) = k$, where k is finite. Then,

$$o(x^m) = \frac{k}{gcd(k, m)}$$

where $m \in \mathbb{Z}$ and $m > 0$ and $gcd(k, m)$ denotes the greatest common divisor of k and m.

Example 14.

Consider $0 \in \mathbb{Z}$ and let $S = \{0\}$. Then, S is a group with the usual addition.

Consider $1 \in \mathbb{Z}$ and let $L = \{1\}$. Then, L is a group with the usual multiplication.

Note that both groups L and S contain exactly one element each. It turns out that all groups which contain exactly one element can be considered essentially to be the same because if $(\{y\}, *)$ is any group that contains exactly one element y, then we have

$$y * y = y, \qquad y \text{ is the identity element in the group} \qquad \text{and} \quad y^{-1} = y$$

Any group that contains exactly one element is called the trivial group. Also, if a group contains more than one element, then it's called a non–trivial group.

Section 1.2 – Subgroups.

Definition 10.

Suppose $(G, *)$ is a group and H is a subset of G. Then, we say that H is a subgroup of G if $(H, *)$ is a group. Note that here the operation on H is the same as the operation on G.

Example 15.

$(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$, where $\mathbb{R}$ denotes the set of real numbers and $+$ is usual addition.

Remark 11.

From now on, when we consider $\mathbb{Z}$ as a group, we wll always be using the operation of usual addition, unless otherwise stated.

Example 16.

Consider the group $\mathbb{Z}_6$.

(a) Is $H = \{0, 3\}$ a subgroup of $\mathbb{Z}_6$?

(b) Is $W = \{0, 1, 3\}$ a subgroup of $\mathbb{Z}_6$?

Solution.

(a) Yes, and here is a proof: H is non–empty and:

(i) $a + b \in H$, for all $a, b \in H$.

(ii) $0 + a = a = a + 0$, for all $a \in H$.

(iii) If $a \in H$, then there exists $b \in H$ such that $a + b = 0 = b + a$.

(iv) $(a + b) + c = a + (b + c)$, for all $a, b, c \in H$.

So, all the conditions in defintion 6 are satisfied and hence H (with the operation $+$) is a group and so H is a subgroup of $\mathbb{Z}_6$.

(b) No, and here is a proof: Condition (i) in definition 6 is not satisfied because $1 + 3 \notin W$ with $1, 3 \in W$. Hence, W is not a group (with the operation $+$) and so W is not a subgroup of $\mathbb{Z}_6$.

Example 17.

Suppose $(G, *)$ is a group with identity element e. Then $(G, *)$ itself is a subgroup of $(G, *)$. Also, the trivial group $(\{e\}, *)$ is a subgroup of $(G, *)$.

MT316A – GROUPS

Fiacre Ó Cairbre

Lecture 4

Proposition 1.

A non–empty subset H of a group G is a subgroup of $G \iff ab^{-1} \in H$, for all $a, b \in H$.

Proof.

We first prove the $\Rightarrow$ part: H is a group and so $b^{-1} \in H$ and hence $ab^{-1} \in H$ and so we have proved the $\Rightarrow$ part:

We next prove the $\Leftarrow$ part: Our aim is to show that H is a group and we will do that by showing that the four conditions of definition 6 are satisfied for H. Suppose e is the identity element of G. Suppose $x \in H$. Then, $xx^{-1} \in H$ and so $e \in H$. Hence, H has an identity element and condition (ii) in definition 6 is satisfied.

Next, suppose $y \in H$. Then, $ey^{-1} \in H$ and so $y^{-1} \in H$. Hence, condition (iii) in definition 6 is satisfied. Now, suppose $v, w \in H$. Then

$$w^{-1} \in H \ \Rightarrow \ v(w^{-1})^{-1} \in H \ \Rightarrow \ vw \in H$$

and so condition (i) in definition 6 is satisfied.

Finally, $(xy)z = x(yz)$, for all $x, y, z \in H$ and so condition (iv) in definition 6 is satisfied. So, overall H is a group and hence H is a subgroup of G. So, we have proved the $\Leftarrow$ part and we are done.

Example 18.

Consider the group $\mathbb{Z}$. Suppose H is the set of even integers. Then, H is a subset of $\mathbb{Z}$. Is H a subgroup of $\mathbb{Z}$?

Solution.

Yes, and here is a proof: Note that if $a, b \in H$, then $ab^{-1} = a - b \in H$ and so by proposition 1 we get that H is a subgroup of $\mathbb{Z}$.

Theorem 1.

Denote the set of positive integers (or natural numbers) by $\mathbb{N}$ and so $\mathbb{N} = \{1, 2, 3, \ldots\}$. Then, the non–trivial subgroups of $\mathbb{Z}$ are $n\mathbb{Z}$, for $n \in \mathbb{N}$, where $n\mathbb{Z}$ is the set of integer multiples of n, i.e.

$$n\mathbb{Z} = \{\ldots, -2n, -n, 0, n, 2n, 3n, \ldots\}$$

Proof.

Suppose H is a non–trivial subgroup of $\mathbb{Z}$. Then, H must contain a smallest positive number t. Now, $t\mathbb{Z}$ is a subset of H. We will prove that H is a subset of $t\mathbb{Z}$ and hence we will have that $H = t\mathbb{Z}$ and we will be done.

Consider $m \in H$. Then, if we divide t into m we get that

$$m = kt + r, \quad \text{where} \quad k,\ r \in \mathbb{Z} \quad \text{with} \quad 0 \leq r < t$$

Now, $r = m - kt \in H$ and so $r = 0$ because t is the least positive number in H. Thus, $m = kt$ and so H is a subset of $t\mathbb{Z}$. Hence $H = t\mathbb{Z}$ and we are done.

CHAPTER 2 – Permutation Groups.

Section 2.1 – Definition and Examples.

Definition 1.

(i) Suppose X and Y are sets and $f : X \to Y$ is a function. Then, f is called $1 - 1$ if

$$a \neq b \ \Rightarrow \ f(a) \neq f(b), \quad \text{for} \ \ a,\ b \in X$$

(ii) Suppose X and Y are sets and $f : X \to Y$ is a function. Then, f is called onto if

$$z \in Y \ \Rightarrow \ z = f(w), \quad \text{for some} \ \ w \in X$$

Definition 2.

Suppose X and Y are sets and $f : X \to Y$ is a function. Then, f is called a bijection if f is $1 - 1$ and onto.

Definition 3.

Suppose V is a non–empty set and $f : V \to V$ is a bijection. Then, we call f a permutation of V. Denote the set of all permutations of V by $\mathrm{Sym}(V)$.

Theorem 1.

Suppose W is a non–empty set. Then, $\mathrm{Sym}(W)$ (with the operation of composition of functions) is a group.

Proof.

First note that $\mathrm{Sym}(W)$ is non–empty because $I \in \mathrm{Sym}(W)$ where I is the function

$$I : W \to W$$

$$x \to x$$

Suppose $f, g \in \mathrm{Sym}(W)$. Denote the composition f after g by $f \circ g$. This means that $(f \circ g)(x) = f(g(x))$, for $x \in W$. Note that $f \circ g \in \mathrm{Sym}(W)$, for all $f, g \in \mathrm{Sym}(W)$ and so condition (i) in definition 6 in chapter 1 is satisfied.

Note that I above will be an identity element of $\mathrm{Sym}(W)$ because $I \circ f = f = f \circ I$, for all $f \in \mathrm{Sym}(W)$ and so condition (ii) in definition 6 is satisfied.

MT316A – GROUPS

Fiacre Ó Cairbre

Lecture 5

Continuation of the proof of Theorem 1.

If $f \in \text{Sym}(W)$, then the inverse function f^{-1} is an element of $\text{Sym}(W)$ and we have $f \circ f^{-1} = I = f^{-1} \circ f$. So, condition (iii) in definition 6 is satisfied.

Finally, we have that

$$(f \circ g) \circ h = f \circ (g \circ h), \quad \text{for all} \quad f,\ g,\ h, \in \text{Sym}(W)$$

and so condition (iv) in definition 6 is satisfied. Hence, $\text{Sym}(W)$ (with the operation of composition of functions) is a group.

Definition 4.

Suppose $n \in \mathbb{N}$. The symmetric group (on n symbols) is denoted by S_n and is defined by:

$$S_n = \text{Sym}(W), \quad \text{where} \quad W = \{1, 2, 3, \ldots, n\}$$

Remark 1.

Note that the elements of S_n are the permutations of $\{1, 2, 3, \ldots, n\}$.

Remark 2.

We will now discuss some notation. Consider the function

$$\alpha : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$$

where $\alpha(1) = 4,\ \alpha(2) = 3,\ \alpha(3) = 1,\ \alpha(4) = 2$.

Then, $\alpha \in \text{Sym}(W)$, where $W = \{1, 2, 3, 4\}$ and so $\alpha \in S_4$. For convenience of notation, we denote the permutation α by

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \qquad (*)$$

where this notation means that α takes a number in the top row to the corresponding number directly below it in the bottom row. It's important to note that the notation in $(*)$ above does not correspond to a matrix. Another example of this notation in $(*)$ is

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

which means that β is the permutation in S_4 given by

$$\beta : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$$

where $\beta(1) = 3,\ \beta(2) = 4,\ \beta(3) = 2,\ \beta(4) = 1$.

In the same way, we can represent any permutation in S_4 using the same type of notation as $(*)$.

Example 1.

Suppose

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \text{ and } \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \text{ in } S_4$$

Then,

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \qquad (*)$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

Remark 3.

From now on we will omit the $\circ$ symbol in $(*)$ in example 1 and so

$$\alpha\beta = \alpha \circ \beta \text{ and } \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

Example 2.

Suppose $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ in S_4. Find α^{-1}.

$$\alpha^{-1} = \begin{pmatrix} 4 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \qquad (*)$$

Remark 4.

We will now discuss some notation. Suppose $k_1, k_2, \ldots, k_m \in \{1, 2, 3, \ldots, n\}$, with $k_i \neq k_j$ for $i \neq j$. Then, $(k_1 k_2 \ldots k_m)$ denotes the permutation in S_n that maps k_1 to k_2, k_2 to k_3, k_3 to k_4 ..... k_{m-1} to k_m and finally maps k_m to k_1 and all other elements of $\{1, 2, 3, \ldots, n\}$ are mapped to themselves.

Definition 5.

(i) $(k_1 k_2 \ldots k_m)$ in remark 4, is called a cycle. The length of a cycle is the number of elements in the cycle and so $(k_1 k_2 \ldots k_m)$ has length m.

(ii) An m–cycle is a cycle of length m.

Example 3.

In S_4 the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$

can be expressed as the cycle (134). Note that (134) is a 3–cycle.

Also, $(134)(12) = (1234)$ and $(134)^{-1} = (143)$.

Note that $(134) = (341) = (413)$.

Example 4.

(i) $S_2 = \{I, (12)\}$, where I is the identity in S_2 from Theorem 1. Note that S_2 is abelian.

(ii)

$$S_3 = \{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\}$$

$$= \{I, (12), (13), (23), (123), (132)\}$$

where I is the identity in S_3 from Theorem 1. Note that $|S_3| = 6$. Also, S_3 is non–abelian because

$$(12)(13) = (132) \quad \text{but} \quad (13)(12) = (123)$$

and so

$$(12)(13) \neq (13)(12)$$

MT316A – GROUPS

Fiacre Ó Cairbre

Lecture 6

Theorem 2.

S_n is non–abelian for $n \geq 3$.

Proof.

Consider $(12),\ (13) \in S_n$ for $n \geq 3$. Then, as in example 4 we have that $(12)(13) \neq (13)(12)$ and so S_n is non–abelian.

Theorem 3.

$|S_n| = n!$, for $n \geq 2$.

Proof.

The different elements of S_n correspond to the different ways of filling in the bottom row of

$$\begin{pmatrix} 1 & 2 & 3 & 4 & . & . & . & n \\ . & . & . & . & . & . & . & . \end{pmatrix}$$

So, there are $n(n-1)(n-2)\ldots.3.2.1 = n!$ different elements in S_n.

Definition 6.

Two cycles are called disjoint if they have no elements in common.

Example 5.

(134) and (25) are disjoint cycles in S_5. (134) and (12) are not disjoint cycles in S_5.

Example 6.

We know from theorem 3 that there are 24 elements in S_4 and here they are:

$$I, (12), (13), (14), (23), (24), (34), (123), (132), (124), (142), (134), (143), (234),$$

$$(243), (1234), (1243), (1324), (1342), (1423), (1432), (12)(34), (13)(24), (14)(23)$$

where I is the identity element in S_4 from Theorem 1.

Example 7.

Suppose $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$ in S_5. Express α as the product (composition) of two disjoint cycles.

Solution.

$\alpha = (143)(25)$, where (143) and (25) are disjoint cycles.

Theorem 4.

Every $\alpha \in S_n$ can be expressed as a cycle or as a product (composition) of disjoint cycles.

Corollary 1.

Up to the ordering of cycles, there is only one way to express a permutation as a product (composition) of disjoint cycles.

Example 8.

Consider the permutation α from example 7. Then, $\alpha = (143)(25)$. Also, $\alpha = (25)(143)$ and there is no other way to express α as a product of disjoint cycles.

Definition 7.

Suppose G is a group and $x, y \in G$. Then, we say that x and y commute in G if $xy = yx$.

Theorem 5.

Suppose α, β are disjoint cycles in S_n. Then α and β commute in S_n, i.e. $\alpha\beta = \beta\alpha$.

Proof.

The elements in α and β come from disjoint subsets of $\{1, 2, 3, \ldots, n\}$.

Example 9.

In S_6, we have $(12)(45) = (45)(12)$.

Lemma 1.

Suppose α is a k–cycle in S_n. Then, $o(\alpha) = k$.

Proof.

Suppose $\alpha = (b_1 b_2 \ldots . b_k)$. Then $\alpha^k = I$, where I is the identity element in S_n. Also, k is the least positive integer such that $\alpha^k = I$. Hence, $o(\alpha) = k$.

Example 10.

Suppose $\alpha = (2351)$ in S_6. Then, $o(\alpha) = 4$.

Theorem 6.

Suppose $\alpha = \beta_1 \beta_2 \ldots \beta_t$, where β_i and β_j are disjoint cycles for $i \neq j$. Suppose $o(\beta_i) = m_i$, for $1 \leq i \leq t$. Then, $o(\alpha) =$ lcm $\{m_1, m_2, \ldots, m_t\}$.

Example 11.

Suppose $\alpha = (12)(45)(367)$ in S_7. Then, $o(\alpha) =$ lcm $\{2, 2, 3\} = 6$.

MT316A – GROUPS

Fiacre Ó Cairbre

Lecture 7

Remark 5.

A 2–cycle is also called a transposition.

Theorem 7.

Suppose $\alpha \in S_n$ with $n \geq 2$. Then, α can be expressed as a product (composition) of transpositions.

Proof.

We know from theorem 4 that α can be expressed as a cycle or product of disjoint cycles. Now, any cycle $(b_1 b_2 \dots b_t)$ can be expressed as the following product of transpositions: $(b_1 b_t)(b_1 b_{t-1}) \dots (b_1 b_3)(b_1 b_2)$. Consequently, α can be expressed as a product of transpositions.

Example 12.

Express $\alpha = (124)(356)$ in S_6 as a product of transpositions.

Solution.

(i) $(124)(356) = (14)(12)(36)(35)$.

Theorem 8.

Suppose $\alpha \in S_n$. Suppose $\alpha = \beta_1 \beta_2 \dots \beta_m$ and $\alpha = \sigma_1 \sigma_2 \dots \sigma_k$, where all the β_i and σ_j are transpositions for $1 \leq i \leq m$, $1 \leq j \leq k$. Then, m and k are either both even or both odd.

Example 13.

Note that $\alpha = (124)(356)$ in S_6 in example 12 can also be expressed as the following product of transpositions: $(14)(13)(13)(12)(36)(35)$ because $(13)(13) = I$, where I is the identity in S_6. So, α can be expressed as the product of four transpositions (as in example 12) and also as the product of six transpositions.

Definition 8.

(i) $\alpha \in S_n$ is called an even permutation if it can be expressed as a product of an even number of transpositions.

(ii) $\alpha \in S_n$ is called an odd permutation if it can be expressed as a product of an odd number of transpositions.

Example 14.

Suppose $\alpha = (1245)(352)$ in S_6. Then, $\alpha = (15)(14)(12)(32)(35)$ and so α is an odd permutation.

Remark 6.

(i) Suppose G is group with identity e. If $x \in G$ with $x \neq e$, then we say that x is a non–identity element.

(ii) If G is a group and $|G|$ is finite, then we say that G is a finite group. If $|G| = \infty$, then we say that G is an infinite group.

Theorem 9.

Suppose $A_n = \{\alpha \in S_n : \alpha \text{ is even}\}$ for $n \geq 2$. Then, A_n is a subgroup of S_n and we call A_n the alternating group.

Proof.

Suppose I is the identity in S_n. Then $I = (12)(12)$ and so $I \in A_n$ and hence A_n is non–empty.

Suppose $\alpha, \beta \in A_n$. Then, $\alpha = \sigma_1\sigma_2 \ldots \sigma_k$, where k is even and the σ_i are transpositions for $1 \leq i \leq k$ and also $\beta = \gamma_1\gamma_2 \ldots \gamma_m$, where m is even and the γ_i are transpositions for $1 \leq i \leq m$.

Now note that

$$\beta^{-1} = \gamma_m^{-1}\gamma_{m-1}^{-1} \ldots \gamma_2^{-1}\gamma_1^{-1} = \gamma_m\gamma_{m-1} \ldots \gamma_2\gamma_1$$

and so

$$\alpha\beta^{-1} = \sigma_1\sigma_2 \ldots \sigma_k\gamma_m\gamma_{m-1} \ldots \gamma_2\gamma_1$$

which means that $\alpha\beta^{-1} \in A_n$. So, by proposition 1 in lecture 4, we get that A_n is a subgroup of S_n.

Theorem 10.

$|A_n| = \dfrac{n!}{2}$, for $n \geq 2$.

Proof.

Suppose $\alpha, \beta \in A_n$ with $\alpha \neq \beta$. Then, $(12)\alpha \neq (12)\beta$ with $(12)\alpha$ and $(12)\beta$ both odd permutations.

Also, suppose γ, σ are odd permutations in S_n with $\gamma \neq \sigma$. Then, $(12)\gamma \neq (12)\sigma$ with $(12)\gamma$ and $(12)\sigma$ both even permutations.

Thus, the number of odd permutations in S_n is equal to the number of even permutations in S_n and so $|A_n| = \dfrac{|S_n|}{2} = \dfrac{n!}{2}$

Example 15.

$|A_4| = 12$.

Example 16.

(i) $A_3 = \{I, (123), (132)\}$, where I is the identity in S_3. Notice that A_3 is abelian.

(ii) Notice that A_4 is non–abelian because $(123), (124) \in A_4$ and $(123)(124) \neq (124)(123)$.

Chapter 3 – Cyclic Groups.

Definition 1.

Suppose G is a group and L is a non–empty subset of G. Then, we say that L is a generating set for G if

$$G = \{x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} : x_i \in L,\ \alpha_i = \pm 1 \ \text{ for } \ 1 \leq i \leq n, \ \text{ and } \ n \ \text{ is any positive integer}\}$$

We also say that G is generated by L.

Remark 1.

Suppose L is a non–empty subset of a group G. Let $\underline{L} = \{x^{-1} : x \in L\}$. Then, definition 1 is essentially saying that L generates G if every element of G can be expressed as a product of elements from $L \cup \underline{L}$, where $\cup$ here denotes the union of two sets.

Example 1.

$\{1\}$ is a generating set for $\mathbb{Z}$ and $\{2, 3\}$ is a generating set for $\mathbb{Z}$.

Example 2.

$\{2\}$ is not a generating set for $\mathbb{Z}$.

Definition 2.

Suppose X is a generating set for a group G. Then, X is called a minimal generating set for G if, by removing any element of X, the resulting set is not a generating set for G.

Example 3.

$\{1\}$ is a minimal generating set for $\mathbb{Z}$ and $\{2, 3\}$ is a minimal generating set for $\mathbb{Z}$.

Example 4.

$\{1, 2, 3\}$ is not a minimal generating set for $\mathbb{Z}$.

Definition 3.

Suppose G is a group and suppose theres exists an $x \in G$ such that $\{x\}$ is a generating set for G. Then, G is called a cyclic group. We also say that G is generated by x and that x is a generator for G.

MT316A – GROUPS

Fiacre Ó Cairbre

Lecture 8

Example 5.

$\mathbb{Z}$ is a cyclic group because $\{1\}$ is a generating set for $\mathbb{Z}$. Also, 1 is a generator for $\mathbb{Z}$.

Example 6.

$\mathbb{Z}_4$ is a cyclic group because $1 \in \mathbb{Z}_4$ is a generator for $\mathbb{Z}_4$. Note also that $3 \in \mathbb{Z}_4$ is a generator for $\mathbb{Z}_4$. However, $2 \in \mathbb{Z}_4$ is a not generator for $\mathbb{Z}_4$.

Remark 2.

If G is a cyclic group and x is a generator for G, then $G = \{x^k : k \in \mathbb{Z}\}$. Consequently, every cyclic group is abelian.

Example 7.

Is S_3 a cyclic group?

Solution.

No, because we know S_3 is non–abelian and hence by remark 2, S_3 is not cyclic.

Definition 4.

Suppose G_1 and G_2 are groups. The product group is denoted by $G_1 \times G_2$ and is defined as the set

$$G_1 \times G_2 = \{(x, y) : x \in G_1,\ y \in G_2\}$$

with the operation defined as

$$(x, y)(a, b) = (xa, yb), \quad \text{for all } \ (x, y),\ (a, b) \in G_1 \times G_2$$

Remark 3.

One can check that $G_1 \times G_2$ (in definition 4) forms a group under the given operation. Note that the identity in $G_1 \times G_2$ is (e_1, e_2) where e_1 is the identity in G_1 and e_2 is the identity in G_2. The inverse of (x, y) in $G_1 \times G_2$ is (x^{-1}, y^{-1}).

Example 8.

Suppose the groups G_1 and G_2 in definition 4 are both $\mathbb{Z}$. Then, we have the product group $\mathbb{Z} \times \mathbb{Z}$. Recall that the operation on $\mathbb{Z}$ is the usual addition which we will denote by $+$. For convenience we will also denote the operation on $\mathbb{Z} \times \mathbb{Z}$ by $+$ and so we have

$$(x, y) + (a, b) = (x + a, y + b), \quad \text{for all} \quad (x, y),\ (a, b) \in \mathbb{Z} \times \mathbb{Z} \qquad (*)$$

Note that the + on the right hand side of = in $(*)$ denotes the usual addition in $\mathbb{Z}$ whereas the + on the left hand side of = in $(*)$ denotes the operation on $\mathbb{Z} \times \mathbb{Z}$.

For example,

$$(3, -2) + (4, 1) = (3 + 4, -2 + 1) = (7, -1)$$

Example 9.

$\mathbb{Z} \times \mathbb{Z}$ (from example 8) is an abelian group.

Example 10.

$\mathbb{Z} \times \mathbb{Z}$ is not a cyclic group.

Proof.

We will prove this by contradiction. So, suppose $\mathbb{Z} \times \mathbb{Z}$ is a cyclic group. Then (a, b) is a generator for $\mathbb{Z} \times \mathbb{Z}$ for some $(a, b) \in \mathbb{Z} \times \mathbb{Z}$.

Hence, by remark 2, $\mathbb{Z} \times \mathbb{Z} = \{(a, b)^k : k \in \mathbb{Z}\}$. Now, for convenience, we will write $(a, b)^k$ as $k(a, b)$ because the operation on $\mathbb{Z} \times \mathbb{Z}$ is the + operation in example 8. For example, $(3, -4)^2 = (3, -4) + (3, -4) = 2(3, -4)$.

Now, $(1, 0) = k(a, b) = (ka, kb)$, for some $k \in \mathbb{Z}$. Hence, $1 = ka$ and $0 = kb$. So, $b = 0$. Now, we also have $(0, 1) = q(a, b)$, for some $q \in \mathbb{Z}$, which implies $1 = qb = 0$ which is impossible.

So, our supposition that $\mathbb{Z} \times \mathbb{Z}$ is a cyclic group is false and thus $\mathbb{Z} \times \mathbb{Z}$ is not a cyclic group.

Example 11.

Note that $X = \{(1, 0), (0, 1)\}$ is a generating set for $\mathbb{Z} \times \mathbb{Z}$ because if $(a, b) \in \mathbb{Z} \times \mathbb{Z}$, then

$$(a, b) = a(1, 0) + b(0, 1) = (1, 0)^a (0, 1)^b$$

Also, X is a minimal generating set for $\mathbb{Z} \times \mathbb{Z}$ because $\{(1, 0)\}$ is not a generating set for $\mathbb{Z} \times \mathbb{Z}$ and $\{(0, 1)\}$ is not a generating for $\mathbb{Z} \times \mathbb{Z}$.

Example 12.

In $\mathbb{Z} \times \mathbb{Z}_4$ we have $o(0, 1) = 4$ and $o(1, 0) = \infty$.

Lemma 1.

(i) Suppose G_1 and G_2 are both finite groups. Then, $|G_1 \times G_2| = |G_1||G_2|$.

(ii) Suppose at least one of the groups G_1, G_2 is an infinite group. Then, $G_1 \times G_2$ is an infinite group.

Example 13.

$|A_4 \times \mathbb{Z}_5| = 60$ and $A_4 \times \mathbb{Z}$ is an infinite group.

Remark 4.

Suppose G is a group and suppose $x_i \in G$ for $1 \leq i \leq n$. Let $X = \{x_1, x_2, \ldots, x_n\}$. Then, the subgroup generated by X is denoted by $< x_1, x_2, \ldots, x_n >$ and so

$$< x_1, x_2, \ldots, x_n >= \{z_1^{\alpha_1} z_2^{\alpha_2} \ldots z_t^{\alpha_t} : z_i \in X,\ \alpha_i = \pm 1,\ \text{for}\ 1 \leq i \leq t\ \text{and}\ t\ \text{any positive integer}\}$$

Remark 5.

(i) One can check that $< x_1, x_2, \ldots, x_n >$ in remark 4 is a subgroup of G.

(ii) If G is a cyclic group that is generated by an element x, then we can now write $G =< x >$.

Example 14.

$\mathbb{Z} =< 1 >$.

Example 15.

In $\mathbb{Z} \times \mathbb{Z}$ we have $< (1, 0) >= \mathbb{Z} \times \{0\}$

Chapter 4 – Lagrange's Theorem.

Definition 1.

Suppose H is a subgroup of a group G and suppose $x \in G$. We define the set xH as follows:

$$xH = \{xy : y \in H\}$$

This set xH is a subset of G and is called a left coset of H in G. The set of all left cosets of H in G is denoted by $\frac{G}{H}$.

We also define the set Hx as follows:

$$Hx = \{yx : y \in H\}$$

This set Hx is a subset of G and is called a right coset of H in G.

Example 1.

Consider the group $\mathbb{Z}_{12}$ and suppose $H = \{0, 3, 6, 9\}$. Then, one can show that H is a subgroup of $\mathbb{Z}_{12}$. We have the following left cosets of H in $\mathbb{Z}_{12}$:

MT316A – GROUPS

Fiacre Ó Cairbre

Lecture 9

Example 1 continued

$$0H = H, \quad 2H = \{2, 5, 8, 11\}, \quad 3H = H$$

Notice that $xH = Hx$, for all $x \in \mathbb{Z}_{12}$ because $\mathbb{Z}_{12}$ is abelian.

Note that since the operation on $\mathbb{Z}_{12}$ is addition (mod 12), then we can write $x + y$ for xy, where $x, y \in \mathbb{Z}_{12}$ and so we can write $2 + H$ for $2H$ and get that $2 + H = \{2, 5, 8, 11\}$.

Example 2.

Consider the subgroup A_3 of the group S_3. Then we have the following left cosets of A_3 in S_3:

$$IA_3 = A_3, \quad (12)A_3 = \{(12), (23), (13)\}, \quad (123)A_3 = A_3$$

where I is the identity in S_3.

Lemma 1.

Suppose H is a subgroup of a group G and suppose $x \in G$. Then, $xH = H \iff x \in H$.

Proof.

Proof of $\Rightarrow$: Suppose e is the identity in G. Then, $e \in H$. Now, $x = xe \in xH = H$ and so $x \in H$ and we are done.

Proof of $\Leftarrow$: xH is a subset of H. Also, if $z \in H$, then $z = xx^{-1}z \in xH$ and so H is a subset of xH. Hence, $xH = H$ and we are done.

Definition 2.

Suppose X is a subset of a group G. Then, the number of elements in X is denoted by $|X|$.

Lemma 2.

Suppose H is a subgroup of the group G. Then, $|xH| = |yH|$, for all $x, y \in G$.

Proof.

It suffices to prove that $|xH| = |H|$, for all $x \in G$. Now, note that

$$f \quad : \quad H \to xH$$

$$k \to xk$$

is a bijection and so $|H| = |xH|$ and we are done.

Lemma 3.

Suppose H is a subgroup of a group G and suppose $x, y \in G$. Then, either $xH = yH$ or $xH \cap yH = \phi$.

Theorem 1 – Lagrange's Theorem.

Suppose H is a subgroup of a finite group G. Then, $|H|$ divides $|G|$.

Proof.

First note that $G = \bigcup_{y \in G} yH$. Then, apply lemma 3 to get that there are elements $x_1, x_2, \ldots, x_n$ in G for some positive integer n such that

$$G = x_1H \cup x_2H \cup \cdots \cup x_nH$$

where $x_iH \cap x_jH = \phi$, for $i \neq j$.

Hence,

$$|G| = |x_1H| + |x_2H| + \cdots + |x_nH|$$

$$= |H| + |H| + \cdots + |H|, \quad \text{where } |H| \text{ appears } n \text{ times here}$$

.

$$\Rightarrow |H| \text{ divides } |G|$$

and we are done.

Example 3.

$\mathbb{Z}_{11}$ has no subgroups except the trivial subgroup and the group $\mathbb{Z}_{11}$ itself.

Proof.

If H is a subgroup of $\mathbb{Z}_{11}$, then by Lagrange's theorem we have that $|H|$ divides 11. Hence, $|H| = 1$ or 11 and we are done.

Example 4.

S_4 has no subgroup of order 5.

Proof.

If H is a subgroup of S_4, then by Lagrange's theorem we have that $|H|$ divides 24. Hence, $|H| \neq 5$ and we are done.

Lemma 4.

Suppose G is a group and $x \in G$. Suppose H is the cyclic subgroup of G that is generated by x, i.e. $H =< x >$. Then, $|H| = o(x)$.

Proof.

Suppose e is the identity in G. There are two cases to consider. The first is where G is a finite group and the second is where G is an infinite group.

Case 1 – Suppose G is a finite group. Then H is a finite group. Now, $H = \{x^k : k \in \mathbb{Z}\}$ and so there exists integers r, s such that $x^r = x^s$ with $r > s$. Hence $x^{r-s} = e$ and so $o(x)$ is finite. Suppose $o(x) = t$, where $t \in \mathbb{N}$. Then, $H = \{e, x, x^2, \ldots, x^{t-1}\}$ and so $|H| = t = o(x)$ and we are done.

Case 2 – Suppose G is an infinite group. Then, either $o(x)$ is finite or infinite. If $o(x)$ is finite, say $o(x) = t$, where $t \in \mathbb{N}$, then $H = \{e, x, x^2, \ldots, x^{t-1}\}$ and so $|H| = t = o(x)$ and we are done. Otherwise, $o(x)$ is infinite and then $H = \{x^k : k \in \mathbb{Z}\}$ has infinitely many different elements in it and so $|H| = \infty = o(x)$ and we are done.

Theorem 2.

Suppose G is a finite group and $x \in G$. Then, $o(x)$ divides $|G|$.

Proof. Proceed as in case 1 in the proof of lemma 4 to get that $H =< x >$ is a subgroup of G with $|H| = o(x)$. Now, by Lagrange's theorem, we have that $|H|$ divides $|G|$ and so $o(x)$ divides $|G|$ and we are done.

Example 5.

$\mathbb{Z}_{11}$ has no element with order 5 because 5 does not divide 11.

MT316A – GROUPS

Fiacre Ó Cairbre

Lecture 11

Remark 4.

(i) The subgroup H in remark 2 is also denoted by $SO(2)$ and is called a special orthogonal group. If we denote the set of 2×2 real matrices by M_2, then it turns out that

$$SO(2) = \{A \in M_2 : A^T A = I_2 \text{ and } \det A = 1\}$$

where I_2 is the 2×2 identity matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and A^T denotes the transpose of A.

$SO(2)$ is an example of what is called a matrix group because it's a group whose elements are matrices. Here are some other examples of matrix groups:

(ii) If $n \in \mathbb{N}$, then

$$SO(n) = \{A \in M_n : A^T A = I_n \text{ and } \det A = 1\}$$

where M_n is the set of real $n \times n$ matrices and I_n is the $n \times n$ identity matrix with 1 everywhere on the main diagonal and zero everywhere else. The group operation here is matrix multiplication. Note that $SO(2)$ is the example of $SO(n)$ when $n = 2$.

(ii) $GL(n)$ from example 12 in chapter 1.

(iii) $O(n) = \{A \in M_n : A^T A = I_n\}$. $O(n)$ is called an orthogonal group. One can show that $A \in O(n) \Rightarrow \det A = \pm 1$. Note that $SO(n)$ is a subgroup of $O(n)$ which is a subgroup of $GL(n)$.

Section 5.2 – Dihedral Groups and Polygons.

Definition 1.

Denote the usual xy plane by $\mathbb{R}^2$ as in remark 1. Recall from definition 3 in chapter 2 that $\mathrm{Sym}(\mathbb{R}^2)$ denotes the set of all permutations on $\mathbb{R}^2$ and also recall from theorem 1 in chapter 2 that $\mathrm{Sym}(\mathbb{R}^2)$ is a group with the operation of composition of functions.

Now, $f \in \mathrm{Sym}(\mathbb{R}^2)$ is called an isometry on $\mathbb{R}^2$ if the distance between a and b equals the distance between $f(a)$ and $f(b)$ for all $a, b \in \mathbb{R}^2$.

Remark 5.

The set of all isometries on $\mathbb{R}^2$ is a subgroup of $\mathrm{Sym}(\mathbb{R}^2)$. Denote this set of isometries on $\mathbb{R}^2$ by T.

Remark 6.

Suppose A is a non–empty subset of $\mathbb{R}^2$. Let T_A denote the set of all $f \in T$ such that

(i) $x \in A \Rightarrow f(x) \in A$.

(ii) $f(x) \in A \Rightarrow x \in A$.

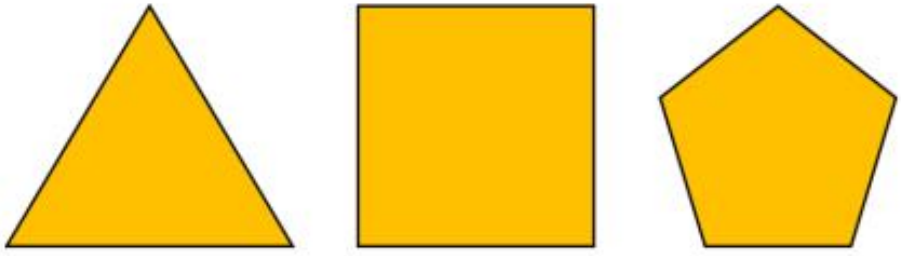
Then, T_A is a subgroup of T and T_A is called the symmetry group of A.

Remark 7.

A regular polygon with n sides is a polygon that has all n sides of equal length and all n angles are equal. A regular polygon with n sides is also called a regular n–gon (or regular n–polygon).

Example 4.

A regular 3–gon is an equilateral triangle. A regular 4–gon is a square. A regular 5–gon is a pentagon.



Definition 2.

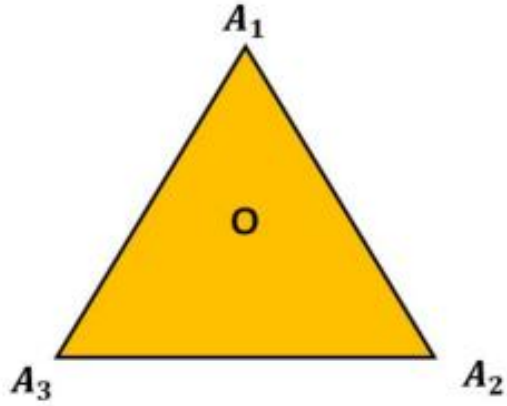
The symmetry group of the regular n–gon is called the Dihedral Group of degree n and is denoted by D_n.

Lemma 1.

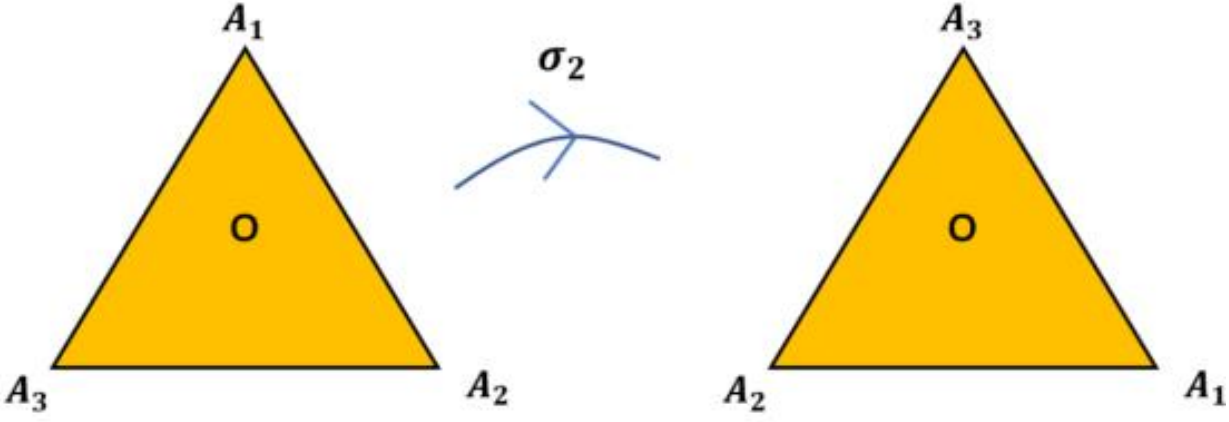
Suppose S is a regular n–gon and $f \in D_n$ and V is the set of vertices of S. Then $f(x) \in V$, for all $x \in V$.

Example 5.

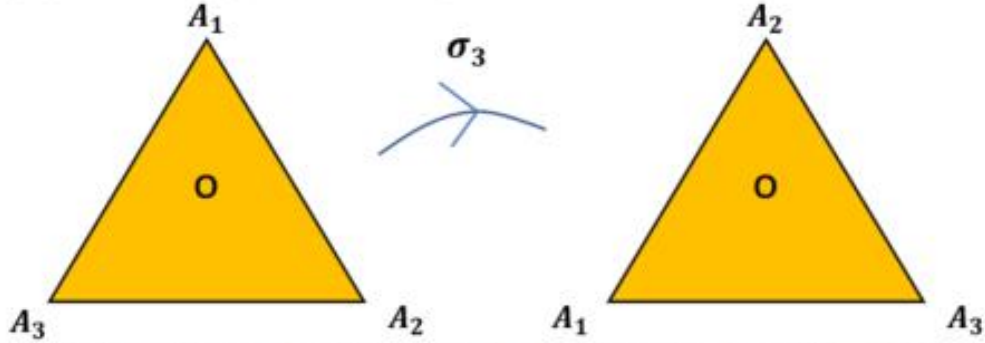
We will now look the group D_3 in detail. Note that D_3 is the symmetry group of an equilateral triangle (i.e. regular 3–gon). Suppose A_1, A_2, A_3 are the vertices of an equilateral triangle and suppose O is the centre of the equilateral triangle.



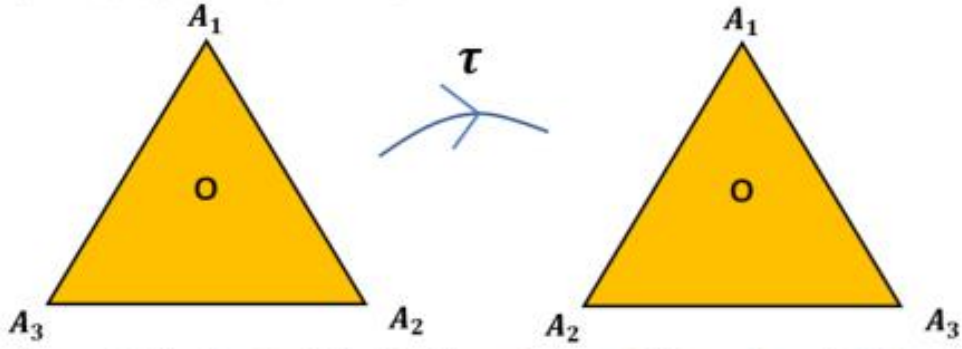
Let σ_2 denote the clockwise rotation through an angle $\frac{2\pi}{3}$ about O. Then $\sigma_2(A_1) = A_2$, $\sigma_2(A_2) = A_3$, $\sigma_2(A_3) = A_1$ and we get



Let σ_3 denote the clockwise rotation through an angle $\frac{4\pi}{3}$ about O. Then $\sigma_3(A_1) = A_3$, $\sigma_2(A_2) = A_1$, $\sigma_2(A_3) = A_2$ and we get



Let τ denote the reflection (or flip) about the line through A_1 and O. Then $\tau(A_1) = A_1$, $\tau(A_2) = A_3$, $\tau(A_3) = A_2$ and we get



Note that $\sigma_2 \circ \tau$ is the flip about the line through A_3 and O since $(\sigma_2 \circ \tau)(A_1) = A_2$, $(\sigma_2 \circ \tau)(A_2) = A_1$, $(\sigma_2 \circ \tau)(A_3) = A_3$ Similarly, $\sigma_3 \circ \tau$ is the flip about the line through A_2 and O. Denote $\sigma_2 \circ \tau$ by $\sigma_2\tau$ and denote $\sigma_3 \circ \tau$ by $\sigma_3\tau$.

Let σ_1 denote the clockwise rotation through an angle zero about O. Then σ_1 is the identity.

One can show that

$$D_3 = \{\sigma_1, \sigma_2, \sigma_3, \tau, \sigma_2\tau, \sigma_3\tau\}$$

and so $|D_3| = 6$. Also, D_3 is non–abelian because $\sigma_2\tau \neq \tau\sigma_2$. Note that $D_3 =< \tau, \sigma_2 >$ and $\{\tau, \sigma_2\}$ is a mimimal generating set for D_3.

Example 6.

Consider D_n with $n \geq 4$. Let S be the regular n–gon with n vertices $A_1, A_2, \ldots, A_n$ and centre O. Suppose σ_j is the clockwise rotation through an angle $\frac{2\pi}{n}(j-1)$ about O and suppose τ is the flip about the line through A_1 and O. One can show that

$$D_n = \{\sigma_1, \sigma_2, \ldots, \sigma_n, \tau, \sigma_2\tau, \sigma_3\tau, \ldots, \sigma_n\tau\}$$

and so $|D_n| = 2n$.

MT316A – GROUPS

Fiacre Ó Cairbre

Lecture 12

Section 5.3 – Some other applications of Groups.

Remark 8.

As mentioned before, there are many important and powerful applications of Groups. We will just mention a few more applications here.

Remark 9 – Physics.

Groups describe the symmetries which the Laws of Physics seem to obey. Also, Group Theory predicted the existence of many elementary particles before they were found experimentally.

Remark 10 – Chemistry.

The symmetry of a molecule is related to its physical properties and provides a method to determine the relevant physical information of the molecule. Groups enable one to determine symmetry.

Remark 11 – Roots of Equations.

Lagrange, Galois and others used ideas from Group Theory to try to understand when there exists a certain type of formula that would give the roots of certain equations, including the quintic (fifth degree polynomial) equation.

Remark 12 – Rubik's Cube.

Permutation groups are used to work out the algorithms that can be used to solve the Rubik's Cube.

Chapter 6 – Homomorphisms and Isomorphisms between Groups.

Section 6.1 – Homomorphisms.

Definition 1.

Suppose G_1 and G_2 are groups and $f : G_1 \to G_2$ is a function such that $f(xy) = f(x)f(y)$, for all $x, y \in G_1$. Then, f is called a group homomorphism.

From now on we will call a group homomorphism just a homomorphism.

Example 1.

Consider $\mathbb{R}$ as a group under the usual addition and consider $\mathbb{R}^+ = \{x \in \mathbb{R} : x > 0\}$ as a group under the usual multiplication. Then

$$f \ : \ \mathbb{R} \to \mathbb{R}^+$$

$$x \to e^x$$

is a homomorphism because $f(x+y) = e^{x+y} = e^x e^y = f(x)f(y), \ \ \forall \ x, y \in \mathbb{R}$.

Example 2.

Consider $\mathbb{R}$ as a group under the usual addition. Then

$$f \ : \ \mathbb{R} \to \mathbb{R} \times \mathbb{R}$$

$$x \to (x, 0)$$

is a homomorphism because $f(x+y) = (x+y, 0) = (x, 0)+(y, 0) = f(x)+f(y), \ \ \forall \ x, y \in \mathbb{R}$.

Lemma 1.

Suppose G_1 and G_2 are groups and suppose e_i is the identity in G_i. Suppose $f : G_1 \to G_2$ is a homomorphism. Then, $f(e_1) = e_2$.

Proof.

Let $y = f(e_1)$. Then, $y = f(e_1 e_1) = f(e_1)f(e_1) = y^2$. Hence $y^{-1}y = y^{-1}y^2$ and so $e_2 = y$ and we are done.

Lemma 2.

Suppose $f : G_1 \to G_2$ is a homomorphism. Then, $f(x^{-1}) = (f(x))^{-1}$, for all $x \in G_1$.

Proof.

Suppose e_i is the identity in G_i. Then,

$$e_2 = f(e_1) = f(xx^{-1}) = f(x)f(x^{-1})$$

$$\Rightarrow (f(x))^{-1} = f(x^{-1})$$

and we are done.

Lemma 3.

Suppose $f : G_1 \to G_2$ is a homomorphism. If $xy = yx$, for some $x, y \in G_1$, then $f(x)f(y) = f(y)f(x)$.

Proof.

$xy = yx \Rightarrow f(xy) = f(yx) \Rightarrow f(x)f(y) = f(y)f(x)$.

Corollary 1.

Suppose $f : G_1 \to G_2$ is a homomorphism that is onto G_2. If G_1 is abelian, then G_2 is abelian.

Lemma 4.

Suppose $f : G_1 \to G_2$ is a homomorphism. If $x \in G_1$ and $o(x)$ is finite, then $o(f(x))$ divides $o(x)$.

Proof.

Let $n = o(x)$. Then, $x^n = e_1$, where e_1 is the identity in G_1. Now, $(f(x))^n = f(x^n) = f(e_1) = e_2$. Hence, $o(f(x))$ divides n and we are done.

Section 6.2 – Isomorphisms.

Definition 2.

(i) Suppose G_1 and G_2 are groups and $f : G_1 \to G_2$ is a homomorphism. Then, f is called a group isomorphism if f is also a bijection. From now on we will call a group isomorphism just an isomorphism.

(ii) If $f : G_1 \to G_2$ is an isomorphism, then we say G_1 and G_2 are isomorphic and we write $G_1 \cong G_2$.

Remark 1.

$G_1 \cong G_2 \Rightarrow |G_1| = |G_2|$.

Remark 2.

If the groups G_1 and G_2 are isomorphic, then even though G_1 and G_2 might look different, G_1 and G_2 are 'essentially' the same group, meaning that they have a similar structure and also share many common properties, (e.g. if G_1 is abelian, then so is G_2, if G_1 has order n, then G_2 has order n etc). Note however that just because two groups A, B have the same order and are both abelian does not mean that A is isomorphic to B.

Lemma 5.

If $f : G_1 \to G_2$ is an isomorphism, then $f^{-1} : G_2 \to G_1$ is also an isomorphism.

Proof:

Note that f^{-1} is a bijection. Now consider $x, y \in G_2$ and let $h = f^{-1}(x), k = f^{-1}(y)$. Then

$$f(hk) = f(h)f(k) = xy$$

$$\Rightarrow f^{-1}(xy) = hk = f^{-1}(x)f^{-1}(y)$$

and so f^{-1} is an isomorphism.

Example 3.

Consider the set T of even integers as a group with the usual addition. Consider the function

$$f : \mathbb{Z} \to T$$

$$x \to 2x$$

Then, f is a bijection and is also a homomorphism because $f(x+y) = 2(x+y) = 2x+2y = f(x) + f(y)$, for all $x, y \in \mathbb{Z}$. So, f is an isomorphism.

MT316A – GROUPS

Fiacre Ó Cairbre

Lecture 13

Example 4.

Consider the homomorphism f in example 1 where

$$f : \mathbb{R} \to \mathbb{R}^+$$

$$x \to e^x$$

f is also a bijection and so f is an isomorphism.

Example 5.

Consider the homomorphism f in example 2 where

$$f : \mathbb{R} \to \mathbb{R} \times \mathbb{R}$$

$$x \to (x, 0)$$

f is not an isomorphism because it is not onto $\mathbb{R} \times \mathbb{R}$

Theorem 1.

(i) If G is a cyclic group with $|G| = n$, then G is isomorphic to $\mathbb{Z}_n$.

(ii) If G is an infinite cyclic group, then G is isomorphic to $\mathbb{Z}$.

Proof.

(i) $G =< x >$, for some $x \in G$. So, $G = \{e, x, x^2, x^3, \ldots, x^{n-1}\}$, where e is the identity in G. As before, $e = x^0$. Now, define

$$f : G \to \mathbb{Z}_n$$

$$x^r \to r, \qquad \text{for} \qquad 0 \leq r \leq n-1$$

Notice that the r on the left hand side of the arrow above is an ordinary integer whereas the r on the right hand side of the arrow above is not an ordinary integer because it's an elment of $\mathbb{Z}_n$.

We will discuss how f is an isomorphism. Firstly, f is actually a function because if $x^r = x^s$, for some r, s with $0 \leq r \leq n-1$ and $0 \leq s \leq n-1$, then $r = s$ in $\mathbb{Z}_n$. The reason for this is because $o(x) = n$. Secondly, f is one–to –one because $r = s$ in $\mathbb{Z}_n \Rightarrow x^r = x^s$.

Thirdly, f is onto $\mathbb{Z}_n$ because if $t \in \mathbb{Z}_n$, then $t = f(x^t)$. Finally, you should check that f is a homomorphism. So, f is an isomorphism and we have that G is isomorphic to $\mathbb{Z}_n$.

(ii) $G =< x >$, for some $x \in G$. So, $G = \{x^k : k \in \mathbb{Z}\}$ Now, define

$$f : G \to \mathbb{Z}$$

$$x^k \to k$$

We will discuss how f is an isomorphism. Firstly, f is actually a function because if $x^u = x^w$, for some $u, w \in \mathbb{Z}$ then $u = w$ in $\mathbb{Z}$. The reason for this is because x has infinite order. Secondly, f is one–to –one because $u = w$ in $\mathbb{Z} \Rightarrow x^u = x^w$.

Thirdly, f is onto $\mathbb{Z}$ because if $t \in \mathbb{Z}$, then $t = f(x^t)$. Finally, f is a homomorphism because $f(x^a x^b) = f(x^{a+b}) = a + b = f(x^a) + f(x^b)$. So, f is an isomorphism and hence G is isomorphic to $\mathbb{Z}$.

Remark 3.

Theorem 1 classifies all cyclic groups, up to isomorphism, in the sense that if we have a cyclic group G of a particular order, then we know a specific group that is isomorphic to G and hence we know a specific group that is essentially the same as G. For example, any cyclic group of order 11 is isomorphic to $\mathbb{Z}_{11}$. This says that even though there may be many different cyclic groups of order 11, they are all essentially the same as $\mathbb{Z}_{11}$.

Remark 4.

If G is a group and $|G| = 2$, then G is cyclic because 2 is prime. Hence, G is isomorphic to $\mathbb{Z}_2$. So, every group of order 2 is isomorphic to $\mathbb{Z}_2$. This means we have classified all groups of order 2, up to isomorphism.

Remark 5.

If G is a group and $|G| = 3$, then G is cyclic because 3 is prime. Hence G is isomorphic to $\mathbb{Z}_3$. In this way, every group of order 3 is isomorphic to $\mathbb{Z}_3$. So, as in remark 4, this means we have classified all groups of order 3, up to isomorphism.

Lemma 6.

Suppose $f : G_1 \to G_2$ is an isomorphism. Then $o(x) = o(f(x))$, for all $x \in G_1$.

Proof:

If $x \in G_1$, then either $o(x)$ is finite or infinite. We divide the proof into two cases.

CASE 1. Suppose $o(x)$ is finite. Lemma 4 says that $o(f(x))$ divides $o(x)$. Apply lemma 4 to the isomorphism $f^{-1} : G_2 \to G_1$ to get that $o(f^{-1}(f(x)))$ divides $o(f(x))$. So, $o(x)$ divides $o(f(x))$ because $f^{-1}(f(x)) = x$.

We have $o(f(x))$ divides $o(x)$ and also $o(x)$ divides $o(f(x))$ and consequently, $o(x) = o(f(x))$.

CASE 2. Suppose $o(x)$ is infinite. Then $o(f(x))$ is also infinite because if $o(f(x))$ is finite, then apply lemma 4 to the isomorphism $f^{-1} : G_2 \to G_1$ to get that $o(f^{-1}(f(x)))$ divides $o(f(x))$ and so $o(x)$ divides $o(f(x))$ which is impossible. Consequently, $o(f(x))$ is infinite and so $o(x) = o(f(x))$.

Remark 6.

Suppose G, H, K are groups. Then

(a) If G is isomorphic to H, then H is isomorphic to G because if $f : G \to H$ is an isomorphism, then $f^{-1} : H \to G$ is an isomorphism, by lemma 5.

(b) If G is isomorphic to H and H is isomorphic to K, then G is isomorphic to K. This is because if $f : G \to H$ is an isomorphism and $w : H \to K$ is an isomorphism, then $w \circ f : G \to K$ is an isomorphism.

Example 6.

All groups of order 17 are isomorphic to each other.

Proof.

Suppose G and H are groups of order 17. By theorem 1, G is isomorphic to $\mathbb{Z}_{17}$ and H is isomorphic to $\mathbb{Z}_{17}$. By remark 6(a), $\mathbb{Z}_{17}$ is isomorphic to H. By remark 6(b), we get that G is isomorphic to H.

Example 7.

$\mathbb{Z}_4$ is not isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ even though both groups are abelian with order 4.

Proof:

$o(1) = 4$ in $\mathbb{Z}_4$ but $\mathbb{Z}_2 \times \mathbb{Z}_2$ has no elements of order 4 because $o(0,0) = 1,\ o(1,0) = 2,\ o(1,1) = 2,\ o(0,1) = 2$. Hence, by Lemma 6, $\mathbb{Z}_4$ is not isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Example 8.

By Corollary 1, S_3 is not isomorphic to $\mathbb{Z}_6$ because S_3 is non–abelian and $\mathbb{Z}_6$ is abelian.

Remark 7.

Examples 7 and 8 illustrate some ways of proving that two groups are not isomorphic. The idea is to show that one group has a certain property (like being abelian for example) and the other group does not have that property.

MT316A – GROUPS

Fiacre Ó Cairbre

Lecture 14

Definition 3.

Suppose $f : G_1 \to G_2$ is a homomorphism. The kernel of f is denoted by $\ker f$ and is defined by

$$\ker(f) = \{x \in G_1 : f(x) = e_2\}$$

The image of f is denoted by $\text{im}(f)$ and is defined by

$$\text{im}(f) = \{f(x) : x \in G_1\}$$

Lemma 7.

If $f : G_1 \to G_2$ is a homomorphism, then $\ker(f)$ is a subgroup of G_1 and $\text{im}(f)$ is a subgroup of G_2.

Theorem 2.

Suppose $f : G_1 \to G_2$ is a homomorphism. Then f is one–to–one $\iff$ $\ker(f) = \{e_1\}$.

Proof.

We will first prove the $\Rightarrow$ part. Suppose $x \in \ker(f)$. Then

$$f(x) = e_2 = f(e_1) \Rightarrow x = e_1$$

We already know that $e_1 \in \ker(f)$ and so we now have that $\ker(f) = \{e_1\}$.

We will now prove the $\Leftarrow$ part. Suppose $f(x) = f(y)$, for some $x, y \in G_1$. Then

$$e_2 = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1})$$

$$\Rightarrow xy^{-1} \in \ker(f)$$

$$\Rightarrow xy^{-1} = e_1$$

$$\Rightarrow x = y$$

Hence, f is one–to–one and we are done.

Theorem 3. Cayley's Theorem

Suppose G is a finite group with $|G| = n$. Then G is isomorphic to a subgroup of S_n.

Remark 8.

Theorem 3 says something a little surprising because it says that every finite group is essentially the same as some subgroup of a permutation group.

Chapter 7 – Conjugacy, Normal Subgroups and Quotient Groups.

Section 7.1 – Conjugacy.

Definition 1.

Suppose G is a group and $x, y \in G$. We say that x is conjugate to y if there exists $h \in G$ such that:

$$x = hyh^{-1}$$

Definition 2.

Suppose G is a group and $x \in G$. The conjugacy class of x is denoted by $[x]$ and is defined as

$$[x] = \{kxk^{-1} : k \in G\}$$

The conjugacy class of x is the set of all elements in G that are conjugate to x.

Example 1.

If e is the identity in a group G, then $[e] = \{e\}$ because $kek^{-1} = e$, for all $k \in G$.

Example 2.

If G is an abelian, then $[x] = \{x\}$. for all $x \in G$ because $kxk^{-1} = kk^{-1}x = x$, for all $k \in G$.

Remark 1.

If x is conjugate to y, then y is conjugate to x because if $x = kyk^{-1}$ for some $k \in G$, then $y = hxh^{-1}$ for $h = k^{-1}$. Also, x is conjugate to itself because $x = exe^{-1}$, where e is the identity in the group.

Notation.

We will now look at S_n because there will be a convenient method for showing when α is conjugate to β in S_n. Suppose $\alpha \in S_n$. Then, the cycle type of α is defined to be

$$\{i_1, i_2, i_3, \ldots, i_m\}$$

where i_1 is the number of elements fixed by α and for $j > 1$, i_j is the number of cycles of length j that appear when you express α as a product of disjoint cycles. Also, m is the length of the longest cycle that appears in this product of disjoint cycles. For example, if

$$\alpha = (341)(26)(79) \quad \text{in} \quad S_9 \qquad (*)$$

then we have α expressed as a product of disjoint cycles and the cycle type of α is $\{2, 2, 1\}$ because there is one cycle of length 3, two cycles of length 2 when you express α as a product of disjoint cycles in $(*)$ and also α fixes two elements. The reason α fixes two elements is because α fixes 5 and 8. The way to work out the number of elements fixed by α is to see that there are seven different numbers in $(*)$ and we are in S_9 and so α fixes $9 - 7 = 2$ numbers (in this case, the numbers 5 and 8).

Theorem 1.

If $\alpha, \beta \in S_n$, then α is conjugate to $\beta \iff \alpha$ and β have the same cycle type.

Example 3.

Suppose $\alpha = (341)(26)(58)$, $\beta = (265)(413)$, $\delta = (12)(364)(95)$ in S_9. Then, the cycle type of α is $\{2, 2, 1\}$, the cycle type of β is $\{3, 0, 2\}$ and the cycle type of δ is $\{2, 2, 1\}$.

By theorem 1, we get that α is conjugate to δ and α is not conjugate to β.

MT316A – GROUPS

Fiacre Ó Cairbre

Lecture 15

Section 7.2 – Normal subgroups.

Definition 3.

Suppose H is a subgroup of G and $x \in G$. Then xHx^{-1} is the subset of G defined as

$$xHx^{-1} = \{xyx^{-1} : y \in H\}$$

Definition 4.

Suppose H_1, H_2 are subgroups of G. Then H_1 and H_2 are said to be conjugate subgroups if there exists an $x \in G$ such that

$$H_2 = xH_1x^{-1}$$

Definition 5.

Suppose H is a subgroup of G. Then H is called a normal subgroup of G if

$$H = xHx^{-1}, \quad \text{for all} \quad x \in G$$

Example 4.

Suppose G is an abelian group and H is a subgroup of G. Then H is a normal subgroup of G.

Proof.

If $x \in G$, then

$$xHx^{-1} = \{xyx^{-1} : y \in H\} = \{xx^{-1}y : y \in H\} = \{y : y \in H\} = H$$

Example 5.

Suppose G is a group and e is the identity in G. Then the trivial group $H = \{e\}$ is a normal subgroup.

Proof.

If $x \in G$, then

$$xHx^{-1} = \{xyx^{-1} : y \in H\} = \{xex^{-1}\} = \{e\} = H$$

Example 6.

Suppose $H =< (12) >$ in S_3. Then, H is a subgroup of S_3 but it is not a normal subgroup of S_3.

Proof:

Let $x = (123)$ in S_3 and $y = (12)$ in H. Then

$$xyx^{-1} = (123)(12)(132) = (32) \notin H$$

Now, $xyx^{-1} \in xHx^{-1}$. Hence $H \neq xHx^{-1}$. So, H is not a normal subgroup of S_3

Remark 2.

Suppose H is a subgroup of G and $x \in G$. Then $xHx^{-1} = H \iff xH = Hx$.

Proof.

Proof of the $\Rightarrow$ part: In this proof, note that $A \subset B$ means that A is a subset of B. Now, suppose $xHx^{-1} = H$. Then if $z \in xH$, we get $zx^{-1} \in xHx^{-1}$ and so $zx^{-1} \in H$. Thus, $z = zx^{-1}x \in Hx$. Hence, $xH \subset Hx$. In a similar way, one can show that $Hx \subset xH$ and hence we have $xH = Hx$.

Proof of the $\Leftarrow$ part. Suppose $xH = Hx$. Then if $w \in xHx^{-1}$, we get that $wx \in xH$ and so $wx \in Hx$. Hence, $w \in H$ and so $xHx^{-1} \subset H$.

Also, if $u \in H$, then $ux \in Hx$ and so $ux \in xH$ which means $u \in xHx^{-1}$. Hence, $H \subset xHx^{-1}$. Hence, $xHx^{-1} = H$ and we are done.

Lemma 1.

Suppose H is a subgroup of G. Then H is a normal subgroup of $G \iff xHx^{-1} \subset H$, for all $x \in G$

Proof.

Proof of the $\Rightarrow$ part. Suppose H is a normal subgroup of G. Then $xHx^{-1} = H$, for all $x \in G$ and so $xHx^{-1} \subset H$, for all $x \in G$.

Proof of the $\Leftarrow$ part. Suppose

$$xHx^{-1} \subset H, \quad \text{for all} \quad x \in G$$

So, if $x \in G$, then $x^{-1} \in G$ and so

$$x^{-1}Hx \subset H \quad \text{because} \quad (x^{-1})^{-1} = x$$

$$\Rightarrow \; x(x^{-1}Hx)x^{-1} \subset xHx^{-1}$$

$$\Rightarrow \ H \subset xHx^{-1}$$

$$\Rightarrow H = xHx^{-1}, \quad \text{for all} \quad x \in G$$

Thus, H is a normal subgroup of G.

Example 7.

A_4 is a normal subgroup of S_4.

Proof.

Suppose $y \in A_4$. Then $xyx^{-1} \in A_4$ for all $x \in S_4$ because if $x \in A_4$, then $xyx^{-1} \in A_4$ since A_4 is a subgroup of S_4 and if $x \notin A_4$, then x is an odd permutation and one can see that $xyx^{-1} \in A_4$.

Theorem 2.

A_n is a normal subgroup of S_n, for $n \geq 2$.

Proof.

The proof is the same as in Example 7. Just replace A_4 by A_n and replace S_4 by S_n.

Example 8.

Suppose $H = \{I, (12)(34)\}$ in A_4 and

$$V = \{I, (12)(34), (13)(24), (14)(23)\} \quad \text{in} \quad A_4$$

where I is the identity permutation in A_4.

We will prove that:

(i) V is a subgroup of A_4 and H is a normal subgroup of V.

(ii) V is a normal subgroup of A_4.

(iii) H is not a normal subgroup of A_4.

MT316A – GROUPS

Fiacre Ó Cairbre

Lecture 16

Proof of example 8.

(i) Note that V is a subgroup of A_4 because V is non–empty and $xy^{-1} \in V$, for all $x, y \in V$. Also, note that H is a subgroup of V because $(12)(34)$ has order 2. We now need to show that $x(12)(34)x^{-1} \in H$, for all $x \in V$. You can check this for the four elements x in V.

(ii) We need to show that $xyx^{-1} \in V$, for all $x \in A_4,\ y \in V$. Note from before that xyx^{-1} is conjugate to y and hence has the same cycle type as y which is $\{0, 2\}$ for $y \neq I$. Now note that the only elements of A_4 that have cycle type $\{0, 2\}$ are the non–identity elements of V. So we have that

$$xyx^{-1} \in V, \quad \text{for all} \quad x \in A_4,\ y \in V$$

and so V is a normal subgroup of A_4.

(iii) Let $x = (123)$ in A_4. Note that $x(12)(34)x^{-1} \in xHx^{-1}$. However,

$$x(12)(34)x^{-1} = (123)(12)(34)(132) = (14)(23) \notin H$$

and so $xHx^{-1} \neq H$ and hence H is not a normal subgroup of A_4.

Example 9.

Suppose G is a group. Then G itself is a normal subgroup of G. Combine this with example 5 to get that a non–trivial group G always has at least two different normal subgroups, namely G and $\{e\}$.

Defintion 6.

A non–trivial group G is called simple if the only normal subgroups of G are $\{e\}$ and G.

Example 10.

Suppose p is a prime number. Then $\mathbb{Z}_p$ is a simple group.

Proof.

$\mathbb{Z}_p$ has order p and so the only subgroups of $\mathbb{Z}_p$ are $\mathbb{Z}_p$ itself and the trivial group $\{0\}$. Hence, the only normal subgroups of $\mathbb{Z}_p$ are $\mathbb{Z}_p$ and $\{0\}$. Thus, $\mathbb{Z}_p$ is a simple group.

Example 11.

S_3 is not a simple group.

Proof.

Use Theorem 2 to get that A_3 is a normal subgroup of S_3. Also, A_3 is a non–trivial subgroup and $A_3 \neq S_3$.

Theorem 3.

A_n is a simple group for all $n \geq 5$.

Remark 3.

A_5 is non–abelian because $(124)(123) \neq (123)(124)$. So, A_5 is a non–abelian simple group of order 60. It turns out that there is no non–abelian simple group with smaller order than 60. It also turns out that if G is a non–abelian simple group of order 60, then G is isomorphic to A_5.

Lemma 2.

Suppose G, H are groups and $f : G \to H$ is a homomorphism. Then $\ker(f)$ is a normal subgroup of G.

Proof.

We know that $\ker(f)$ is a subgroup of G. Suppose $x \in \ker(f)$ and $y \in G$. Then

$$f(yxy^{-1}) = f(y)f(x)f(y^{-1}) \qquad (*)$$

because f is a homomorphism.

Now

$$(*) = f(y)f(y^{-1}), \quad \text{because} \quad x \in \ker(f)$$

$$= f(yy^{-1})$$

$$= f(e_G) = e_H$$

where e_G is the identity in G and e_H is the identity in H.

Thus, $f(yxy^{-1}) = e_H$ and so $yxy^{-1} \in \ker(f)$. So, by Lemma 1, we get that $\ker(f)$ is a normal subgroup of G.

Theorem 4.

Suppose H is a subgroup of G. Then, H is a normal subgroup of $G \iff \dfrac{G}{H}$ is a group under the operation

$$xHyH = xyH, \quad \text{for} \quad xH,\ yH \in \frac{G}{H}$$

$\frac{G}{H}$ is called a quotient group.

Remark 4.

Suppose G is a finite group and H is a normal subgroup of G. Then the order of the quotient group $\frac{G}{H}$ is $\frac{|G|}{|H|}$. As mentioned in lemma 5 in chapter 4, we also denote the order of $\frac{G}{H}$ by $[G : H]$ and it's called the index of H in G.

Example 12.

Suppose $H = \{0, 3\}$ in $\mathbb{Z}_6$. Then H is a normal subgroup of $\mathbb{Z}_6$. The order of the quotient group $\frac{\mathbb{Z}_6}{H}$ is $\frac{|\mathbb{Z}_6|}{|H|} = \frac{6}{2} = 3$

and so $\frac{\mathbb{Z}_6}{H}$ is isomorphic $\mathbb{Z}_3$ by theorem 1 in chapter 6.

MT316A – GROUPS

Fiacre Ó Cairbre

Lecture 17

Remark 5.

One can use quotient groups and other ideas to prove that if G is a group of order p^2, for a prime number p, then G is abelian. So, 6 is the smallest order of a non–abelian group because:

(i) $|G| = 1 \Rightarrow G$ is the trivial group which is abelian.

(ii) $|G| = 2 \Rightarrow G$ is abelian since it's cyclic because 2 is prime.

(iii) $|G| = 3 \Rightarrow G$ is abelian as in (ii).

(iv) $|G| = 4 \Rightarrow G$ is abelian because 4 is the square of the prime number 2.

(v) $|G| = 5 \Rightarrow G$ is abelian as in (ii).

(vi) S_3 is an example of a non–abelian group of order 6.

Lemma 3.

Suppose H is a normal subgroup of G. Then, define

$$q : G \to \frac{G}{H}$$

$$x \to xH$$

Then, q is a homomorphism and is called the quotient map. Also, $\ker(q) = H$.

Proof.

Suppose $x, y \in G$. Then

$$q(xy) = xyH$$

$$= xHyH$$

$$= q(x)q(y)$$

and so q is a homomorphism.

Also, $\ker(q) = \{x \in G : q(x) = H\}$, because H is the identity element in $\dfrac{G}{H}$.

Now,

$$q(x) = H \iff xH = H \iff x \in H$$

and so $\ker(q) = H$.

Lemma 4.

H is a normal subgroup of $G \iff$ there exists a homomorphism with domain G and kernel H.

Proof.

Proof of $\Rightarrow$ part. Use Lemma 3.

Proof of $\Leftarrow$ part. H is the kernel of a homomorphism and so by Lemma 2 we get that H is a normal subgroup of G.

Theorem 5 – First Isomorphism Theorem for Groups.

Suppose $f : G \to H$ is a homomorphism, Then

$$\frac{G}{\ker(f)} \quad \text{is isomorphic to} \quad im(f)$$

Note that $\dfrac{G}{\ker(f)}$ is a quotient group.

Example 13.

Suppose G is a group with order 24 and $f : G \to \mathbb{Z}_5$ is a homomorphism. Prove that $f(x) = f(y)$, for all $x, y \in G$.

Proof.

Theorem 5 says that

$$\frac{G}{\ker(f)} \quad \text{is isomorphic to} \quad im(f), \qquad \text{which is a subgroup of} \quad \mathbb{Z}_5$$

So, $|im(f)| = 1$ or $|im(f)| = 5$. If $|im(f)| = 5$, then

$$\frac{G}{\ker(f)} \quad \text{has order} \quad 5$$

which is impossible because 5 does not divide $|G|$.

So, we must have $|im(f)| = 1$ and hence $f(x) = f(y)$, for all $x, y \in G$.

Chapter 8 – Finitely Generated Abelian Groups.

Lemma 1.

$\mathbb{Z}_{mn}$ is isomorphic to $\mathbb{Z}_m \times \mathbb{Z}_n \iff m$ and n have no common prime divisors (i.e. m and n are coprime).

Proof.

Proof of $\Rightarrow$ part.

$\mathbb{Z}_{mn}$ is cyclic and so $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic too. Hence,

$$\mathbb{Z}_m \times \mathbb{Z}_n =< (a,b) >, \quad \text{for some} \quad a \in \mathbb{Z}_m,\ b \in \mathbb{Z}_n$$

We will prove m and n are coprime by contradiction. So, suppose m and n are not coprime. Then, there exists $r > 1$ such that r divides n and r divides m. So,

$$m = kr \quad \text{and} \quad n = lr, \quad \text{for some} \quad l, k \in \mathbb{N}$$

Now, $o(a,b) = mn = klr^2$ and so

$$klr^2(a,b) \text{ is the smallest positive multiple of } (a,b) \text{ that equals } (0,0) \text{ in } \mathbb{Z}_m \times \mathbb{Z}_n \qquad (*)$$

However,

$$kra = ma = 0 \quad \text{in} \quad \mathbb{Z}_m \quad \text{and} \quad lrb = nb = 0 \quad \text{in} \quad \mathbb{Z}_n$$

$$\Rightarrow klra = 0 \quad \text{in} \quad \mathbb{Z}_m \quad \text{and} \quad klrb = 0 \quad \text{in} \quad \mathbb{Z}_n$$

$$\Rightarrow klr(a,b) = (0,0) \quad \text{in} \quad \mathbb{Z}_m \times \mathbb{Z}_n$$

.

which is impossible because of $(*)$ and the fact that $klr < klr^2$. So, m and n are coprime.

Proof of $\Leftarrow$ part.

Consider $(1,1) \in \mathbb{Z}_m \times \mathbb{Z}_n$. We will now show that $o(1,1) = mn$ by proving (by contradiction) that mn is the least positive integer such that $mn(1,1) = (0,0) \quad \text{in} \quad \mathbb{Z}_m \times \mathbb{Z}_n$.

MT316A – GROUPS

Fiacre Ó Cairbre

Lecture 18

Continuation of the proof of Lemma 1.

Suppose $r(1,1) = (0,0)$, for some r with $0 < r < mn$. Then,

$$r = 0 \quad \text{in} \quad \mathbb{Z}_m \quad \text{and} \quad r = 0 \quad \text{in} \quad \mathbb{Z}_n$$

and so

$$m \ \text{divides} \ r \quad \text{and} \quad n \quad \text{divides} \quad r$$

Hence,

$$mn \quad \text{divides} \quad r \quad \text{because} \quad m \quad \text{and} \quad n \quad \text{are coprime}$$

This is impossible because $0 < r < mn$. Now

$$mn(1,1) = (0,0) \quad \text{in} \quad \mathbb{Z}_m \times \mathbb{Z}_n$$

and hence $o(1,1) = mn$. So,

$$\mathbb{Z}_m \times \mathbb{Z}_n =< (1,1) >$$

and so $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic with order mn. Hence,

$$\mathbb{Z}_m \times \mathbb{Z}_n \quad \text{is isomorphic to} \quad \mathbb{Z}_{mn}$$

Notation

The notation $G \ncong H$ means that the group G is not isomorphic to the group H.

Example 1.

(i) $\mathbb{Z}_4 \times \mathbb{Z}_5 \cong \mathbb{Z}_{20}$ because 4 and 5 are coprime.

(ii) $\mathbb{Z}_4 \times \mathbb{Z}_6 \ncong \mathbb{Z}_{24}$ because 4 and 6 are not coprime.

Definition 1.

Suppose G_i is a group for $1 \leq i \leq n$. The product group $G_1 \times G_2 \times \cdots \times G_n$ is defined by

$$G_1 \times G_2 \times \cdots \times G_n = \{(x_1, x_2, \ldots, x_n) : x_i \in G_i\}$$

where the group operation on $G_1 \times G_2 \times \cdots \times G_n$ is defined by

$$(x_1, x_2, \ldots, x_n)(y_1, y_2, \ldots, y_n) = (x_1 y_1, x_2 y_2, \ldots, x_n y_n), \quad \text{for all} \quad x_i, y_i \in G_i$$

Lemma 2.

Suppose G_i is a group for $1 \leq i \leq n$. Then

$$|G_1 \times G_2 \times \cdots \times G_n| = |G_1||G_2| \ldots |G_n|$$

This says that the order of the product group is the product of orders of the groups.

If any of the groups G_i has infinite order, then $G_1 \times G_2 \times \cdots \times G_n$ has infinite order.

Example 2.

$$|\mathbb{Z}_3 \times S_3 \times A_3| = 54$$

Theorem 1 – Fundamental Theorem for finite abelian groups – Version 1

Every finite abelian group is isomorphic to a product of cyclic groups. In particular, if G is a finite abelian group, then G is isomorphic to a group of the form

$$\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}} \qquad (*)$$

where the p_i are primes (which are not necessarily different) and $\alpha_i \in \mathbb{N}$ for $1 \leq i \leq k$. Also, $|G| = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Note that $\mathbb{Z}_{p_i^{\alpha_i}}$ in $(*)$ above is the group $\mathbb{Z}_q$ where q is the number $p_i^{\alpha_i}$.

The order in which the cyclic groups $\mathbb{Z}_{p_i^{\alpha_i}}$ appear in $(*)$ above doesn't matter because $\mathbb{Z}_r \times \mathbb{Z}_t \cong \mathbb{Z}_t \times \mathbb{Z}_r$, for all $r, t \in \mathbb{N}$. Furthermore, it turns out that (apart from changing tho order in which the groups in $(*)$ appear) no two different groups of the form $(*)$ are isomorphic to each other.

Example 3.

How many different groups are there of order 4, up to isomorphism? I will explain what the expression 'up to isomorphism' means, as we work out the solution.

Solution.

Suppose G is a group with order 4. Remark 5 in chapter 7 says that G is abelian. Now theorem 1 says that

$$G \cong \mathbb{Z}_{2^2} \quad \text{or} \quad G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \qquad (**)$$

because 4 can only be written in two different ways as a product of powers of primes (where the primes are not necessarily different), i.e.

$$4 = 2^2 \quad \text{and} \quad 4 = 2 \times 2$$

$(**)$ above says that

$$G \cong \mathbb{Z}_4 \quad \text{or} \quad G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

Note that lemma 1 says that

$$\mathbb{Z}_4 \ncong \mathbb{Z}_2 \times \mathbb{Z}_2$$

Hence, there are two different groups of order 4, up to isomorphism, and they are

$$\mathbb{Z}_4, \qquad \mathbb{Z}_2 \times \mathbb{Z}_2$$

This means that if G is any group of order 4, then either $G \cong \mathbb{Z}_4$ or $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ and furthermore $\mathbb{Z}_4 \ncong \mathbb{Z}_2 \times \mathbb{Z}_2$. This explains what it means to say there are two different groups of order 4, up to isomorphism.

Remark 1.

Continuing on from the last paragraph in the solution in example 3, if there are k different groups of order n, up to isomorphism, this means there are k different groups $H_1, H_2, \ldots, H_k$ of order n (no pair of which are isomorphic to each other) such that given any group G of order n, then G has to be isomorphic to exactly one of the H_i.

Remark 2.

Example 3 classifies all groups of order 4 in the sense that we now know what every group of order 4 looks like, up to isomorphism. We can now say that every group of order 4 is either isomorphic to $\mathbb{Z}_4$ or is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Example 4.

How many different abelian groups are there of order 16, up to isomorphism?

Solution.

Suppose G is an abelian group of order 16. Before we use theorem 1, we look at how many different ways we can write 16 as a product of powers of primes (where the primes are not necessarily different) and the order in which the primes appear doesn't matter. Well there are five different ways and they are

$$16 = 2^4, \quad 16 = 2 \times 2^3, \quad 16 = 2^2 \times 2^2, \quad 16 = 2 \times 2 \times 2^2, \quad 16 = 2 \times 2 \times 2 \times 2 \qquad (***)$$

Theorem 1 now says that G is isomorphic to exactly one of the following five groups

$$\mathbb{Z}_{2^4}, \quad \mathbb{Z}_2 \times \mathbb{Z}_{2^3}, \quad \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2}, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{2^2}, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \qquad (****)$$

MT316A – GROUPS

Fiacre Ó Cairbre

Lecture 19

Continuation of example 4.

and so G is isomorphic to exactly one of the following five groups

$$\mathbb{Z}_{16}, \quad \mathbb{Z}_2 \times \mathbb{Z}_8, \quad \mathbb{Z}_4 \times \mathbb{Z}_4, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

So, the answer to the original question is that there are five different abelian groups of order 16, up to isomorphism.

Notice that theorem 1 also says that no two of the groups in $(**)$ are isomorphic to each other.

Remark 3.

The fact that there are five different ways in $(***)$ in example 4 of writing $16 = 2^4$ as a product of powers of primes (where the primes are not necessarily different and the order in which the primes appear doesn't matter) is the same as saying there are five different ways of writing 4 (the power of 2 in $16 = 2^4$) as a sum of positive integers (where the order of the integers doesn't matter). The five different expressions in $(***)$ in example 4 correspond to the following five different ways of writing 4 as a sum of positive integers:

$$4 = 4 \quad \text{corresponds to} \quad 16 = 2^4$$

$$4 = 1 + 3 \quad \text{corresponds to} \quad 16 = 2 \times 2^3$$

$$4 = 2 + 2 \quad \text{corresponds to} \quad 16 = 2^2 \times 2^2$$

$$4 = 1 + 1 + 2 \quad \text{corresponds to} \quad 16 = 2 \times 2 \times 2^2$$

$$4 = 1 + 1 + 1 + 1 \quad \text{corresponds to} \quad 16 = 2 \times 2 \times 2 \times 2$$

This will motivate definitions 2 and 3 below.

Definition 2.

Suppose $m \in \mathbb{N}$. Suppose $c_1, c_2, \ldots, c_k$ are positive integers with $c_1 \leq c_2 \leq \ldots \leq c_k$ and

$$m = c_1 + c_2 + \cdots + c_k$$

Then, we say that $\{c_1, c_2, \ldots, c_k\}$ forms a partition of m.

Example 5.

In remark 3 above we see that $\{1, 3\}$ forms a partition of 4 because $1 \leq 3$ and $4 = 1 + 3$. Similarly, $\{1, 1, 2\}$ forms a partition of 4 because $1 \leq 1 \leq 2$ and $4 = 1 + 1 + 2$. In this way, remark 3 shows that there are five different partitions of 4.

Definition 3.

Suppose $m \in \mathbb{N}$. The number of different partitions of m is denoted by $p(m)$ and is called the partition function of m.

Theorem 2.

Suppose $m \in \mathbb{N}$ and

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$$

where the p_i are different primes and $\alpha_i \in \mathbb{N}$, for $1 \leq i \leq r$. The number of different abelian groups of order m, up to isomorphism, is equal to

$$p(\alpha_1)p(\alpha_2)\ldots p(\alpha_r)$$

where $p(\alpha_i)$ is the partition function of α_i, for $1 \leq i \leq r$.

Remark 4.

You could try to show that $p(7) = 15$. I won't ask you to confirm that $p(10) = 42$. The values of the partition function get large very quickly. For example, $p(22) = 1002$ and $p(100) = 190,569,292$. There is no known formula for the partition function. If you find one, then let me know!

In the early 1900s, the remarkable Indian mathematician, Srinivasa Ramanujan, proved some interesting results about the partition function. For example, he proved that if the last digit of m is 4 or 9, then $p(m)$ will be divisible by 5. There was a movie made in 2015 about Ramanujan's life. The movie is called 'The man who knew infinity'.

Remark 5.

Theorem 2 says, surprisingly, that the number of different abelian groups of order m, up to isomorphism, does not depend on the primes p_i. The number of different abelian groups of order m, up to isomorphism, only depends on the powers α_i of the primes p_i.

Example 6.

(i) How different abelian groups are there of order 125, up to isomorphism?

(ii) How many different abelian groups are there of order 343, up to isomorphism?

Solution.

(i) $125 = 5^3$ and so, by theorem 2, the number of different abelian groups of order 125, up to isomorphism, is equal to $p(3) = 3$.

(ii) $343 = 7^3$ and so the number of different abelian groups of order 343, up to isomorphism, is equal to $p(3) = 3$.

Remark 6.

In example 6(i) we showed that there are three different abelian groups of order 125, up to isomorphism. If we wanted to write down three different abelian groups of order 125, up to isomorphism, then we can use theorem 1 to get

$$\mathbb{Z}_{125} \quad \text{from} \quad 125 = 5^3$$

$$\mathbb{Z}_5 \times \mathbb{Z}_{25} \quad \text{from} \quad 125 = 5 \times 5^2$$

$$\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \quad \text{from} \quad 125 = 5 \times 5 \times 5$$

Example 7.

How many different abelian groups are there of order 720, up to isomorphism?

Solution.

$720 = 2^4 3^2 5$ and so the number of different abelian groups of order 720, up to isomorphism, is equal to $p(4)p(2)p(1) = 10$.

Example 8.

(i) Prove that there are three different abelian groups of order 40, up to isomorphism?

(ii) If G is an abelian group of order 40, then how do you determine which of the three groups G is isomorphic to?

Solution.

(i) $40 = 2^3 5$ and so the number of different abelian groups of order 40, up to isomorphism, is equal to $p(3)p(1) = 3$.

(ii) Use theorem 1 to get the following three different abelian groups of order 40, up to isomorphism.

$$\mathbb{Z}_8 \times \mathbb{Z}_5 \quad \text{from} \quad 40 = 2^3 \times 5$$

$$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \quad \text{from} \quad 40 = 2 \times 2^2 \times 5$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \quad \text{from} \quad 40 = 2 \times 2 \times 2 \times 5$$

No pair from these three groups are isomorphic to each other. Now, suppose G is an abelian group of order 40. We know that G is isomorphic to exactly one of the three groups above. How do we determine which of the three groups G is isomorphic to?

It can be useful to look at the orders of elements. If two groups are isomorphic, then given any positive integer n, the two groups have exactly the same number of elements of order n.

MT316A – GROUPS

Fiacre Ó Cairbre

Lecture 20

Continuation of example 8.

Note that only one of the three groups above has an element of order 40 because if a group of order 40 has an element of order 40, then the group is cyclic and we know that there is only one cyclic group of order 40, up to isomorphism. The only one of the three groups above that has an element of order 40 is

$$\mathbb{Z}_8 \times \mathbb{Z}_5$$

because

$$\mathbb{Z}_8 \times \mathbb{Z}_5 \cong \mathbb{Z}_{40} \qquad \text{which is cyclic of order 40}$$

So, if G has an element of order 40, then $G \cong \mathbb{Z}_8 \times \mathbb{Z}_5$

Now, if G doesn't have an element of order 40, then either

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5$$

or

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$$

Now, $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5$ has exactly three elements of order 2 and they are the elements

$$(1,0,0), \qquad (0,2,0), \qquad (1,2,0)$$

Also, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$ has more than three elements of order 2.

So, overall we have the following:

(a) If G has an element of order 40, then

$$G \cong \mathbb{Z}_8 \times \mathbb{Z}_5$$

(b) If G has no element of order 40 and has exactly three elements of order 2, then

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5$$

(c) If G has no element of order 40 and doesn't have exactly three elements of order 2, then

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$$

Definition 4.

A finitely generated group is a group that is generated by a finite set of elements.

Example 9.

(i) Every cyclic group G is a finitely generated group because a cyclic group is generated by a set consisting of one element.

(ii) Every finite group G is a finitely generated group because G is generated by the set G itself.

(iii) $\mathbb{Z}$ is an infinite group that is a finitely generated group because $\mathbb{Z}$ is cyclic from before.

Example 10.

$\mathbb{Z} \times \mathbb{Z}$ is a finitely generated group.

Proof.

We will show that $\mathbb{Z} \times \mathbb{Z} =< (1,0), (0,1) >$

Well, if $(a,b) \in \mathbb{Z} \times \mathbb{Z}$, then

$$(a,b) = a(1,0) + b(0,1)$$

and so we see why

$$\mathbb{Z} \times \mathbb{Z} =< (1,0), (0,1) >$$

So, $\mathbb{Z} \times \mathbb{Z}$ is an example of an infinite group that is not cyclic but is finitely generated.

Example 11.

Consider the group

$$\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

where we take the product group of $\mathbb{Z}$ with itself finitely many times. In a similar way to example 10, one can show that

$$\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

is a finitely generated group. For example,

$$\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} =< (1,0,0), (0,1,0), (0,0,1) >$$

Example 12.

Consider the set of rational numbers $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z},\ b \neq 0\}$ which is group under ordinary addition. We will prove that $\mathbb{Q}$ is not a finitely generated group.

Proof by contradiction.

Suppose $\mathbb{Q}$ is a finitely generated group. So, there is a finite set C of rational numbers such that $\mathbb{Q}$ is generated by C.

Suppose

$$C = \{\frac{a_1}{b_1}, \frac{a_2}{b_2}, \ldots, \frac{a_n}{b_n}\}$$

Every element in $< C >$ is an integer multiple of $\frac{1}{h}$ where h is the least common multiple of $b_1, b_2, \ldots, b_n$. To see this, consider any element $x \in < C >$. Then,

$$x = \sum_{i=1}^{n} k_i \frac{a_i}{b_i}, \quad \text{for some} \quad k_i \in \mathbb{Z},\ 1 \leq i \leq n$$

$$= \sum_{i=1}^{n} \frac{k_i a_i}{b_i}$$

$$= \frac{w}{h}, \quad \text{for some} \quad w \in \mathbb{Z}$$

So, every element in $\mathbb{Q}$ is an integer multiple of $\frac{1}{h}$ but this is impossible because $\frac{1}{h+1}$ is not an integer multiple of $\frac{1}{h}$.

We have a contradiction and hence $\mathbb{Q}$ is not finitely generated.

Notation.

We denote

$$\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z} \qquad (*)$$

by $\mathbb{Z}^t$ if $(*)$ is the product group of $\mathbb{Z}$ with itself t times, where $t \in \mathbb{N}$.

We also denote the trivial group by $\mathbb{Z}^0$.

MT316A – GROUPS

Fiacre Ó Cairbre

Lecture 21

Remark 7.

From example 9 we see that every finite abelian group is a finitely generated abelian group. The following theorem will generalise theorem 1.

Theorem 3 – Fundamental Theorem for finitely generated abelian groups.

If G is a finitely generated abelian group, then G is isomorphic to a group of the form

$$\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}} \times \mathbb{Z}^t \qquad (*)$$

where $t \in \mathbb{N} \cup \{0\}$ and the p_i are primes (which are not necessarily different) and $\alpha_i \in \mathbb{N}$ for $1 \leq i \leq k$.

Remark 8.

If G is a finite abelian group in theorem 3, then we get $t = 0$ and we have theorem 1. If G is an infinite abelian group that is finitely generated in theorem 3, then $t > 0$.

Chapter 9 – More on Matrix Groups.

Section 9.1 – Linear Transformations.

Definition 1.

Define

$$\mathbb{R}^n = \{(x_1, x_2, \ldots, x_n) : x_i \in \mathbb{R}\} \quad \text{for} \quad n \in \mathbb{N}$$

Addition on $\mathbb{R}^n$ is defined by

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$$

Scalar multiplication is defined by

$$k(x_1, x_2, \ldots, x_n) = (kx_1, kx_2, \ldots, kx_n), \qquad \text{for} \quad k \in \mathbb{R}$$

Definition 2.

The function $f : \mathbb{R}^n \to \mathbb{R}^n$ is called a linear transformation if

$$f(k\underline{u} + h\underline{w}) = kf(\underline{u}) + hf(\underline{w}), \qquad \text{for all} \quad \underline{u}, \underline{w} \in \mathbb{R}^n, \quad k, h \in \mathbb{R}$$

Example 1.

Suppose M_n is the set of $n \times n$ matrices with real entries. Suppose $A \in M_n$. Now consider $\underline{u} = (u_1, u_2, \ldots, u_n) \in \mathbb{R}^n$ as a column vector which means we consider $\underline{u}$ as

$$\underline{u} = \begin{pmatrix} u_1 \\ u_2 \\ . \\ . \\ u_n \end{pmatrix}$$

In this way $\underline{u}$ can be considered as an $n \times 1$ matrix so that we can perform the matrix multiplication $A\underline{u}$ which will produce an $n \times 1$ matrix which can be considered as an element of $\mathbb{R}^n$ as above.

Now define

$$f : \mathbb{R}^n \to \mathbb{R}^n$$

$$\underline{u} \to A\underline{u}$$

One can show that f is a linear transformation.

Definition 3.

Suppose $\underline{u} = (u_1, u_2, \ldots, u_n) \in \mathbb{R}^n$ and $\underline{w} = (w_1, w_2, \ldots, w_n) \in \mathbb{R}^n$

Then we define

$$\underline{u}.\underline{w} = u_1w_1 + u_2w_2 + \cdots u_nw_n$$

and this is called the dot (or scalar) product of $\underline{u}$ and $\underline{w}$.

Also, we define

$$||\underline{u}|| = \sqrt{u_1^2 + u_2^2 + \cdots + u_n^2}$$

and this is called the length of $\underline{u}$.

Example 2.

Suppose $\underline{u} = (0, 1, 3, -2)$ and $\underline{w} = (-2, 0, 3, 2)$ in $\mathbb{R}^4$, then

$$\underline{u}.\underline{w} = 5$$

$$||\underline{u}|| = \sqrt{14} \quad \text{and} \quad ||\underline{w}|| = \sqrt{17}$$

Example 3.

Suppose $A = \begin{pmatrix} 2 & -1 \\ 3 & 2 \end{pmatrix}$ in example 1. Find the corresponding function, f, and show that f is a linear transformation.

Solution.

We have that

$$f : \mathbb{R}^2 \to \mathbb{R}^2$$

$$\underline{u} \to A\underline{u}$$

and so

$$f(u_1, u_2) = \begin{pmatrix} 2 & -1 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \end{pmatrix} \quad \text{where} \quad \underline{u} = (u_1, u_2)$$

$$= \begin{pmatrix} 2u_1 - u_2 \\ 3u_1 + 2u_2 \end{pmatrix}$$

So, we can consider f as the following function

$$f : \mathbb{R}^2 \to \mathbb{R}^2$$

$$(u_1, u_2) \to (2u_1 - u_2, 3u_1 + 2u_2)$$

Now, to prove that f is a linear transformation we need to show that

$$f(k\underline{u} + h\underline{w}) = kf(\underline{u}) + hf(\underline{w}), \qquad \text{where} \quad \underline{u}, \underline{w} \in \mathbb{R}^2, \quad k, h \in \mathbb{R}$$

So, let $\underline{u} = (u_1, u_2)$ and $\underline{w} = (w_1, w_2)$ and we have

$$f(k\underline{u} + h\underline{w}) = f(k(u_1, u_2) + h(w_1, w_2))$$

$$= f(ku_1 + hw_1, ku_2 + hw_2)$$

$$= (2(ku_1 + hw_1) - (ku_2 + hw_2), 3(ku_1 + hw_1) + 2(ku_2 + hw_2))$$

$$= k(2u_1 - u_2, 3u_1 + 2u_2) + h(2w_1 - w_2, 3w_1 + 2w_2)$$

$$= kf(u_1, u_2) + hf(w_1, w_2)$$

$$= kf(\underline{u}) + hf(\underline{w})$$

and so we are done.

Remark 1.

We can generalise the proof from example 3 to show that

$$f : \mathbb{R}^n \to \mathbb{R}^n$$

$$\underline{u} \to A\underline{u}$$

is a linear transformation where A is any $n \times n$ matrix, as follows:

$$f(k\underline{u} + h\underline{w}) = A(k\underline{u} + h\underline{w})$$

$$= A(k\underline{u}) + A(h\underline{w})$$

$$= k(A\underline{u}) + h(A\underline{w})$$

$$= k(f(\underline{u})) + h(f(\underline{w}))$$

and we are done.

MT316A – GROUPS

Fiacre Ó Cairbre

Lecture 22

Remark 2.

Recall from section 5.1 that the orthogonal group $O(n)$ was given by

$$O(n) = \{A \in M_n : AA^T = I_n\}$$

We will now look at some geometry related to the linear transformations corresponding to the matrices in $O(n)$.

Theorem 1.

$A \in O(n) \iff (A\underline{u}).(A\underline{w}) = \underline{u}.\underline{w}, \quad \text{for all} \quad \underline{u}, \underline{w} \in \mathbb{R}^n.$

Proof.

Proof of the $\Rightarrow$ part.

We first note that we can express $\underline{u}, \underline{w} \in \mathbb{R}^n$ as column vectors

$$\underline{u} = \begin{pmatrix} u_1 \\ u_2 \\ . \\ . \\ u_n \end{pmatrix} \qquad \underline{w} = \begin{pmatrix} w_1 \\ w_2 \\ . \\ . \\ w_n \end{pmatrix}$$

So, in this way we can consider $\underline{u}$ and $\underline{w}$ as $n \times 1$ matrices as well as vectors in $\mathbb{R}^n$. Then we have that

$$\underline{u}.\underline{w} = \underline{u}^T\underline{w} \qquad (*)$$

because the left hand side of $(*)$ is $u_1w_1 + u_2w_2 + \cdots u_nw_n$ and the right hand side of $(*)$ involves the matrix multiplication

$$\underline{u}^T\underline{w} = (u_1u_2 \ldots u_n) \begin{pmatrix} w_1 \\ w_2 \\ . \\ . \\ w_n \end{pmatrix} = u_1w_1 + u_2w_2 + \cdots u_nw_n$$

Now, we have that $A^{-1} = A^T$ because $AA^T = I_n$ and so

$$(A\underline{u}).(A\underline{w}) = (A\underline{u})^T A\underline{w}$$

$$= \underline{u}^T A^T A\underline{w} \quad \text{because} \quad (A\underline{u})^T = \underline{u}^T A^T$$

$$= \underline{u}^T I_n \underline{w}$$

$$= \underline{u}^T \underline{w}$$

$$\underline{u}.\underline{w}$$

Proof of the $\Leftarrow$ part.

First one can show that if $\underline{a}.\underline{b} = 0 \quad$ for all $\quad \underline{a} \in \mathbb{R}^n$, then $\underline{b} = (0, 0, \ldots, 0)$. One way to see this is to note that if $\underline{e_i}$ is the vector with 1 in the i^{th} component and zero in all the other components, then

$$\underline{e_i}.\underline{b} = 0, \quad \text{for} \quad 1 \leq i \leq n$$

and so $b = (0, 0, \ldots, 0)$

Now, for all $\underline{u}, \underline{w} \in \mathbb{R}^n$, we have

$$\underline{u}.\underline{w} = (A\underline{u}).(A\underline{w})$$

$$= (A\underline{u})^T (A\underline{w})$$

$$= \underline{u}^T A^T A\underline{w}$$

$$= \underline{u}.A^T A\underline{w}$$

$$\Rightarrow \underline{u}.(\underline{w} - A^T A\underline{w}) = 0$$

$$\Rightarrow \underline{w} - A^T A\underline{w} = 0$$

$$\Rightarrow A^T A\underline{w} = \underline{w}$$

$$\Rightarrow A^T A = I_n \quad \text{by letting} \quad \underline{w} = \underline{e_i} \quad \text{for} \quad 1 \leq i \leq n$$

$$\Rightarrow A \in O(n)$$

and we are done.

Theorem 2.

$A \in O(n) \iff ||A(\underline{u})|| = ||\underline{u}|| \quad \text{for all} \quad \underline{u} \in \mathbb{R}^n$

Proof.

Proof of the $\Rightarrow$ part.

First note that

$$\underline{w}.\underline{w} = ||\underline{w}||^2, \quad \text{for all} \quad \underline{w} \in \mathbb{R}^n$$

Next we have, for all $\underline{u} \in \mathbb{R}^n$,

$$||A(\underline{u})||^2 = A(\underline{u}).A(\underline{u})$$

$$= \underline{u}.\underline{u} \quad \text{from theorem 1}$$

$$= ||\underline{u}||^2$$

$$\Rightarrow ||A(\underline{u})||^2 = ||\underline{u}||^2$$

$$\Rightarrow ||A(\underline{u})|| = ||\underline{u}||$$

and we are done.

Proof of the $\Leftarrow$ part.

First note that we have

$$||A(\underline{u} + \underline{w})|| = ||\underline{u} + \underline{w}||, \quad \text{for all} \quad \underline{u}, \underline{w} \in \mathbb{R}^n$$

and so for all $\underline{u}, \underline{w} \in \mathbb{R}^n$

$$||A(\underline{u} + \underline{w})||^2 = ||\underline{u} + \underline{w}||^2$$

$$\Rightarrow A(\underline{u} + \underline{w}).A(\underline{u} + \underline{w}) = (\underline{u} + \underline{w}).(\underline{u} + \underline{w}),$$

MT316A – GROUPS

Fiacre Ó Cairbre

Lecture 23

Proof of the $\Leftarrow$ part in theorem 2.

First note that we have

$$||A(\underline{u}+\underline{w})|| = ||\underline{u}+\underline{w}||, \quad \text{for all} \quad \underline{u},\underline{w} \in \mathbb{R}^n$$

and so for all $\underline{u},\underline{w} \in \mathbb{R}^n$

$$||A(\underline{u}+\underline{w})||^2 = ||\underline{u}+\underline{w}||^2$$

$$\Rightarrow A(\underline{u}+\underline{w}).A(\underline{u}+\underline{w}) = (\underline{u}+\underline{w}).(\underline{u}+\underline{w}),$$

$$\Rightarrow A(\underline{u}).A(\underline{u}) + A(\underline{u}).A(\underline{w}) + A(\underline{w}).A(\underline{u}) + A(\underline{w}).A(\underline{w}) = \underline{u}.\underline{u} + \underline{u}.\underline{w} + \underline{w}.\underline{u} + \underline{w}.\underline{w}$$

$$\Rightarrow ||A(\underline{u})||^2 + 2A(\underline{u}).A(\underline{w}) + ||A(\underline{w})||^2 = ||\underline{u}||^2 + 2\underline{u}.\underline{w} + ||\underline{w}||^2$$

$$\Rightarrow 2A(\underline{u}).A(\underline{w}) = 2\underline{u}.\underline{w}$$

$$\Rightarrow A(\underline{u}).A(\underline{w}) = \underline{u}.\underline{w}$$

$$\Rightarrow A \in O(n) \quad \text{from theorem 1}$$

and we are done.

Remark 3.

The distance between two points $\underline{u},\underline{w} \in \mathbb{R}^n$ is $||\underline{u}-\underline{w}||$. We will now see that linear transformations corresponding to the matrices in $O(n)$ will preserve the distance between points in $\mathbb{R}^n$, i.e. we will show that

$$A \in O(n) \Rightarrow ||A(\underline{u}) - A(\underline{w})|| = ||\underline{u}-\underline{w}||, \quad \text{for all} \quad \underline{u},\underline{w} \in \mathbb{R}^n \qquad (*)$$

Proof of $(*)$

$$||A(\underline{u}) - A(\underline{w})|| = ||A(\underline{u} - \underline{w})||$$

$$= ||\underline{u} - \underline{w}||$$

and so we have proved $(*)$.

Remark 4.

A function from $\mathbb{R}^n$ to $\mathbb{R}^n$ that preserves distance, is called a Euclidean isometry. The previous remark shows that the linear transformations corresponding to the matrices in $O(n)$ are Euclidean isometries.

Remark 5.

If $\underline{u}, \underline{w}$ are two non–zero vectors in $\mathbb{R}^n$, then one can define the angle $\theta \in [0, \pi]$ between $\underline{u}$ and $\underline{w}$ and also one can show that

$$\cos\theta = \frac{\underline{u}.\underline{w}}{||\underline{u}||||\underline{w}||} \qquad (*)$$

This angle will correspond to our usual notion of angle between vectors in $\mathbb{R}^2$ and $\mathbb{R}^3$. We say $\underline{u}$ and $\underline{w}$ are perpendicular (or orthogonal) if the angle between them is $\frac{\pi}{2}$. One can then show that $\underline{u}$ and $\underline{w}$ are perpendicular $\iff \underline{u}.\underline{w} = 0$.

Remark 6.

Theorems 1 and 2 and $(*)$ in remark 5 show that linear transformations corresponding to the matrices in $O(n)$ preserve angles between vectors in $\mathbb{R}^n$, i.e. for all $A \in O(n)$, if θ is the angle between $\underline{u}$ and $\underline{w}$, then θ is also the angle between $A(\underline{u})$ and $A(\underline{w})$.

Renark 7.

Here is a proof of remark 6:

Proof.

We need to show that if θ is the angle between any two non–zero vectors $\underline{u}, \underline{w}$ in $\mathbb{R}^n$ and if α is the angle between $A\underline{u}$ and $A\underline{w}$, then $\theta = \alpha$.

Now, $(*)$ in remark 5 implies that

$$\cos\theta = \frac{\underline{u}.\underline{w}}{||\underline{u}||||\underline{w}||}$$

$$= \frac{A\underline{u}.A\underline{w}}{||\underline{u}||||\underline{w}||} \qquad \text{by theorem 1}$$

$$= \frac{A\underline{u}.A\underline{w}}{||A\underline{u}||||A\underline{w}||} \qquad \text{by theorem 2}$$

$$= \cos\alpha \qquad \text{by } (*) \text{ in remark 5}$$

Hence $\theta = \alpha$ because $\theta, \alpha \in [0, \pi]$ and we are done

Remark 8.

The reason $O(n)$ is called the orthogonal group is because linear transformations corresponding to the matrices in $O(n)$ take orthogonal vectors to orthogonal vectors, i.e

$$\underline{u}.\underline{w} = 0 \Rightarrow A(\underline{u}).A(\underline{w}) = 0 \qquad (**)$$

Note that $(**)$ is true from theorem 1.

DEPARTMENT OF MATHEMATICS & STATISTICS

MT316A

Homework 3

Due by 4 p.m. on November 11, 2022.

1. In each case below, state whether the statement is true or false. Justify your answer in each case.

(i) Every group of order 31 is abelian.

(ii) S_6 has an element α with $o(\alpha) = 720$.

(iii) There is an element x in an infinite non–abelian group with $o(x) = 2$.

2. Give an example of a non–abelian group with order 36. Justify your answer.

3. Suppose that H is a subgroup of a group G and suppose $x, y \in G$. Prove that either $xH = yH$ or $xH \cap yH = \phi$.

4. Suppose K_1 and K_2 are subgroups of a group G with $|K_1| = 8$ and $|K_2| = 15$. Prove that $K_1 \cap K_2$ is the trivial group.

5. Prove that $\mathbb{Z}_5 \times \mathbb{Z}$ is not cyclic.

6. In each case below, state whether the statement is true or false. Justify your answer in each case.

(i) $GL(3)$ is not cyclic.

(ii) There is an element in $O(2)$ that is not in $SO(2)$.

(iii) A_5 has an element with order 7.

DEPARTMENT OF MATHEMATICS & STATISTICS

MT316A

Homework 4

Due by 4 p.m on December 2, 2022

1. In each case below, state whether the statement is true or false. Justify your answer in each case.

(i) $A_4 \times \mathbb{Z}_3$ is isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_9$.

(ii) Every group of order 17 has an element of order 17.

(iii) There is an infinite group with an element of order 4.

2. (a) Consider the symmetry group of the square, which we called the dihedral group D_4. Is D_4 abelian? Justify your answer.

(b) Using the notation in example 6 in lecture 11, prove that $D_4 =< \tau, \sigma_2 >$.

3. Consider the permutations $\alpha = (216)(342)(78)$ and $\beta = (261)(75)(438)$ in S_8. Is α conjugate to β? Justify your answer.

4. Give an example of a function $h : D_3 \to GL(3)$ that is not a homomorphism. Justify your answer.

5. Give an example of two groups of order 54 that are not isomorphic to each other. Justify your answer.

6. Prove Lemma 7 in lecture 14: Suppose $f : G_1 \to G_2$ is a homomorphism. Then, prove that $\ker(f)$ is a subgroup of G_1 and that $\text{im}(f)$ is a subgroup of G_2.

7. For each of the three groups, S_7, $\mathbb{Z}_7$, $\mathbb{Z}$, determine whether the group is simple or not. Justify your answer in each case.

DEPARTMENT OF MATHEMATICS & STATISTICS

MT 316A

Homework 1, 2022

Due by 4 p.m. on October 7, 2022.

1. Suppose $\mathbb{Q}$ is the set of rational numbers and suppose $A = \{x \in \mathbb{Q} : x < 0\}$. Also, suppose $+$ denotes the usual addition on A. Is $(A, +)$ a group? Justify your answer.

2. Suppose $\mathbb{W} = \{x \in \mathbb{R} : x > 0\}$ is the set of positive real numbers and suppose $*$ denotes the usual multiplication on W. Is $(W, *)$ a group? Justify your answer.

3. Find the order of each element in $\mathbb{Z}_9$.

4. Find the inverse of each element in $\mathbb{Z}_6$.

5. Prove that the following cancellation property holds in every group $(G, *)$:

If $a, b, c \in G$ and $a * b = a * c$, then $b = c$.

6. Find the order of $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ in the group $GL(2)$. Also, find the order of $\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$ in the group $GL(2)$. Justify your answer in each case.

7. In each case below, state whether the statement is true or false. Justify your answer in each case.

(i) Every subgroup of an abelian group is abelian.

(ii) Every non–trivial subgroup of a non–abelian group is non–abelian.

8. Prove that $(xy)^{-1} = y^{-1}x^{-1}$, for all x, y in every group G.

DEPARTMENT OF MATHEMATICS & STATISTICS

MT316A

Homework 2

Due by 4 p.m. on October 21, 2022

1. In each case below, state whether the statement is true or false. Justify your answer in each case.

(i) $\alpha \in S_6$ is odd $\iff$ α^2 is odd.

(ii) $\alpha \in S_6$ is odd $\iff$ α^{-1} is odd.

(iii) There is an x in some group G that satisfies $o(x) = 2$ and $x^4 = x^3$.

2. Identify the orders of all the elements in $\mathbb{Z}_2 \times \mathbb{Z}_3$.

3. (i) Is $A \cup B$ a subgroup of G for all subgroups A, B of every group G? Justify your answer.

(ii) Prove that $H \cap K$ is a subgroup of G for all subgroups H, K of every group G.

4. Consider the 2×2 matrix $A_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ and let $H = \{A_\theta : \theta \in [0, 2\pi)\}$. Then,

(i) Prove that H is a subgroup of $GL(2)$.

(ii) Is H an abelian group? Justify your answer.

5. (i) Prove that $S_3 =< (1,2), (1,3) >$.

(ii) Is $< (1,2), (1,3) >$ a minimal generating set for S_3? Justify your answer.

6. In each case below, state whether the statement is true or false. Justify your answer in each case.

(i) $\{x \in G : o(x) \leq 2\}$ is a subgroup of G for every non–abelian group G.

(ii) $\{x \in G : o(x) \leq 3\}$ is a subgroup of G for every abelian group G.

7. Suppose $\alpha = (125)(24)(314)$ in S_6.

(i) Express α as a product of disjoint cycles.

(ii) Find $o(\alpha)$

(iii) Find α^3.

(iv) Is α^{-1} an even permutation? Justify your answer.