Lectures in the Group Theory

(First Semester 2017-2018)

For the second Stage

By

Assist. Prof Dr. Muna Abbas

University of Baghdad\College of Science for Women\Department of Mathematics

The First Lecture

Basic Definitions

Generalizations of the quadratic formula for finding the roots of cubic and quartic polynomials were discovered in the early 1500s. Over the next three centuries, many tried to find analogous formulas for the roots of higher-degree polynomials, but in 1824, N. H. Abel (1802–1829) proved that there is no such formula giving the roots of the general polynomial of degree 5. In 1831, E. Galois (1811– 1832) completely solved this problem by finding precisely which polynomials, of arbitrary degree, admit such a formula for their roots. His fundamental idea involved his invention of the idea of *group*. Since Galois's time, groups have arisen in many other areas of mathematics.

Definition (1): A **binary operation** on a set G is a function

$$*: G \times G \to G.$$

Definition (2): A **group** is a set G with an operation $*$ and a special element $e \in G$ (sometimes denoted by 1), called the **identity**, such that:

(i) The **associative law** holds: for every $a, b, c \in G$,

$$a * (b * c) = (a * b) * c;$$

(ii) $e * a = a$ for all $a \in G$;

(iii) For every $a \in G$, there is $a^{\mathrm{I}} \in G$ with $a^{\mathrm{I}} * a = e$.

Remark (3):

An **additive group** is a set G equipped with an

operation (+) and an identity element $0 \in G$ such that

(i) $a + (b + c) = (a + b) + c$ for every $a, b, c \in G$;

(ii) $0 + a = a$ for all $a \in G$;

(iii) For every $a \in G$, there is $-a \in G$ with $(-a) + a = 0$.

Note that the inverse of a, in additive notation, is written -a instead of a^{-1}.

Definition (4): A group G is called **abelian** if it satisfies the following:

$x * y = y * x$ holds for every $x, y \in G$.

Remark (5):

This term honors N. H. Abel who proved a theorem, in 1827, equivalent to there being a formula for the roots of a polynomial if its Galois group is commutative. This theorem is virtually forgotten today, because it was superseded by a theorem of Galois around 1830.

Definition (6): If G is a group and $a \in G$, then the unique element $a^{-1} \in G$ such that $a^{-1} * a = e$ is called the **inverse of a**, and it is denoted by a^{-1}.

Here are three more properties holding in all groups.

Lemma (7): If G be a group, then the following statement are holds:

(i) The cancellation laws hold: if $a, b, x \in G$, and either $x * a = x * b$ or $a * x = b * x$, then $a = b$.

(ii) $(a^{-1})^{-1} = a$, for all $a \in G$.

(iii) If $a, b \in G$, then:

$$(a * b)^{-1} = b^{-1} * a^{-1}.$$

More generally, for all $n \geq 2$,

$$(a_1 * a_2 * \cdots * a_n)^{-1} = a_n^{-1} * \cdots * a^{2-1} * a^{1-1}.$$

Proof:

(i) $a = e * a = (x^{-1} * x) * a = x^{-1} * (x * a)$

$= x^{-1} * (x * b) = (x^{-1} * x) * b = e * b = b.$

In similar proof, when x is on the right.

From now on, we will usually denote the product a b in a group by $a\mathring{b}$ (we have already abbreviated α β to αβ in symmetric groups), and we will denote the identity by 1 instead of by e. When a group is abelian, however, we will often use additive notation. Here is the definition of group written in additive notation.

The Second Lecture

Some Examples

In this lecture we give some examples about groups, such as (Z,+), (Q\{0},.), S_n with the composition operator and Boolean group.

Examples:

(i) (Z,+); The set of all integers is an additive abelian group with identity $e = 0$, and with the inverse of an integer n being - n. Similarly, one can see that (Q,+) and (R,+) are additive abelian groups, where Q is the set of rational numbers and R is the set of real numbers.

(ii) (Q\{0}, .); The set of all nonzero rational numbers, is an abelian group, where (.) is the ordinary multiplication, the number 1 is the identity, and the inverse of r is 1/r . Similarly, (R\{0},.) is a multiplicative abelian group.

(iii) Let X be a set. Recall that if A and B are subsets of X, then their symmetric difference is $A \Delta B = (A-B) \cup (B-A)$. The **Boolean group** P (X) is the family of all the subsets of X with addition given by symmetric difference.

(iv) Consider S_n , the set of all permutations of $X = \{1, 2, \ldots, n\}$. It is form a group with the composition operation.

Remark: Let G be a group, let a, b G, and let m and n be (not necessarily positive) integers.

(i) If a and b commute, then $(ab)^n = a^n b^n$.

(ii) $(a^m)^n = a^{mn}$

(iii) $a^m a^n = a^{m+n}$.

The Third Lecture

Subgroups and Langrage Theorem

A subgroup of a group G is a subset which is a group under the same operation as in G. The following definition will help to make this last phrase precise.

Definition (1): Let $*$ be an operation on a set G, and let S $\subseteq$ G be a

subset. We say that S is **closed under** $*$ if $x * y \in S$ for all x , y $\in$ S.

The operation on a group G is a function *: G x G $\rightarrow$ G.
(for example, 2 and -2 lie in Z_+, but their sum $-2 + 2 = 0 \notin Z_+$.

Definition (2): A subset H of a group G is a **subgroup** if:

(i) $1 \in H$;

(ii) If $x, y \in H$, then $xy \in H$; that is, H is closed under $*$.

(iii) If $x \in H$, then $x^{-1} \in H$.

Proposition (3): Every subgroup $H \leq G$ of a group G is itself a group.

Proof: Axiom (ii) (in the definition of subgroup) shows that H is closed under the operation of G; that is, H has an operation (namely, the restriction of the operation $*: G \times G \rightarrow G$ to $H \times H \subseteq G \times G$. This operation is associative:
since the equation $(xy)z = x(yz)$ holds for all $x, y, z \in G$, it holds, in particular, for all $x, y, z \in H$. Finally, axiom (i) gives the identity, and axiom (iii) gives

inverses.

It is quicker to check that a subset H of a group G is a subgroup (and hence that it is a group in its own right) than to verify the group axioms for H, for associativity is inherited from the operation on G and hence it need not be verified again.

One can shorten the list of items needed to verify that a subset is, in fact, a subgroup.

Proposition (4): A subset H of a group G is a subgroup if and only if H is nonempty and, whenever $x, y \in H$, then $x y^{-1} \in H$.

Proof: If H is a subgroup, then it is nonempty, for $1 \in H$. If $x , y \in H$, then $y^{-1} \in H$, by part (iii) of the definition, and so $x y^{-1} \in H$, by part (ii).
Conversely, assume that H is a subset satisfying the new condition. Since
H is nonempty, it contains some element, say, h. Taking $x = h = y$, we see that $e = hh^{-1} \in H$, and so part (i) holds. If $y \in H$, then set $x = e$ (which we can now do because $e \in H$), giving $y^{-1} = ey^{-1} \in H$, and so part (iii) holds. Finally, we know that $(y^{-1})^{-1} = y$, by. Hence, if $x , y \in H$, then $y^{-1} \in H$ and so $x y = x (y^{-1})^{-1} \in H$. Therefore, H is a subgroup of G.

Since every subgroup contains e, one may replace the hypothesis "H is nonempty" in Proposition by "$e \in H$".

Note that if the operation in G is addition, then the condition in the proposition is that H is a nonempty subset of G such that $x, y \in H$ implies $x- y \in H$.

Proposition (5): Let G be a finite group, and $a \in G$. Then the order of a, is the number of elements in (a).

Definition (6): If G is a finite group, then the number of elements in G, denoted by |G|, is called the **order of G**.

Definition (7): If X is a subset of a group G, such that X generates G, then G is called **finitely generated**, and G generated by **X**.

In particular; If G = ({a}), then G is generated by the subset X = {a}.

Definition (8):

A group G is called **cyclic** if G = (a); that is G can be generated by only one element say a, and this element is called a generator of G.

Note that we can define cyclic subgroup as follows.

Definition (9): If G is a group and a ∈ G, write

(a)= $\{a^n: n \in Z_+\}$ = {all powers of a}
(a) is called **cyclic subgroup** of G
generated by a.

Proposition (10): The intersection of any family of subgroups is again subgroup.

The Forth Lecture

Coset of sets

Definition (1): If H is a subgroup of a group G and a G, then the **coset a H** is the subset a H of G, where

$$a H = \{ah: h \in H \}$$

Of course, a = ae ∈ a H. Cosets are usually not subgroups.

The cosets just defined are often called left cosets; there are also right cosets of H, namely, subsets of the form H a {ha| h ∈H}; these arise in further study of groups, but we shall work almost exclusively with (left) cosets.

In particular, if the operation is addition, then the coset is denoted by

$$a + H = \{a + h : h \in H \}.$$

Proposition (2): Let G be a group, and H be a subgroup of G, for any a, b ∈ G we have the following:

(i) a H = b H if and only if $b^{-1}a \in H$. In particular, a H = H if and only if a ∈ H.

(ii) If a H ∩ b H ≠∅, then a H = b H.

(iii) For each a∈G:

Order of H is equal

to the order of aH.

Proof:

(i) It is clear.

(ii) It is clear.

(iii) The function f: H → a H which is given by f (h) = ah, is easily seen to be a bijective [its inverse a H → H is given by ah r→ a^{-1}(ah) = h]. Therefore, H and a H have the same number of elements.

Theorem (3): (Lagrange's Theorem)

If H is a subgroup of a finite group G, then |H | is a divisor of |G|. That is:

$$|G| = [G : H]|H |$$

This formula shows that the index [G : H] is also a divisor of |G|.

Corollary (4): If H is a subgroup of a finite group G, then

$$[G : H] = |G|/|H |$$

Corollary (5): If G is a finite group and $a \in G$, then the order of a is a divisor of $|G|$.

Corollary (6): If a finite group G has order m, then $a^m = e$ for all $a \in G$.

Corollary (7): If p is a prime, then every group G of order p is cyclic.

Proof: Choose $a \in G$ with $a \neq e$, and let $H = (a)$ be the cyclic subgroup generated by a. By Lagrange's theorem, $|H|$ is a divisor of $|G| = p$. Since p is a prime and $|H| > 1$, it follows that $|H| = p = |G|$, and so $H = G$.

Lagrange's theorem says that the order of a subgroup of a finite group G is a divisor of G . Is the "converse" of Lagrange's theorem true? That is, if d is a divisor of G, must there exists a subgroup of G having order d? The answer is "no;" We can show that the alternating group A4 is a group of order 12 which has no subgroup of order 6.

The Fifth Lecture

Homomorphism

An important problem is determining whether two given groups G and H are somehow the same.

Definition (1): If (G, *) and (H, ◦) are groups, then a function f: G → H is a **homomorphism** if:

$$f(x * y) = f(x) \circ f(y)$$

for all x , y ∈ G. If f is also a bijective, then f is called an **isomorphism**. We say that G and H are isomorphic, denoted by G ≅ H, if there exists an isomorphism f: G → H.

Example (2):
Let be the group of all real numbers with operation addition, and let R^+ be the group of all positive real numbers with operation multiplication. The function f: R→ R^+ , defined by f(x)=tx , where t is constant number, is a homomorphism; for if x , y ∈R, then

$$f(x + y) = t(x+y) = tx\ ty = f(x)\, f(y).$$

We now turn from isomorphisms to more general homomorphisms.

Lemma (3): Let f: G → H be a homomorphism.

(i) f (e) = e;
(ii) $f(x^{-1}) = f(x)^{-1}$;

Remark (4):
We can show that any two finite cyclic groups G and H of the same order m are isomorphic. It will then follow from that any two groups of prime order p are isomorphic.

Definition (5):
A property of a group G that is shared by every other group isomorphic to it is called an **invariant of G**. For example, the order, G, is an invariant of G, for isomorphic groups have the same order. Being abelian is an invariant [if a and b commute,

then ab = ba and

$$f(a)\, f(b) = f(ab) = f(ba) = f(b)\, f(a);$$

hence, f (a) and f (b) commute]. Thus, M_{2x2} and GL(2,R) are not isomorphic, for is abelian and GL(2,R) is not.

Definition (6): If $f: G \to H$ is a homomorphism, define

$$\textbf{kernel } f = \{x \in G : f(x) = e\}$$

and

$$\textbf{image } f = \{h \in H : h = f(x) \text{ for some } x \in G\}$$

We usually abbreviate kernel f to ker f and image f to im f

So that if f: G $\rightarrow$ H is a homomorphism and B is a subgroup of H then f^{-1}(B) is a subgroup of G containing ker f .

Note: Kernel comes from the German word meaning "grain" or "seed" (corn comes from the same word).

Its usage here indicates an important ingredient of a homomorphism, we give it without proof.

Proposition: Let f: G $\rightarrow$ H be a homomorphism.

(i) ker f is a subgroup of G and im f is a subgroup of H .

(ii) If x $\in$ ker f and if a $\in$ G, then ax $a^{-1} \in$ ker f.

(iii) f is an injection if and only if ker f = {e}.

The Sixth Lecture

Normal Subgroups

Definition (1): A subgroup K of a group G is called **normal,** if for each k $\in$ K and g $\in$ G imply gk$g^{-1} \in$ K. that is g$Kg^{-1} \subseteq$ G for every g$\in$G.

Definition (2):

Define the **center of a group G,** denoted by Z (G), to be

$$Z(G) = \{z \in G: zg = gz \text{ for all } g \in G\};$$

that is, Z (G) consists of all elements commuting with every element in G. (Note that the equation zg

= gz can be rewritten as $z = gzg^{-1}$, so that no other elements in G are conjugate to z.

Remark (3):

Let us show that Z (G) is a subgroup of G. We can easily show that Z(G is subgroup of G. It is clear that $Z(G)\neq\emptyset$ since $1 \in Z(G)$, for 1 commutes with everything. Now, If $y, z \in Z(G)$, then yg = gy and zg = gz for all $g \in G$. Therefore, (yz)g = y(zg) = y(gz) = (yg)z = g(yz), so that yz commutes with everything, hence $yz \in Z(G)$. Finally, if $z \in Z(G)$, then zg = gz for all $g \in G$; in particular, $zg^{-1} = g^{-1}z$. Therefore,

$$gz^{-1} = (zg^{-1})^{-1} = (g^{-1}z)^{-1} = z^{-1}g$$

(we are using $(ab)^{-1} = b^{-1}a^{-1}$ and $(a^{-1})^{-1} = a$). So that Z(G) is subgroup pf G.

Clearly che center Z (G) is a normal subgroup; since if $z \in Z(G)$ and $g \in G$, then

$$gzg^{-1} = zgg^{-1} = z \in Z(G)$$

A group G is abelian if and only if Z (G) = G. At the other extreme are groups G for which Z (G) = {1}; such groups are called centerless. For example, it is easy to see that $Z(S_3) = \{1\}$; indeed, all large symmetric groups are centerless.

Proposition (4):

(i) If H is a subgroup of index 2 in a group G, then $g^2 \in H$ for every $g \in G$.

(ii) If H is a subgroup of index 2 in a group G, then H is a normal subgroup of G.

Proof:

(i) Since H has index 2, there are exactly two cosets, namely, H and a H, where $a \in G\backslash H$. Thus, G is the disjoint union $G = H \cup a H$. Take $g \in G$ with

$g \notin H$. So that $g = ah$ for some $h \in H$. If $g^2 \notin H$, then $g^2 = ah_1$, where $h_1 \in H$. Hence,

$$g = g^{-1} g^2 = (ah)^{-1} a h_1 = h^{-1}a^{-1}a h_1 = h^{-1} h_1 \in H,$$

and this is a contradiction.

(ii) It suffices to prove that if $h \in H$, then the conjugate $ghg^{-1} \in H$ for every $g \in G$. Since H has index 2, there are exactly two cosets, namely, H and a H, where $a \notin H$. Now, either $g \in H$ or $g \in a H$. If $g \in H$, then $ghg^{-1} \in H$, because H is a subgroup. In the second case, write $g = ax$, where $x \in H$. Then $ghg^{-1} = a(x hx^{-1})a^{-1} = ah_I a^{-1}$, where $h_I = x hx^{-1} \in H$ (for h_I is a product of three elements in H). If $ghg \notin H$, then $ghg^{-1} = ah_I a^{-1} \in a H$; that is,

$ah_I a^{-1} = ay$ for some $y \in H$. Canceling a, we have $hIa^{-1} = y$, which gives the contradiction $a = y^{-1}h_I \in H$. Therefore, if $h \in H$, every conjugate of h also lies in H; that is, H is a normal subgroup of G.

Proposition(5) : If K is a normal subgroup of a group G, then

$$bK = K b$$

for every $b \in G$.

Proof: We must show that $bK \subseteq Kb$ and $Kb \subseteq bK$. So if $bk \in bK$, then clearly $bK = bKb^{-1}b$.

Since $bKb^{-1} \in K$, then $bKb^{-1} = k_1$ for some $k_1 \in K$. This implies that $bK \in Kb$. Similarity for the other case. Thus $bK = Kb$.

The Seventh Lecture

Quotient Group

Here is a fundamental construction of a new group from a given group.

Theorem (1): Let G/K denotes the family of all the cosets of a subgroup K of G. If K is a normal subgroup, then:

$$a\,K\,bK = abK$$

for all $a, b \in G$, and G/K is a group under this operation

Definition (2): The group G/K is called the **quotient group**; when G is finite, its order G/K is the index [G:K] (presumably, this is the reason quotient groups are so called).

We can now prove the converse of Proposition 2.91(ii).

Proposition (3): Every normal subgroup K of a group G is the kernel of some homomorphism.

Proof:

Define the natural map $\pi: G \to G/K$ by $\pi(a) = a\,K$. With this notation, the formula $a\,K\,bK = abK$ can be rewritten as $\pi(a)\pi(b) = \pi(ab)$; thus, π is a (surjective) homomorphism. Since K is the identity element in G/K,

$$\ker \pi = \{a \in G : \pi(a) = K\} = \{a \in G : a\,K = K\} = K$$

The Eighth Lecture
First Isomorphism Theorem

The following theorem shows that every homomorphism gives rise to an isomorphism, and that quotient groups are merely constructions of homomorphic images.

Theorem (1): (First Isomorphism Theorem)

If f: G→H is a homomorphism, then:

$$G/\ker f \cong \text{im } f$$

Where im f = f(H). In more detail, if we put ker f = K , then the function $\phi : G/K \rightarrow f(H)$ is given by:

ϕ: a K r→ f (a) for each a∈G, is an isomorphism.

Proof:

It is clear that ker f is a normal subgroup of G, and we can easily show that ϕ is well-defined. Let us now see that ϕ is a homomorphism. Since f is a homomorphism and $\phi(a K) = f(a)$,

$\phi(a K bK) = \phi(abK) = f(ab) = f(a) f(b) = \phi(a K)\phi(bK)$.

Also ϕ is surjective and injective Therefore, ϕ: G/K → im f is an isomorphism.

Remark (2):

1. Here is a minor application of the first isomorphism theorem. For any group G, the identity function f: G → G is a surjective homomorphism with ker f =

{1}. By the first isomorphism theorem, we have

$$G/\{1\} \cong G$$

2. Given any homomorphism $f:G\to H$, one should immediately ask for its kernel and its image; the first isomorphism theorem will then provide an isomorphism

$G/\ker f \cong \text{im } f$. Since there is no significant difference between isomorphic groups, the first isomorphism theorem also says that there is no significant difference between quotient groups and homomorphic images.

Proposition (3):

1. If H and K are subgroups of a group G, and if one of them is a normal subgroup, then HK is a subgroup of G. Moreover, HK = KH.
2. If both H and K are normal subgroups, then HK is a normal subgroup.

Proof:

1. Assume first that K is normal in G. We claim that HK = KH. If $hk \in HK$, then:

$$hk = hkh^{-1}h = k_1 h \in KH$$

where $k_1 = hkh^{-1}$, then $k_1 \in K$, because K is normal subgroup

Hence, HK = KH. For the reverse inclusion, write $kh = hh^{-1}kh = hk_2 \in HK$, where $k_2 = h^{-1}kh$.

(Note that the same argument shows that HK = KH if H is normal subgroup of G.)

We now show that HK is a subgroup. Since $e \in H$ and $e \in K$, we have $e = e \cdot e \in HK$.

If $hk \in HK$, then $(hk)^{-1} = k^{-1} h^{-1} \in KH = HK$. If $hk, h_1k_1 \in HK$, then $h_1^{-1} kh_1 = ke \in K$ and

$$Hkh_1 k_1 = hh_1(h_1^{-1} kh_1)k_1 = (hh_1)(kek_1) \in HK.$$

Therefore, HK is a subgroup of G.

2. If $g \in G$, then:

$$ghkg^{-1} = (ghg^{-1})(gkg^{-1}) \in HK$$

Therefore, HK is normal in G.

The Ninth Lecture
Second Isomorphism Theorem

Here is a useful counting result.

Definition (1): If H and K are subgroups of a finite group G, then then the **Product Formula** is:

$$|HK||H \cap K| = |H||K|$$

Theorem (2): (Second Isomorphism Theorem)

If H and K are subgroups of a group G with H is normal in G, then HK is a subgroup of G and $H \cap K$ is normal in K. Moreover:

$$K/(H \cap K) \cong HK/H$$

Proof:

We begin by showing first that HK/H makes sense, and then describing its elements. Since H is normal subgroup of G, then HK is a subgroup of G. Normality of H in HK follows

from a more general fact: if $H \subseteq S \subseteq G$ and if H is normal in G, then H is normal in S.

We can easily show that each coset $x H \in HK/H$ has the form $k H$ for some $k \in K$. It follows that the function $f: K \to HK/H$, given by $f(k) = k H$, is surjective. Moreover, f is a homomorphism, for it is the restriction of the natural map $\pi: G \to G/H$. Since $\ker \pi = H$, it follows that $\ker f = H \cap K$ and so $H \cap K$ is a normal subgroup of K. The first isomorphisim theorem gives:

$$K /(H \cap K) \cong HK/H$$

Remark (3):

The second isomorphism theorem gives the product formula in the special case when one of the subgroups is normal: if $K /(H \cap K) \cong H K /H$, then: $|K /(H \cap K)| = |H K /H |$, and so $|H K ||H \cap K | = |H ||K |$.

The Tenth Lecture
Third Isomorphism Theorem

In the following lecture we study the third important theorem of fundamental isomorphism theorem.

Theorem (1): (Third Isomorphism Theorem)

If H and K are normal subgroups of a group G with $K \leq H$, then H/K is normal in G/K and

$$(G/K)/(H/K) \cong G/H$$

Proof:

Define f: G/K$\rightarrow$G/H by f(a K) = a H. Note that f is a (well- defined function, for if a G = b K, then $a^{-1}b \in K$ But $K \subseteq H$, thus $a^{-1}b \in H$, and so a H= b H , and we are done. It is easy to see that f is an epimorphism.

Now ker f = H/K. Also clearly H/K is a normal subgroup of G/K. Since f is monomorphism, so by the first isomorphism theorem we have:

$$(G/K)/(H/K) \cong G/H$$

The third isomorphism theorem is easy to remember: the K's in the fraction (G/K)/(H/K) can be canceled. One can better appreciate the first isomorphism theorem after having proved the third one. The quotient group (G/K)/(H/K) consists of cosets (of H/K) whose representatives are themselves cosets (of G/K).

Here is another construction of a new group from two given groups.

Definition (2): If H and K are groups, then their **direct product**, denoted by HxK, is the set of all ordered pairs (h, k) equipped with the following operation:

$$(h, k)(h_1, k_1) = (hh_1, kk_1)$$

It is routine to check that HXK is a group [the identity element is (e, e_1) and $(h, k)^{-1} = (h^{-1}, k^{-1})$.

Remark (3): let G and h be groups.Then HxK is abelian if and only if both H and K are abelian.

We end the tenth lecture by the following example.

Example:

Zx2Z is the direct product between (Z, +) and (2Z, +) groups.

The identity element is (0, 0), and the inverse element of (a, b) is (-a, -b).

References

[1] D. M. Burton, Abstract and linear algebra, 1972.

[2] Joseph J.Rotman, Advanced Modren Algebra, 2003.

[3] John B. Fraleigh, A First Course in Abstract Algebra, Seventh Edition, 2002.

[4] Joseph A. Gallian, Contemporary Abstract Algebra, 2010.

End of the Lectures of the First Semester of Group Theory

Second Stage

2017-2018