MATH 323, Algebra I, Fall 2020

Course notes, Chapter 5, Normal subgroups

Laurence Barker, Bilkent University. Version: 27 November 2020.

These notes, updated as the course progresses, are a record of the prepared text of the lectures, with a little more detail added, but they cannot cover much of the oral component of the lectures.

Summary of contents

We have already seen how groups give rise to smaller groups called subgroups. We have also seen how abelian groups give rise to another kind of smaller group, called a quotient group. In this section, we introduce and discuss quotient groups of arbitrary groups.

Fuller details on the material we shall be summarizing can be found in Judson, mainly in Chapters 10 and 11.

We shall be reviewing:

- conjugacy classes of elements,
- conjugacy classes of subgroups,
- normal subgroups,
- quotient groups,
- group homomorphisms,
- the Three Isomorphism Theorems for groups,
- the Direct Product Recognition Theorem.

Conjugacy classes of group elements: For a group G and elements $g, x \in g$, we write

$$^g x = gxg^{-1} \ .$$

We call $^g x$ the **conjugate** of x by g. We also call $^g x$ a G**-conjugate** of x or, when no ambiguity can arise, a **conjugate** of x.

We mention that many texts discuss conjugation of elements using the notation $x^g = g^{-1}xg$. Thus, $x^g = {}^{g^{-1}}x$.

Remark 5.1: *Let g be an element of a group G. Then there is an equivalence relation $=_G$ on G such that, given $x, y \in G$, then $x =_G y$ provided $x = {}^g y$ for some $g \in G$.*

Proof: Plainly $=_G$ is reflexive. Given $g, x \in G$, then

$$^{g^{-1}}({}^g x) = x \ .$$

So $=_G$ is symmetric. Given $f \in G$, then

$$^f({}^g x) = {}^{fg}x \ .$$

So $=_G$ is transitive. $\square$

The relation $=_G$ on G is called G**-conjugation**. The equivalence class of $x \in G$ under $=_G$, denoted $[x]_G$, is called the G**-conjugacy class** of x or, when no ambiguity can arise, the **conjugacy class** of x. Thus,

$$[x]_G = \{{}^g x : g \in G\} \ .$$

Recall, $S_3 = \{1, a, a^2, b, ab, a^2b\}$ and the group operation on S_3 is determined by the conditions $a^3 = b^2 = 1$ and $ba = a^2b$. We have

$$^1a = {}^a a = {}^{a^2}a = a \ , \qquad {}^b a = {}^{ab}a = {}^{a^2b}a = a^2 \ .$$

So the conjugacy class of a is $[a]_{S_3} = \{a, a^2\}$. Similar calculations for the other elements of S_3 show that the conjugacy classes in S_3 are

$$[1]_{S_3} = \{1\} \ , \quad [a]_{S_3} = [a^2]_{S_3} = \{a, a^2\} \ , \quad [b]_{S_3} = [ab]_{S_3} = [a^2b]_{S_3} = \{b, ab, a^2b\} \ .$$

As another example, consider the group $D_8 = \{1, c, c^2, c^3, d, cd, c^2d, c^3d\}$. The Cayley table for D_8 is recorded in the previous chapter. By inspection of the Cayley table for D_8, it is not hard to see that the conjugacy classes of in D_8 are

$$\{1\} \ , \qquad \{c, c^3\} \ , \qquad \{c^2\} \ , \qquad \{d, c^2d\} \ , \qquad \{cd, c^3d\} \ .$$

But, as we noted in that chapter, examination of larger groups is not often accomplished just by crudely considering the Cayley table. Other methods are needed. In the next section, we present a result that can often be useful for examining conjugacy classes in finite groups.

The size of a conjugacy class of a finite group: In this section, we give a formula that can be used to calculate the size of a conjugacy class of a finite group.

For any group G and an element $x \in G$, we define the **centralizer** of x in G to be

$$C_G(x) = \{g \in G : gx = xg\} \ .$$

Observe that, given $f, g \in C_G(x)$, then $fgx = fxg = xfg$, hence $fg \in C_G(x)$. We also have $gxg^{-1} = x$, that is $xg^{-1} = g^{-1}x$, hence $g^{-1} \in C_G(x)$. We have shown that $C_G(x)$ is closed under products and inverses. In other words, $C_G(x)$ is a subgroup of G. We call $C_G(x)$ the **centralizer** of x in G.

In the case where G is finite, the next result relates the size of the conjugacy class $[x]_G$ with the size of the centralizer $C_G(x)$.

Theorem 5.2: *Let G be a finite group and $x \in G$. Then $|[x]_G|.|C_G(x)| = |G|$.*

Proof: Let $\equiv$ be the equivalence relation on G such that, given $f, g \in G$, then $f \equiv g$ if and only if ${}^f x = {}^g x$. That condition on f and g can be expressed as ${}^{f^{-1}g}x = x$, in other words, $f^{-1}g \in C_G(x)$, put another way, $gC_G(x) = fC_G(x)$. So there is a bijective correspondence ${}^g x \leftarrow gC_G(x)$ between the G-conjugates ${}^g x$ of x and the left cosets $gC_G(x)$ of $C_G(x)$ in G. In particular, the number of G-conjugates of x is equal to the number $|G|/|C_G(x)|$ of left cosets of $C_G(x)$ in G. □

As an example, letting a be an element with order 3 in S_3, then $[a]_{S_3} = \{a, a^2\}$ and $C_{S_3}(a) = \{1, a, a^2\}$. In this case, the equality in Theorem 5.2 is $|[a]_{S_3}|.|C_{S_3}(x)| = 6 = |S_3|$.

The centre of a group:

An element z of any group G is said to be **central** provided $zg = gz$ for all $g \in G$. That is equivalent to the condition that the conjugacy class of z is a singleton set, $[z]_G = \{z\}$. We write $Z(G)$ to denote the set of central elements of G. Thus,

$$Z(G) = \{z \in G : \forall g \in G, gz = zg\} \ .$$

It is easy to check that $Z(G)$ is closed under composites and inverses. So $Z(G)$ is a subgroup of G. We call $Z(G)$ the **centre** of G.

Of course, $Z(G) = G$ if and only if G is abelian. As two non-abelian examples, $Z(S_3) = \{1\}$, while

$$Z(D_8) = \{1, c^2\} \cong C_2 \ .$$

Conjugacy classes of subgroups: We modify some of the notions in the previous section, now with subgroups in place of elements. For a group G, an element $g \in G$ and a subgroup $H \leq G$, we define

$${}^g H = \{{}^g x : x \in H\} \ .$$

Observe that, for all $x, y \in G$, we have ${}^g(x^{-1}) = ({}^g x)^{-1}$ and ${}^g(xy) = {}^g x . {}^g y$. By considering the case where $x, y \in h$, we see that ${}^g H$ is closed under inverses and composites. So ${}^g H$ is a subgroup of G. We call ${}^g H$ the **conjugate** of H by g. As with conjugates of elements, we occasionally write conjugates of subgroups as $H^g = \{x^g : x \in H\} = {}^{g^{-1}}H$.

We omit proof of the next remark, since the argument is easy and much the same as for Remark 5.1.

Remark 5.3: *Let g be an element of a group G. Then, on the set of subgroups of G, there is an equivalence relation $=_G$ such that, given subgroups $H, I \leq G$, then $H =_G I$ provided $H = {}^g I$ for some $g \in G$.*

Note that we are abusing the expression $=_G$, since we employed it for a different equivalence relation in the previous section. Further abuses of that symbol will appear later. We rely on context to resolve the ambiguity.

The relation $=_G$ in the latest remark is again called G-**conjugation**. The equivalence class of $H \leq G$ under $=_G$, again called the G**-conjugacy class** of H or just the **conjugacy class** of H, is written as

$$[H]_G = \{{}^g H : g \in G\} \ .$$

In the notation of the previous section, the conjugacy classes of proper subgroups of S_3 are $[\langle a\rangle]_{S_3}$ and $[\langle b\rangle]_{S_3}$.

Normal subgroups: The next remark is obvious.

Remark 5.4: *Let G be a group. Let H be a subgroup of G. Then the following five conditions are equivalent:*
(a) *The left cosets of H in G are the same as the right cosets of H in G.*
(b) *For all $g \in G$, we have $gH = Hg$.*
(c) *For all $g \in G$, we have ${}^gH = H$.*
(d) *For all $g \in G$, we have $H^g = H$.*
(e) *The G-conjugacy class of H is a singleton set, $[H]_G = \{H\}$.*

When the equivalent conditions in the remark hold, we call H a **normal subgroup** of G and we write $H \trianglelefteq G$.

A group with order 1 is called a **trivial group**. The cyclic group C_1 is a trivial group. All trivial groups are isomorphic to each other, so it makes sense to speak of *the* trivial group, denoted C_1.

In any group G, there is exactly one trivial subgroup, namely $\{1_G\}$. Of course, the element 1_G of G is not the same thing as the trivial subgroup $\{1_G\}$. Nevertheless, it is common practise to abuse notation by writing the trivial subgroup as 1. That is potentially confusing and, when that notation is used, care must be taken to ensure that the context resolves ambiguity. One can do that using accompanying words, say, "the identity element 1" versus "the trivial subgroup 1".

Plainly, the trivial subgroup is a normal subgroup, $1 \trianglelefteq G$. We also have $G \trianglelefteq G$.

Recall, the proper subgroups of S_3 are $\langle a\rangle$, $\langle b\rangle$, $\langle ab\rangle$, $\langle a^2b\rangle$. Among those four, only the one with order 3 is normal, $\langle a\rangle \trianglelefteq S_3$.

Discussion: What are the proper subgroups of D_8? Which ones are normal?

We have the following general example of a normal subgroup.

Remark 5.5: *For any group G, we have $Z(G) \trianglelefteq G$.*

Proof: Plainly, for all $g \in G$, we have $gZ(G) = Z(G)g$. □

Quotient groups: Let G be a group and $H \trianglelefteq G$. Since the left cosets of H in G coincide with the right cosets of H in G, we can speak simply of the cosets of H in G. We write the set of cosets of H in G as

$$G/H = \{gH : g \in G\} = \{Hg : g \in G\} .$$

We make become a group by imposing the operation given by

$$fH.gH = fgH$$

for $f, g \in G$. To see that the operation is well-defined, observe that, given $f', g' \in G$ such that $f'H = fH$ and $g'H = gH$, then $f' = fh$ and $g' = gi$ for $h, i \in H$, whereupon $f'g' = fhgi$. But $Hg = gH$, so $hg = gk$ with $k \in H$, hence $fhgi = fgki$. Since $ki \in H$, we have $f'g'H = fgH$. We have confirmed that the operation on G/H is well-defined. The group axioms are easy to check too, indeed, the identity element of G/H is H and inverses are given by $(gH)^{-1} = g^{-1}H$. We call G/H the **quotient group** of G by H.

When G is abelian, every subgroup H of G is normal, hence we can always form the quotient group G/H. For instance, $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ for any positive integer n. We have already discussed the quotient group is

$$\mathbb{Z}/n = \mathbb{Z}/n\mathbb{Z} \; .$$

For any group G, the quotient by the trivial subgroup 1 is an isomorphic copy of G. That is, $G/1 \cong G$. At the other extreme, the quotient of G by G is trivial, $G/G \cong 1$.

Now let us look at the quotients of the smallest non-abelian group, namely S_3. As a special case of the observations in the previous paragraph, $S_3/1 \cong S_3$ and $S_3/S_3 \cong 1$.

Since $\langle a \rangle$ is the unique subgroup of S_3 isomorphic to S_3, let us write $C_3 = \langle a \rangle$. Since $|S_3/C_3| = 2$ and every group with order 2 is cyclic, we have

$$S_3/C_3 \cong C_2 \; .$$

It was okay to speak of the subgroup C_3 of S_3, because of the uniqueness. But S_3 has 3 distinct subgroups with order 2. We can, of course, pick one of them and write, say $C_2 = \langle b \rangle$. Anyway, none of the C_2 subgroups of S_3 is normal. We cannot form a quotient group of S_3 by any of the C_2 subgroups. It is informative to see what goes wrong when we try: put $H = \langle b \rangle = \{1, b\}$. According to the formula for multiplying cosets, the product of the left cosets aH and a^2H perhaps ought to be $a^3H = H$. But $aH = \{a, ab\} = abH$ and $a^2H = \{a^2, a^2b\}$. We have $ab.a^2b = a^2$. So, according to the formula, the product of aH and a^2H perhaps ought to be a^2H. Yet $H \neq a^2H$. The point, here, is that when H is a non-normal subgroup of G, the formula for the product of two cosets is not well-defined.

Homomorphisms: We have already discussed homomorphisms of abelian groups and isomorphisms of arbitrary groups. We now generalize both of those notions.

Given groups F and G, we define a **homomorphism** $F \leftarrow G$ to be a function $\theta : F \leftarrow G$ such that

$$\theta(xy) = \theta(x)\theta(y)$$

for all $x, y \in G$. Proof of the next remark is easy. It is much the same as for abelian groups. But let us write it out again, now using multiplicative notation.

Lemma 5.6: *Let F and G be groups. Let $\theta : F \leftarrow G$ be a homomorphism. Then $\theta(1_G) = 1_F$ and, for all $g \in G$, we have $\theta(g)^{-1} = \theta(g^{-1})$.*

Proof: The first required equality holds because $\theta(1)^2 = \theta(1^2) = \theta(1)$. The second holds because $\theta(g)\theta(g^{-1}) = \theta(g.g^{-1}) = \theta(1) = 1$. □

For such θ, we again define the **image** of θ as a function in the usual way, $\mathrm{im}(\theta) = \{\theta(g) : g \in G\}$. We again define the **kernel** of θ to be

$$\ker(\theta) = \{g \in G : \theta(g) = 1\} \; .$$

The next result says that the image is a subgroup, the kernel is a normal subgroup.

Lemma 5.7: *Let F and G be groups. Let $\theta : F \leftarrow G$ be a homomorphism. Then* $\mathrm{im}(\theta) \leq F$ *and* $\ker(\theta) \trianglelefteq G$.

The First Isomorphism Theorem: In this section and the next two, we generalize the three isomorphism theorems that we previously proved for abelian groups. The arguments are much the same as before except that, this time around, we have to be careful over the treatment of normality. Actually, most of the new difficulty is in formulating the theorems correctly. Once that has been done, the earlier proofs carry over without much change.

Theorem 5.8: (First Isomorphism Theorem for Groups:) *Let F and G be groups. Let $\theta : F \leftarrow G$ be a homomorphism. Then* $\ker(\theta) \trianglelefteq G$ *and* $\mathrm{im}(\theta) \leq F$*. Moreover,*

$$\mathrm{im}(\theta) \cong G/\ker(\theta) \ .$$

In fact, there is a group isomorphism $\Theta : \mathrm{im}(\theta) \leftarrow G/\ker(\theta)$ *given by* $\Theta(g\ker(\theta)) = \theta(g)$.

Proof: Let $K = \ker(\theta)$. Plainly, $\mathrm{im}(\theta) \leq F$ and $K \leq G$. Given $g \in G$ and $k \in K$, then $\theta({}^g k) = {}^{\theta(g)}1 = 1$. So $\theta({}^g K) = \{1\}$ and ${}^g K \leq K$. Similarly, $K^g \leq K$, hence $K = {}^g(K^g) \leq {}^g K$. We have shown that $K = {}^g K$. Since g is arbitrary, $K \trianglelefteq G$.

It is straightforward to check that the Θ is a well-defined homomorphism. Plainly, Θ is surjective. Given $g, g' \in G$ such that $\Theta(gK) = \Theta(g'K)$, then $\theta(g) = \theta(g')$, hence

$$1 = \theta(g)^{-1}\theta(g') = \theta(g^{-1})\theta(g') = \theta(g^{-1}g') \ .$$

So $g^{-1}g' \in K$ and $gK = g'K$. We have shown that Θ is injective, hence bijective. $\square$

To see an example, consider the automorphism group $\mathrm{Aut}(G)$. We define a function

$$\alpha \ : \ \mathrm{Aut}(G) \leftarrow G$$

given by $\alpha(g) = \alpha_g$, where α_g is the automorphism of G such that $\alpha_g(x) = {}^g x$ for $x \in G$. We call those automorphisms the **inner automorphisms** of G. The set $\mathrm{Inn}(G)$ of inner automorphisms of G is, by Lemma 5.7, a subgroup of $\mathrm{Aut}(G)$. The kernel is $\ker(\alpha) = Z(G)$. We have already noted, in Remark 5.5, that $Z(G)$ is a normal subgroup of G.

Corollary 5.9: *For any group G, we have an isomorphism* $\mathrm{Inn}(G) \cong G/Z(G)$.

Proof: This follows immediately from the First Isomorphism Theorem. $\square$

The Second Isomorphism Theorem: Given subgroups E and F of a group G, we define $EF = \{ef : e \in E, f \in F\}$. In general, EF need not be a subgroup. A small part of the next result says that, if at least one of E or F is normal in G, then EF is a subgroup.

Theorem 5.10: (Second Isomorphism Theorem for Groups:) *Let $H \leq G \trianglerighteq K$ be groups. Then $K \trianglelefteq HK \leq G$ and $H \cap K \trianglelefteq H$, furthermore,*

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

In fact, there is an isomorphism $HK/K \leftarrow H/(H \cap K)$ given by $hK = h(H \cap K)$ for $h \in H$.

Proof: Using closure of multiplication and inversion as a criterion for a subset to be a subgroup, it is clear that $K \leq HK \leq G$ and $H \cap K \leq H$. Using the definition of a normal subgroup in terms of conjugation, it is also clear that $K \trianglelefteq HK$ and $H \cap K \trianglelefteq H$. The homomorphism $HK/K \leftarrow H$ given by $hK \leftarrowtail h$ has kernel $K \cap H$. The required conclusion now follows from the First Isomorphism Theorem. □

The Third Isomorphism Theorem: The next result says that, under suitable circumstances, quotienting out by a normal subgroup and then quotienting out by another normal subgroup is the same as quotienting out all at once by a larger normal subgroup.

Theorem 5.11: (Third Isomorphism Theorem for Groups:) *Let $E \trianglelefteq F \trianglelefteq G$ be groups with $E \trianglelefteq G$. Then $F/E \trianglelefteq G/E$ and*

$$G/F \cong (G/E)/(F/E) \ .$$

In fact, there is a group isomorphism $(G/F) \leftarrow (G/E)/(F/E)$ given by $gF \leftarrowtail gE(F/E)$ for $g \in G$.

Proof: Plainly, $F/E \leq G/E$. Given $f \in F$ and $g \in G$, then ${}^g f \in F$. Hence, ${}^{gE}(fE) = ({}^g f)E \in F/E$. So $F/E \trianglelefteq G/E$. The homomorphism $G/F \leftarrow G/E$ given by $gF \leftarrowtail gE$ has kernel F/E. Again, the required conclusion follows from the First Isomorphism Theorem. □

The Direct Product Recognition Theorem: Given groups U and V, we make the direct product $U \times V$ become a group such that

$$(u, v)(u', v') = (uu', vv')$$

for $u, u' \in U$ and $v, v' \in V$.

Now suppose that U and V are normal subgroups of a group G. Then the set $UV = \{uv : u \in U, v \in V\}$ is subgroup of G, indeed, $uvu'v' = uvu'v^{-1}vv'$ and we have $uvu'v^{-1} \in U$ and $vv' \in V$. In fact, UV is a normal subgroup of G, since ${}^g(uv) = {}^g.{}^g v$ for all $g \in G$.

Theorem 5.12: (Direct Product Recognition Theorem.) *Let U and V be normal subgroups of a group G such that $U \cap V = \{1\}$. Then*

$$UV \cong U \times V \ .$$

in fact, there is an isomorphism $\theta : UV \leftarrow U \times V$ given by $\theta(u, v) = uv$.

Proof: Given $u \in U$ and $v \in V$, then $vu^{-1}v^{-1} \in U$, hence $uvu^{-1}v^{-1} \in U$. Also, $uvu^{-1} \in V$, hence $uvu^{-1}v^{-1} \in V$. Therefore, $uvu^{-1}v^{-1} = \{1\}$, in other words, $uv = vu$.

Given $u_1, u_2 \in U$ and $v_1, v_2 \in V$, then

$$\theta((u_1, v_1)(u_2, v_2)) = \theta(u_1 u_2, v_1 v_2) = u_1 u_2 v_1 v_2 = u_1 v_1 u_2 v_2 = \theta(u_1, v_2)\theta(u_2, v_2) \ .$$

Thus, θ is a homomorphism. Plainly, θ is surjective. Given $u \in U$ and $v \in V$ such that $(u, v) \in \ker(\theta)$, then $u = v^{-1} \in U \cap V$, so $(u, v) = (1, 1)$. Therefore θ is injective. In conclusion, θ is an isomorphism. □

In the context of the theorem, the subgroup UV is sometimes called an **internal direct product**, whereas the abstract constrauction $U \times V$ is called the **external direct product**.