ISOMORPHISM THEOREMS AND COMPOSITION SERIES

COLTON GRAINGER (MATH 6130 ALGEBRA)

5. Assignment due 2018-10-03

5.1. **[1, No. 3.3.6].** Let $M = \langle u, v : u^2 = v^8 = 1, vu = uv^5 \rangle$ be the modular group of order 16.

To show the subgroup $\langle v^4 \rangle$ is normal in M, we conjugate the generator v^4 by the generators u, v in M.

- $uv^4u^{-1} = uv^4u = u^2v^{20} = v^4$
- $vv^4v^{-1} = v^4$
- $N_M(\langle v^4 \rangle)$ contains $< u, v >= M$ by closure.

Since $\langle v^4 \rangle$ is normal in M, the quotient group $M/\langle v^4 \rangle$ is well defined. By the lattice isomorphism theorem, the lattice of subgroups of $M/\langle v^4 \rangle$ order isomorphic to the lattice pictured below (where the order isomorphism maps each subgroup to itself mod $\langle v^4 \rangle$).

```
                  M
                / | \
               /  |  \
              /   |   \
             /    |    \
       <u,v^2>   <v>    <uv>
       /  |  \    |    /
      /   |   \   |   /
     /    |    \  |  /
    /     |     \ | /
<u,v^4>  <uv^2>  <v^2>
    \     |     /
     \    |    /
      \   |   /
       \  |  /
        <v^4>
```

In the previous assignment, we proved that $Z_2 \times Z_4 \cong \bar{M} = M/\langle v^4 \rangle$ by defining an isomorphism between the two groups. We can also prove $Z_2 \times Z_4 \cong \bar{M}$ by mapping the generators $\bar{u}$ and $\bar{v}$ of $\bar{M}$ to $Z_2 \times Z_4$ and showing that $\bar{u}$ and $\bar{v}$ satisfy the relations on $Z_2 \times Z_4$. By the fourth isomorphism theorem, $\bar{M} = \overline{\langle u, v \rangle} = \langle \bar{u}, \bar{v} \rangle$. Now note

- $|\bar{u}| = 2$,
- $|\bar{v}| = 4$, and
- $\bar{u}\bar{v} = \bar{v}\bar{u}$.

So $\langle \bar{u}, \bar{v} \rangle \cong Z_2 \times Z_4$.

5.2. **[1, No. 3.3.7].** Let M and N be subgroups normal in G such that $G = MN$.

Considering the lattice of G, we have that $G/(M \cap N) \cong (G/M) \times (G/N)$.

Date: 2018-09-29.
Compiled: 2018-10-03.

```
       MN      (NM = G)
     /  \
    /    \
  M       N
    \    /
     \  /
  M \cap N
```

Proof. Since the intersection of subgroups normal in G is also a subgroup normal in G, we have $M \cap N \triangleleft G$. Further, since $M \leq G$ and $N \leq G$, it follows that $M \cap N \triangleleft M$ and $M \cap N \triangleleft N$.

Now to show $G/N \cong M/(M \cap N)$. Define an epimorphism $\varphi\colon M \to G/N$ by $\varphi(m) = mN$. Note φ is a homomorphism because it's the restriction to M of the natural homomorphism from G to G/N. Note also that φ is surjective as for all $gN \in G/N$, we can write $g = mn$, so there's $m \in M$ such that $mN = mnN = gN$. An element $m \in M$ is in the kernel of φ if $mN = 1N$. It follows that $m \in \ker\varphi$ if and only if $m \in N$, hence $\ker\varphi = M \cap N$. By the first isomorphism theorem,

$$M/(M \cap N) \cong G/N.$$

Repeating this argument, one may find $N/(M \cap N) \cong G/M$.

Proceeding, define an epimorphism $\psi\colon G \to (G/M) \times (G/N)$ given by $mn \mapsto nM \times mN$. Because every element of $G = MN$ is of the form mn, ψ is well defined. ψ is clearly surjective. Lastly, because ψ is in its coordinates the restriction of natural homomorphisms, we expect ψ will be a homomorphism. To wit:

$$\begin{aligned}
\psi(mn)\psi(\mu\nu) &= (nM \times mN)(\nu M \times \mu N) \\
&= (nM\nu M \times mN\mu N) \\
&= (n\nu M \times m\mu N) \\
&= \psi((m\mu)(n\nu)) \\
&= \psi(m(n\mu')\nu) && \text{for some } \mu' \in M \text{ since } M \triangleleft G \\
&= \psi((mn)(\mu\nu)) && \text{(why?)}
\end{aligned}$$

where from $\mu N = N\mu'$ and $N \triangleleft G$ one deduces that $\mu N = \mu' N$. To obtain the desired isomorphism, observe $nM \times mN = 1M \times 1N$ if and only if both $m \in N$ and $n \in M$, so the kernel of ψ is $M \cap N$. By the first isomorphism theorem, we conclude $G/(M \cap N) \cong (G/N) \times (G/M)$. □

5.3. **[1, No. 3.3.9].** Let p be a prime and let G be a group of order $p^a m$ where p does not divide m. Further, let P be a subgroup[1] of G of order p^a and N is a normal subgroup of G order $p^b n$, where p does not divide n. Then $|P \cap N| = p^b$ and $|PN/N| = p^{a-b}$.

Proof. As $P \leq N_G(N) = G$, by the third isomorphism theorem $PN \leq G$. We deduce $|PN| = p^a k$ where $k|m$ and $n|k$ from Lagrange's theorem for, respectively, $PN \leq G$ together with $P \leq PN$ for $k|m$, and $N \leq PN$, for $n|k$. By the orbit stabilizer theorem,

$$|PN| = \frac{|P|\,|N|}{|P \cap N|}.$$

Hence

$$|P \cap N| = \frac{|P|\,|N|}{|PN|} = \frac{p^a p^b n}{p^a} = p^b \frac{n}{k} = p^b,$$

where the equality $n/k = 1$ is justified: $n|k$ implies $\frac{n}{k} \leq 1$, yet k does not divide p, where $|P \cap N|$ must be a natural number.

Appealing to the third isomorphism theorem, $PN/N \cong P/(P \cap N)$ hence $|PN/N| = \frac{|P|}{|P \cap N|} = p^{a-b}$. □

[1]The subgroup P of G is called a *Sylow p-subgroup* of G. Hence, the intersection of any Sylow p-subgroup of G with a normal subgroup N is a Sylow p-subgroup of N.

5.4. **[1, No. 3.3.10].** A subgroup H of a finite group G is called a *Hall subgroup* of G if its index in G is relatively prime to its order: $(|G : H|, |H|) = 1$. If H is a Hall subgroup of G and $N \trianglelefteq G$, then $H \cap N$ is a Hall subgroup of N and HN/N is a Hall subgroup of G/N.

Proof.[2] First, since $H \cap N \leq H \leq G$ it's true that $|H \cap N|$ divides $|H|$. Second, observe $|N : H \cap N| = |HN : H| = \frac{|G:H|}{|G:HN|}$ divides $|G : H|$. (We have $H \leq N_G(N) = G$, so by the second isomorphism theorem $|G : HN|$ is an integer.) By assumption, H is a Hall subgroup of G, so we must have that $(|N : H \cap N|, |H \cap N|) = 1$.

Now $|HN/N| = |H : H \cap N|$ must divide $|H|$. Also

$$\left|\frac{G}{N} : |HN|\,N\right| = \left|\frac{G}{HN}\right| = \left|\frac{G : H}{HN : H}\right|$$

must divide $|G : H|$. Again, because H is a Hall subgroup of G, we conclude $(|G/N : HN/N|, |HN/N|) = 1$. □

5.5. **[1, No. 3.4.2].** We exhibit all 3 composition series for Q_8 and all 7 composition series for D_8. We list the composition factors in each case.

Demonstration. By inspection, Q_8 has composition series

- $Q_8 \triangleright \langle i \rangle \triangleright \langle -1 \rangle \triangleright 1$
- $Q_8 \triangleright \langle j \rangle \triangleright \langle -1 \rangle \triangleright 1$
- $Q_8 \triangleright \langle k \rangle \triangleright \langle -1 \rangle \triangleright 1$
- each with factors Z_2, Z_2, Z_2.

On the other hand, D_8 has composition series

- $D_8 \triangleright \langle s, r^2 \rangle \triangleright \langle s \rangle \triangleright 1$
- $D_8 \triangleright \langle s, r^2 \rangle \triangleright \langle r^2 s \rangle \triangleright 1$
- $D_8 \triangleright \langle s, r^2 \rangle \triangleright \langle r^2 \rangle \triangleright 1$
- $D_8 \triangleright \langle r \rangle \triangleright \langle r^2 \rangle \triangleright 1$
- $D_8 \triangleright \langle rs, r^2 \rangle \triangleright \langle r^2 \rangle \triangleright 1$
- $D_8 \triangleright \langle rs, r^2 \rangle \triangleright \langle r^2 \rangle \triangleright 1$
- $D_8 \triangleright \langle rs, r^2 \rangle \triangleright \langle rs \rangle \triangleright 1$
- $D_8 \triangleright \langle rs, r^2 \rangle \triangleright \langle r^3 s \rangle \triangleright 1$
- each with factors Z_2, Z_2, Z_2.

5.6. **[1, No. 3.4.7].** If G is a finite group and $H \trianglelefteq G$, then there is a composition series of G one of whose terms in H. TODO

5.7. **[1, No. 3.4.11].** If H is a nontrivial normal subgroup of the solvable group G, then there is a nontrivial subgroup A of H with $A \trianglelefteq G$ and A abelian. TODO

5.8. **[1, No. 3.5.6].** The group $H = \langle (1\,3), (1\,2\,3\,4) \rangle$ is a proper subgroup of S_4. We give the isomorphism type of H. TODO

5.9. **[1, No. 3.5.10].** We find a composition series for A_4, and argue that A_4 is not solvable. TODO

[2] See also `https://math.stackexchange.com/questions/811039`.

5.10. **[1, No. 4.1.7].** Let G be a transitive permutation group on the finite set A. A *block* is a nonempty subset B of A such that for all $\sigma \in G$ either $\sigma(B) = B$ or $\sigma(B) \cap B = \varnothing$ (where $\sigma(B)$ is the set $\{\sigma(b) : b \in B\}$).

(a) If B is a block containing the element a of A, then the set $\mathrm{Stab}_G(B)$ defined by $\{\sigma \in G : \sigma(B) = B\}$ is a subgroup of G containing $\mathrm{Stab}_G(a)$.

Proof. Let $\sigma, \tau \in \mathrm{Stab}_G(B)$. To satisfy the subgroup criterion, we want to show that $\sigma\tau^{-1} \in \mathrm{Stab}_G(B)$. Well $\sigma(B) = B$ and $\tau(B) = B$. So $\tau^{-1}(B) = B$. Now B is stabilized under τ^{-1}, then under σ. By definition of a group action, $\sigma\tau^{-1}(B) = (\sigma \circ \tau^{-1})(B) = B$. Therefore $\sigma\tau^{-1} \in \mathrm{Stab}_G(B)$.

Now to verify $\mathrm{Stab}_G(a) \leq \mathrm{Stab}_G(B)$. For $a \in B$, let $\nu \in \mathrm{Stab}_G(a)$. Then $\nu(a) = a \in B$. Assuming B is a block, we require either $\nu(B) = B$ or $\nu(B) \cap B = \varnothing$. Observing $a = \nu(a) \in \nu(B) \cap B$, it must be that $\nu(B) = B$. We conclude $\nu \in \mathrm{Stab}_G(B)$. □

(b) If B is a block and $\sigma_1(B), \sigma_2(B), \ldots, \sigma_n(B)$ are *all* the distinct images of B under the elements of G, then these form a partition of A.

Proof. To show by contrapositive that distinct images of B are disjoint. Suppose $\sigma, \tau \in G$ such that $a \in \sigma(B) \cap \tau(B)$. Then $\tau^{-1}(a) \in (\tau^{-1} \circ \sigma)(B) \cap B$. Because B is a block we must have that $(\tau^{-1} \circ \sigma)(B) = B$. Hence $\sigma(B) = \tau(B)$.

Now to show the union of the distinct images of B is the whole of A. It suffices to argue that if $a \in A$, there exists $j \in \{1, \ldots, n\}$ such that $a \in \sigma_j(B)$. Because G is transitive, there's *some* $\tau \in G$ such that $a \in \tau(B)$. Is τ one of the σ_i? For contradiction, suppose not. Then a is a point in the set $A \setminus \cup_1^n \sigma_i(B)$. Since G is transitive, we can map an element of B to a under the permutation ω. Because distinct images are disjoint, and we have an image $\omega(B)$ disjoint from each of $\sigma_1(B), \ldots, \sigma_n(B)$; but the $\sigma_i(B)$ are *all* the distinct images of B, a contradiction. Therefore τ is one of the σ_i. □

(c) A (transitive) group G on a set A is said to be *primitive* if the only blocks in A are the trivial ones, the sets of size 1 and $|A|$. We demonstrate that S_4 is primitive on $A = \{1, 2, 3, 4\}$. Further, D_8 is not primitive as a permutation group on the four vertices of a square.

Demonstration. Suppose, for contradiction, I have a block of size 2 or 3 in $\{1, 2, 3, 4\}$. Since S_4 is transitive and contains all permutations of $\{1, 2, 3, 4\}$, there's a $\sigma \in S_4$ that maps one element in the block outside the block, fixing the other(s). Whence the only possible blocks have size 1 and 4. (It is trivial to check that indeed the singleton subsets of A and the whole of A are blocks.) So S_4 is primitive on A.

On the other hand, when D_8 acts on A, we have the nontrivial blocks $\{1, 3\}$ and $\{2, 4\}$. To verify, the images of the blocks under action by the generators of r and s of D_8 are given

- $r(\{1, 3\}) = \{2, 4\}$ and $r(\{2, 4\}) = \{1, 3\}$,
- $s(\{1, 3\}) = \{1, 3\}$ and $s(\{2, 4\}) = \{2, 4\}$.

Now any element of D_8 is a finite product of these two generators, whose action on B can be decomposed into repeated applications of the maps above. We conclude $\{1, 3\}$ and $\{2, 4\}$ are blocks under the action of D_8. □

(d) The transitive group G is primitive on A if and only if for each $a \in A$, the only subgroups of G containing $\mathrm{Stab}_G(a)$ are $\mathrm{Stab}_G(a)$ and G (i.e., $\mathrm{Stab}_G(A)$ is a *maximal* subgroup of G).

Proof. ($\Rightarrow$) Suppose for all $a \in A$ that $\mathrm{Stab}_G(a)$ is a maximal subgroup of G. We know if B is a block containing a, then $\mathrm{Stab}_G(a) \leq \mathrm{Stab}_G(B)$. But then either $\mathrm{Stab}_G(B) = G$ or $\mathrm{Stab}_G(B) = \mathrm{Stab}_G(a)$. In the former case we have that every $g \in G$ stabilizes B, and given that G acts transitively on $A \supset B$, we must have $B = A$. In the later case we have that exactly those elements of g that stabilize $\{a\}$ also stabilize B, and further, since G acts transitively on $A \setminus \{a\}$ if B is to be stabilized by $g \in \mathrm{Stab}_G(a)$ then $B \subset \{a\}$. Since $B \neq \varnothing$, we have $B = \{a\}$. Whence G is primitive on A.

($\Leftarrow$) Suppose now that G is primitive of A. We set out to argue if H is a subgroup such that $\mathrm{Stab}_G(a) \leq H \leq G$, then either $H = \mathrm{Stab}_G(a)$ or $H = G$. Consider $a \in A$. I claim $H(a)$ is a block. Why? Let $g \in G$. Let

$$g(H(a)) = \{(gh)(a) : h \in H\}.$$

Since the cosets of H partition G, either $gH = H$ or $gH \cap H = \varnothing$. In the former case $g(H(a)) = H(a)$ and in the later $g(H(a)) \cap H(a) = \varnothing$. To verify the later, suppose $g(H(a)) \cap H(a) \neq \varnothing$. Then there exist $h, k \in H$ such that $gh(a) = k(a)$, hence $ghk^{-1}(a) = a$, hence $ghk^{-1} \in \mathrm{Stab}_G(a) \leq H$. It follows that $g \in H$ and so too $gH = H$, but we've already identified this as the former case $g(H(a)) = H(a)$. Therefore $H(a)$ is a block.

Because G is primitive, the block $H(a)$ is either A or $\{a\}$. Because G is *transitive*, we are forced to accept that $H(a) = A$ implies $H = G$, and likewise that $H(a) = \{a\}$ implies $H = \mathrm{Stab}_G(a)$. □

5.11. **[1, No. 4.1.9].** Assume G acts transitively on the finite set A and let H be a normal subgroup of G. Let $\mathscr{O}_1, \mathscr{O}_2, \ldots, \mathscr{O}_r$ be the distinct orbits of H on A.

(a) G permutes the sets $\mathscr{O}_1, \mathscr{O}_2, \ldots, \mathscr{O}_r$ in the sense that for each $g \in G$ and each $i \in \{1, \ldots, r\}$ there is a j such that $g\mathscr{O}_i = \mathscr{O}_j$, where $g\mathscr{O} = \{g(a) : a \in \mathscr{O}\}$. Then G is transitive on $\{\mathscr{O}_1, \ldots, \mathscr{O}_r\}$. Furthermore, all orbits of H on A have the same cardinality.

Proof. We'll immediately show that G permutes the $\mathscr{O}_i$. Let $g \in G$ and $i \in \{1, \ldots, r\}$. Then

$$\begin{aligned}
g\mathscr{O}_i &= gH(a) && \text{for some } a \in A \\
&= \{g(h(a)) : h \in H\} \\
&= \{(gh)(a) : h \in H\} \\
&= \{(h'g)(a) : h' \in H\} && \text{as } H \triangleleft G \text{, so } gH = Hg \\
&= \{h'(g(a)) : h' \in H\} \\
&= \{h'(b) : h' \in H\} && g(a) = b\text{, noting } G \text{ acts transitively} \\
&= H(b) \\
&= \mathscr{O}_j
\end{aligned}$$

Now, G not only permutes the orbits $\mathscr{O}_i$, but acts *transitively* on them. To justify:

- Given any $a, b \in A$, we can find a $g \in G$ such that $gH(a) = H(b)$.
- The map $A \to \{\mathscr{O}_i\}_1^r$ defined $a \mapsto H(a)$ is a surjection.
- So given any $\mathscr{O}_i$, we can find $g \in G$ such that $g\mathscr{O}_i = \mathscr{O}_j$.

To show $\left|\mathscr{O}_j\right| = |\mathscr{O}_i|$ we appeal to the second isomorphism theorem. Its hypotheses are met: G has subgroups H and $\mathrm{Stab}_G(a)$, with $\mathrm{Stab}_G(a) \leq N_G(H) = G$ (note also that $\mathrm{Stab}_G(a) \cap H = \mathrm{Stab}_H(a)$). Therefore $H\mathrm{Stab}_G(a)/H \cong \mathrm{Stab}_G(a)/\mathrm{Stab}_H(a)$. Now by the orbit stabilizer theorem (noting H also acts on A),

$$|H(a)| = \frac{|H|}{|\mathrm{Stab}_H(a)|} = \frac{|H\mathrm{Stab}_G(a)|\,|H|}{|\mathrm{Stab}_G(a)|\,|H|} = \frac{|H\mathrm{Stab}_G(a)|}{|\mathrm{Stab}_G(a)|}.$$

Since G acts transitively on A, it seems[3] that size of the stabilizer $\mathrm{Stab}_G(a)$ is constant for any $a \in A$. Assuming this is the case, then the cardinality of each orbit $H(a)$ is constant with respect to the choice of element $a \in A$. Therefore the orbits $\mathscr{O}_i$ are all of the same cardinality. □

(b) If $a \in \mathscr{O}_1$, then $|\mathscr{O}_1| = |H : H \cap \mathrm{Stab}_G(a)|$. Furthermore, $r = |G : H\mathrm{Stab}_G(a)|$.

Proof. The first assertion is justified in part (a), given that $|H : H \cap \mathrm{Stab}_G(a)| = \frac{|H|}{|\mathrm{Stab}_H(a)|}$ by the second isomorphism theorem.

The second assertion requires us to count the number of orbits of H on A. I am guessing this an application of Burnside's lemma, the "orbit counting theorem", but I don't see how to approach a proof.

[3] How would one go about proving this?

References

[1] D. S. Dummit and R. M. Foote, *Abstract algebra*, 3rd ed. Hardcover; Prentice Hall, 2004 [Online]. Available: http://www.worldcat.org/isbn/0471433349