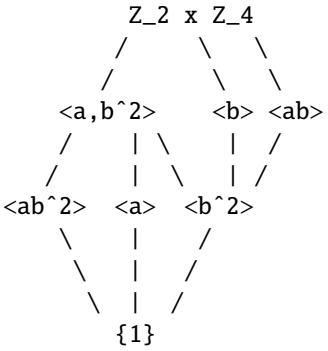
QUOTIENT GROUPS

COLTON GRAINGER (MATH 6130 ALGEBRA)

4. Assignment due 2018-09-26

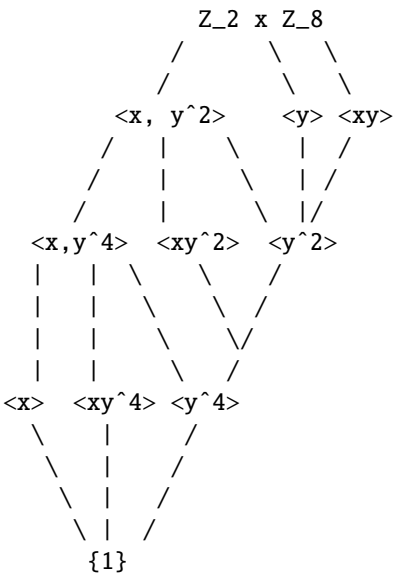
4.1. **[1, No. 2.5.12].** The group $Z_2 \times Z_4 = \langle a, b | a^2 = b^4 = 1, ab = ba \rangle$ of order 8 has three subgroups of order 4. They are $\langle a, b^2 \rangle \cong V_4$, $\langle b \rangle \cong Z_4$, and $\langle ab \rangle \cong Z_4$.

Here's the lattice[1] of subgroups of $Z_2 \times Z_4$, with each subgroup expressed in terms of at most two generators.



4.2. **[1, No. 2.5.13].** The group $Z_2 \times Z_8 = \langle x, y : x^2 = y^8 = 1, xy = yx \rangle$ has order 16 has three subgroups of order 8. They are $\langle x, y^2 \rangle \cong Z_2 \times Z_4$, $\langle y \rangle \cong Z_8$, and $\langle xy \rangle \cong Z_8$.

Here's the lattice of subgroups of $Z_2 \times Z_8$.



Date: 2018-09-19.

Compiled: 2018-09-28.

[1] TODO, use TikZ. See, e.g., https://tex.stackexchange.com/questions/47392/how-to-draw-a-poset-hasse-diagram-using-tikz or https://ctan.math.washington.edu/tex-archive/graphics/pgf/contrib/tikz-cd/tikz-cd-doc.pdf.

4.3. **[1, No. 2.5.14].** Let M be the (*modular*) group of order 16 with the following presentation:

$$\langle u, v : u^2 = v^8 = 1, vu = uv^5 \rangle$$

M has three subgroups of order 8, they are

$\langle u, v^2 \rangle$, $\langle v \rangle$, $\langle uv \rangle$.

One can show the lattice of subgroups of M is the same as the lattice of subgroups of $Z_2 \times Z_8$, replacing everywhere x with u and y with v.

However, $Z_2 \times Z_8$ is abelian but M is not. Hence the two groups are not isomorphic.

4.4. **[1, No. 3.1.11].** Let $\mathbf{F}$ be a field and consider the subgroup of upper triangular matrices in $GL_2(\mathbf{F})$,

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbf{F}, ac \neq 0 \right\}.$$

Note that for all $A, B \in G$ we have

$$AB = \begin{pmatrix} a & b \\ & c \end{pmatrix} \begin{pmatrix} d & e \\ & f \end{pmatrix} = \begin{pmatrix} ad & b+e \\ & cf \end{pmatrix}.$$

(a) The map $\varphi : \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto a$ is a surjective homomorphism from G onto $\mathbf{F}^\times$ (the multiplicative group of nonzero elements in $\mathbf{F}$). We describe the fibers and kernel of φ.

- φ is well defined and onto, noting $A_{1,1} \in \mathbf{F}^\times$ for all $A \in G$.
- φ is a homomorphism as for all $A, B \in G$ we have that $\varphi(AB) = A_{1,1}B_{1,1} = \varphi(A)\varphi(B)$.
- For $x \in \mathbf{F}^\times$ we have

$$\varphi^{-1} = \left\{ \begin{pmatrix} x & b \\ & c \end{pmatrix} c \neq 0 \right\},$$

in particular $\ker \varphi = \left\{ \begin{pmatrix} 1 & b \\ & c \end{pmatrix} c \neq 0 \right\}$

(b) The map $\psi : \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto (a, c)$ is a surjective homomorphism from G onto $\mathbf{F}^\times \times \mathbf{F}^\times$. We describe the fibers and kernel of ψ.

- φ again is well defined and onto.
- φ is a homomorphism as for all $A, B \in G$ we have that

$$\varphi(AB) = (A_{1,1}B_{1,1}, A_{2,2}B_{2,2}) = (A_{1,1}, A_{2,2}) \cdot (B_{1,1}, B_{2,2}) = \varphi(A)\varphi(B).$$

- For $(x, y) \in \mathbf{F}^\times \times \mathbf{F}^\times$, note $\varphi^{-1} \left\{ \begin{pmatrix} x & b \\ & y \end{pmatrix} \right\}$ and in particular $\ker \varphi = \left\{ \begin{pmatrix} 1 & b \\ & 1 \end{pmatrix} \right\}$.

(c) Let H be the subgroup of unit upper triangular matrices[2] in $GL_2(\mathbf{F})$. Then $H \cong \mathbf{F}$ (the additive group).

- Consider the map $\varphi \colon H \to \mathbf{F}$ defined by $\begin{pmatrix} 1 & b \\ & 1 \end{pmatrix} \mapsto b$.
- Here φ is well defined and onto.
- For $A, B \in H$, note that $\varphi(AB) = A_{1,2} + B_{1,2} = \varphi(A) + \varphi(B)$, so φ is a homomorphism.
- Lastly, observe $\ker \varphi = \begin{pmatrix} 1 & 0 \\ & 1 \end{pmatrix}$, whence the kernel is trivial and φ is an isomorphism.
- We conclude that $H \cong \mathbf{F}$.

[2] A *unit* upper triangular matrix is an upper triangular matrix with 1 in each diagonal entry. In the 2×2 case, the unit upper triangular matrices are completely determined by the element $b \in \mathbf{F}$ in row 1, column 2. The isomorphism should be clear.

4.5. **[1, No. 3.1.19].** Let M be the modular group of order 16 and let $\overline{M} = M/\langle v^4\rangle$ be the quotient of M by the (normal) subgroup generated by v^4.

(a) The order of $\overline{M}$ is 8. Consider that the order of $\langle v^4\rangle$ in M is 2, whence there are 8 left cosets of $\langle v^4\rangle$ in M, and these cosets are the distinct elements of $\overline{M}$.

(b) Each element of $\overline{M}$ is of the form $\overline{u}^a\overline{v}^b$ for some integers a and b. Why? Suppose $\overline{x} \in \overline{M}$, then $\overline{x}$ is a coset of $\langle v^4\rangle$ in M. If x is a representative of $\overline{x} = \{x, xv^4\}$. Suppose $x = u^a v^c$ (any element of M can be written in such form). To take advantage of the quotient structure, notice that $u^a v^{c+4}\{1, v^4\} = u^a v^c\{v^4, 1\}$. Generalizing, we write $\overline{x} = \overline{u}^a\overline{v}^b$ where b is the least residue of c modulo 4.

(c) The order of each of the elements in part (b) is given.

- $\overline{v}$, $\overline{uv}$, $\overline{v}^3$, $\overline{uv}^3$ of order 4
- $\overline{u}$, $\overline{v}^2$, $\overline{uv}$, $\overline{uv}^2$ of order 2
- $\overline{1}$ the identity

(d) We reduce the following elements of $\overline{M}$ to their "least residue" (i.e., to the form $\overline{u}^a\overline{v}^b$).

- $\overline{vu} = \overline{uv}$
- $\overline{uv^{-2}u} = \overline{v}^2$
- $u^{-1}v^{-1}uv = \overline{1}$

(e) $\overline{M} \cong Z_2 \times Z_4$. How come? Let $\varphi\colon \overline{M} \to Z_2 \times Z_4$ be defined by $\varphi(\overline{u}^a\overline{v}^b) = (a, b)$.

- φ is here well defined and surjective, for there's a $\overline{u}^a\overline{v}^b$ for each $a \in \{0, 1\}$ and $b \in \{0, 1, 2, 3\}$.
- φ is a homomorphism when we consider at multiplication of $\overline{x}$ in $\overline{M}$ is addition in the exponents.
- Now $\ker\varphi = \{\overline{u}^0, \overline{v}^0\}$ is trivial.
- Whence φ is an isomorphism of groups.

4.6. **[1, No. 3.1.22].**

(a) If H and K are normal subgroups of a group G then their intersection $H \cap K$ is also a normal subgroup of G.

Proof. Let G act on itself by conjugation. What's the normalizer of $H \cap K$ in G? It's $\{g \in G : gxg^{-1} \in H \cap K, \text{ for all } x \in H \cap K\}$.

Both H and K are normal in G, hence $x \in H \cap K$ implies every element g of G conjugates x into H and also K. Therefore the normalizer of $H \cap K$ in G is G itself, hence $H \cap K$ is normal. □

(b) The intersection of an arbitrary nonempty collection of normal subgroups of a group is a normal subgroup.

Proof. Let H_λ be normal in G for all $\lambda \in \Lambda$. Suppose $x \in H_\lambda$ for all λ. Then for every $g \in G$, by normality of H_λ we have $gxg^{-1} \in H_\lambda$. Whence for all $g \in G$, $gxg^{-1} \in \cap H_\lambda$. So the normalizer of $\cap H_\lambda$ in G is G itself. □

4.7. **[1, No. 3.1.36].** If $G/Z(G)$ is cyclic then G is abelian.[3]

Proof. Choose a generator of the cyclic group $G/Z(G)$, say the coset $xZ(G)$ for some $x \in G$. Now let $g \in G$, so the coset $gZ(G) \in G/Z(G) = \langle xZ(G)\rangle$. Hence for some $a \in \mathbf{Z}$ we have $gZ(G) = x^aZ(G)$. By definition of a coset, we have $y, w \in Z(G)$ such that

$$\begin{aligned} gw &= x^a y, && \text{hence} \\ g &= x^a y w^{-1}, && \text{hence} \\ gw &= x^a z, && \text{for } yw^{-1} = z \in Z(G). \end{aligned}$$

Every element of G has such a representation. Now G is abelian because for any two $g, h \in G$, we have $n, m \in Z(G)$ such that $gh = x^a n x^b m = x^{a+b} nm = x^b m x^a n = hg$, exploiting that n, m commute. □

[3] If $G/Z(G)$ is cyclic with generator $xZ(G)$, every element of G can be written in the form $x^a z$ for some integer $a \in \mathbf{Z}$ and some element $z \in Z(G)$.

4.8. **[1, No. 3.1.41].** Let G be a group. Then *commutator subgroup* $N = \langle x^{-1}y^{-1}xy : x, y \in G\rangle$ is a normal subgroup of G, also for which the quotient group G/N is abelian.

Proof. Suppose the word $x_1 \cdots x_n \in N$ and consider an element $g \in G$. We'll conjugate the word by g and show that it lies in the commutator subgroup.

Consider that strategically inserting $g^{-1}g$ into the conjugate word produces $gx_1 \cdots x_n g^{-1} = gx_1g^{-1} \cdots gx_ng^{-1}$. Take the individual segment gx_ig^{-1}, which explodes to $ga_i^{-1}b_i^{-1}a_ib_ig^{-1}$ since x_i is a commutator. Again inserting $g^{-1}g$ into the conjugate of the segment, we have $(ga_ig^{-1})^{-1}(gb_ig^{-1})^{-1}(ga_ig^{-1})(gb_ig^{-1})$ which is itself a commutator in N.

So the conjugate $gx_1 \cdots x_ng^{-1}$ is the product of commutators, and thus in N. We conclude that the normalizer of N is G is all of G, so N is normal in G.

Now to show that G/N is abelian, let $g, h \in G$. Since $g^{-1}h^{-1}gh \in N$, we have $(hg)^{-1}gh \in N$. Thus $(hg)^{-1}ghN = 1N$, and because N is normal we have the equality of cosets $ghN = hgN$. So G/N is abelian.□

4.9. **[1, No. 3.2.4].** A finite abelian group has a subgroup of order n for each positive divisor n of its order.[4]

Proof. We proceed by strong induction on the order of the group.

For small orders of the group G, say $1, 2, 3$ and 4, the claim is obviously true. It's trivial to check for $1, Z_2, Z_3$ and we (exhaustively) list that both Z_4 and V_4 have subgroups of orders $1, 2$ and 4.

Now suppose for all $k \leq |G|$ a finite abelian group of order k has subgroups of order d for every positive integer d such that $d|k$.

Let d be a proper divisor of $n = |G|$. If $d = 1$ the trivial subgroup of G will do. So assume that $d \neq 1$ and choose a prime p in the factorization of d.

Assuming Cauchy's theorem, there's a (cyclic) subgroup $\langle x\rangle$ of G of order p. The subgroup $\langle x\rangle$ is normal in G because $\langle x\rangle$ is abelian.

We have the natural homomorphism $\pi\colon G \to G/\langle x\rangle$, where $|G/\langle x\rangle| = \frac{n}{p}$. By the inductive hypothesis, there's a subgroup H of $G/\langle x\rangle$ of order $\frac{d}{p}$.

Now consider $K = \pi^{-1}(H)$. Since H is a group, the inverse image $K \leq G$ in the domain. The restriction of π to K is a surjective homomorphism onto H with kernel $\langle x\rangle$. Now $K/\langle x\rangle \cong H$ by the first isomorphism theorem, hence

$$\frac{|K|}{|\langle x\rangle|} = |H| \text{ and thus } |K| = \frac{d}{p} \cdot p = d.$$

□

4.10. **[1, No. 3.2.9].** A proof of Cauchy's theorem.[5]

Let G be a finite group and let p be a prime dividing $|G|$. Let $\mathscr{S}$ denote the set of p-tuples of elements of G the product of whose coordinates is 1:

$$S\mathscr{S} = \left\{(x_1, x_2, \ldots, x_p) : x_i \in G \text{ and } x_1x_2 \cdots x_p = 1\right\}.$$

(a) $\mathscr{S}$ has $|G|^{p-1}$ elements, hence has order divisible by p. Why? Of $|G|$ elements, choose $p-1$ with repetitions, and such that the product of the p elements is 1, we must take the unique inverse $x_p = (x_1 \cdots x_{p-1})^{-1}$. So $|\mathscr{S}| = |G|^{p-1}$. By Fermat's little theorem, p divides $|G|^{p-1}$.

For notation's sake, let C_p (considered as a subgroup of the symmetric group on p letters) act on $\mathscr{S}$ by

$$\sigma(x_1, \ldots, x_p) \mapsto (x_{\sigma(1)}, \ldots, x_{\sigma(p)}).$$

[4]Notably, I consulted (1) "If G is abelian, it has a subgroup in every order of $|G|$'s divisors?" `https://math.stackexchange.com/q/1352384/` (2) "every Abelian group is a converse lagrange theorem group" `https://math.stackexchange.com/q/910426/`.

[5]Due to James McKay (*Another proof of Cauchy's group theorem*, Amer. Math. Monthly, 66(1959), p. 119)

Now we identify each cyclic permutation shifting j entries right of every $\alpha \in \mathscr{S}$ with $\sigma^j(\alpha)$ where for $j \in \mathbf{Z}$ σ^j is the p-cycle $(1\,2\,\cdots\,p)^j$. Now the action is faithful, and additionally for all $j \in ZZ$ and all $\alpha \in \mathscr{S}$ we know $\sigma^j(\alpha) \in \mathscr{S}$ since x_p remains nested in cyclic order between $x_{p-1} and x_1$.

Define the relation $\sim$ on $\mathscr{S}$ by letting $\alpha \sim \beta$ if β is a cyclic permutation of α.

(b) We've shown a cyclic permutation of an element of S is again an element of $\mathscr{S}$.

(c) $\sim$ is an equivalence relation on S. Why?

- $\sigma^0(\alpha) = \alpha$ gives reflexivity,
- $\sigma^{-k}(\beta) = \alpha$ whenever $\sigma^j(\alpha) = \beta$ gives symmetry, and lastly
- for $\sigma^j(\alpha) = \beta$, $\sigma^k(\beta) = \gamma$ then $\sigma^{k+j}(\alpha) = \gamma$.

(d) An equivalence class in $\mathscr{S}$ contains a single element if and only if it is of the form $(x, x, \ldots, x)$ with $x^p = 1$.

Note that σ^j stabilizes elements of the form $(x, x, \ldots, x)$ for all $j \in \mathbf{Z}$. Now if $\alpha \in \mathscr{S}$ is not of the form $(x, x, \ldots, x)$ then the equivalence class in α has p distinct elements, because $\sigma^j(\alpha) = \alpha$ if and only if $j \in \mathbf{Z}/p\mathbf{Z}$. There are no more distinct elements in α's equivalence class than those already conspicuous, namely $\alpha, \sigma(\alpha), \ldots, \sigma^{p-1}(\alpha)$.

(e) Every equivalence class has order 1 or p (note that p is a prime). Whence $|G|^{p-1} = k + pd$, where k is the number of classes of size 1 and d is the number of classes of size p.

Since $\mathscr{S}$ is partitioned by $\sim$, summing the elements in each class will produce $|G|^{p-1}$. Well, an $\overline{\alpha} \in \mathscr{S}/\sim$ has size 1 or p. Say there are k classes of size 1 and d classes of size p. Thus $|G|^{p-1} = k + dp$.

(f) Since $\{(1, 1, \ldots, 1)\}$ is an equivalence class of size 1, from (e) there must be a nonidentity element x in G with $x^p = 1$, that is, G contains an element of order p.

Since p divides $|G|^{p-1}$ we must have that p divides $k + dp$ hence $p|k$. Because $k > 1$, we have $k = mp$ for some integer $m \neq 0$, so there's a non-identity element $x \in G$ with $x^p = 1$.

4.11. **[1, No. 3.2.18].** Let G be a finite group, let H be a subgroup of G and let $N \trianglelefteq G$. If $|H|$ and $|G : N|$ are relatively prime then $H \leq N$.

Proof. Consider the natural projection $\pi\colon G \to G/N$. Since $H \leq G$, we have $\pi(H) \leq G/N$. So $|\pi(H)|$ divides $|G : N|$. Now note that $|\pi(H)|$ divides $|H|$ (it's "like" a subgroup). Because the greatest common divisor of $|G : N|$ and $|H|$ is 1, we have $|\pi(H)| = 1$, whence $H \leq \ker \pi = N$. □

4.12. **Minimal and maximal subgroups.** Suppose N is a nontrivial abelian subgroup of G, minimal with the property that it is normal in G. Let H be a proper subgroup of G such that $NH = G$. The intersection of N with H is trivial and H is a maximal subgroup of G.

Proof. Consider the natural homomorphism π onto the group G/N. I claim $H \cap N \subset \ker \pi = N$, and noting that N is abelian, we have that $H \cap N$ is normal in N. Since N is minimal normal we have that $H \cap N = \{1\}$ or $H \cap N = N$. But because H is a proper subgroup of G, there's some $g \in G$ for which $gN \not\subset \pi^{-1}(H)$, so $H \cap N \neq \ker \pi = N$. Whence $H \cap N$ is seen to be trivial.

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