Rose-Hulman Undergraduate Mathematics Journal

Volume 7
Issue 2

Article 4

Subgroup Lattices That Are Chains

Amanda Jez
King's College, ajez@kings.edu

SUBGROUP LATTICES THAT ARE CHAINS

AMANDA JEZ

ABSTRACT. A group G has a subgroup lattice that is a *chain* if for all subgroups H and K of G, we have that H is a subset of K or K is a subset of H. In this article, we first provide elementary proofs of results describing groups whose subgroup lattices are chains, and then generalize this concept to look at groups in which the subgroup lattice can be constructed by pasting together chains.

I. INTRODUCTION

A *subgroup lattice* provides a visual depiction of the subgroup structure of a group. A subgroup lattice is a diagram that includes all the subgroups of the group and then connects a subgroup H at one level to a subgroup K at a higher level with a sequence of line segments if and only if H is a proper subgroup of K [2, pg. 81]. In Example 1.1, you see the subgroup lattice of the quaternion group of order 8, denoted by Q_8. Many other nice examples of subgroup lattices can also be found in [1, pg. 67-70].

We consider this group as presented by $Q_8 = \{1,-1,i,-i,j,-j,k,-k\}$ where

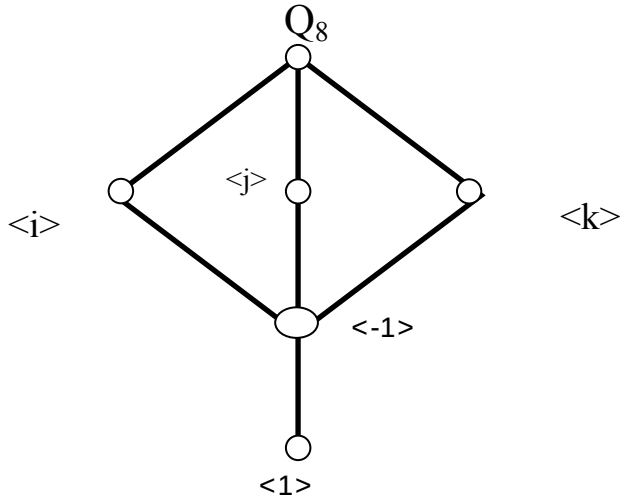
1) 1a=a1=a for all a in Q_8

2) -1a=-a for all a in Q_8

3) $i^2 = j^2 = k^2 = -1$ and

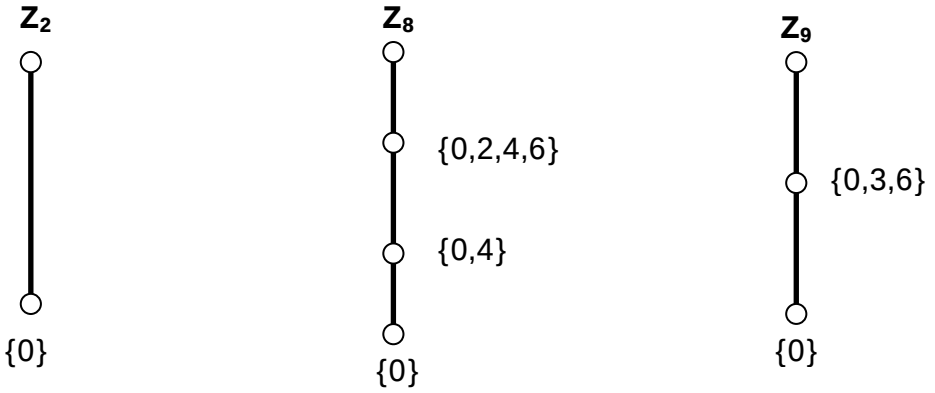
4) ij=k, ji=-k, jk=i, kj=-i, ki=j, ik=-j [1, pg. 34].

Example 1.1



Subgroup lattices have been studied in great depth, as one can see by examining Roland Schmidt's book *Subgroup Lattices of Groups* [3]. But in this article we study what is perhaps the most basic type of subgroup lattice that can occur. We will focus on groups whose subgroup lattices are chains. We say a group G has a subgroup lattice that is a *chain* if for all subgroups H and K of G, we have that H is a subset of K or K is a subset of H. Example 1.2 identifies some groups whose subgroup lattices are chains.

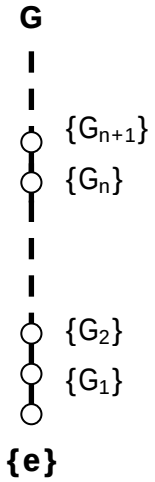
Example 1.2
Note: $Z_n = < \{0,1,2,\ldots,n-1\}, + \bmod n >$



One can readily see that in all of these examples, the groups are cyclic of prime power order. It indeed turns out that a finite group has a subgroup lattice that is a chain if and only if it is isomorphic to Z_{p^n} for some prime p and nonnegative integer n. We dedicate Section 2 of this article to the proof of this result. Although we did not find it presented in the literature, this characterization is likely well known by those with expertise in the field of group theory. We present it in this article using elementary proofs. That is, the reader will find that we do not quote deeper group theoretic results such as Cauchy's Theorem or Sylow's Theorem.

There is also an infinite group whose subgroup lattice is a chain. Consider the group $G = \{k/p^n + Z|\ k,n$ are varying elements of Z and p is a fixed prime$\}$, which is a subgroup of Q/Z, where Q is the group of rational numbers under addition. For each nonnegative integer i, there is a proper subgroup G_i of G such that $G_i = \{k/p^i + Z$: k is an element of Z$\}$. It turns out that for any proper subgroup of G, there is a nonnegative integer i such that the proper subgroup is equal to G_i. We present the subgroup lattice of G in Example 1.3 and prove that the subgroup lattice is a chain in Theorem 2.5.

Example 1.3
Subgroup lattice for $G = \{k/p^n + Z|\ k,n$ are varying elements of Z and p is a fixed prime$\}$



While it is interesting to consider the subgroup lattices of specific groups, one may also ask the question, "Given a lattice, is it possible to find a group for which this lattice is the subgroup lattice?" Our investigations in Section 3 stem from this question. We examine whether a subgroup lattice might be constructed by taking two chains and pasting them together. In particular, given a group G, is it possible that the collection of all of its subgroups splits into 2 non-empty sets of subgroups of G, each of which forms a chain with respect to set containment? Definition 1.4 carefully describes the scenario that we wish to consider.

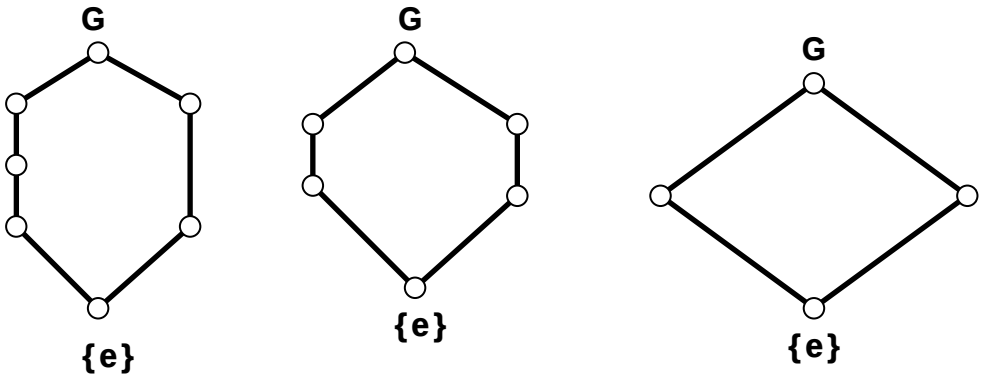
Definition 1.4 - A group G is a group whose *subgroup lattice is formed by two chains* if there are two nonempty sets of proper subgroups S and T of G such that:

- S U T is the set of all *nontrivial* proper subgroups of G.
- S ∩ T is the empty set.
- For all H in S, every *nontrivial* subgroup of H is in S and similarly for all K in T, every *nontrivial* subgroup of K is in T.
- For all S_1, S_2 in S, S_1 is a subset of S_2 or S_2 is a subset of S_1. Similarly, for all T_1, T_2 in T, T_1 is a subset of T_2 or T_2 is a subset of T_1 .

If a group G had any of the lattices from Example 1.5 as its subgroup lattice, then it would satisfy this definition. We will see in Section 3 that there are no groups for which the first two lattices in Example 1.5 serve as subgroup lattices. We prove in Theorem 2.1 that if G is a group whose subgroup lattice is formed by two chains, then G is isomorphic to Z_{pq} where p and q are primes such that $p \neq q$. The only possible subgroup lattice from the three presented in Example 1.5 is the third.

Example 1.5

Lattices that would satisfy the definition of being formed by two chains.



We close the article by considering how we might generalize Definition 1.4 to describe groups with subgroup lattices that are formed by n chains for any positive integer n, and providing examples of such groups. The reader should also observe that all of the groups examined in Sections 2 and 3 are groups in which every proper subgroup is a group whose subgroup lattice is a chain. Yet groups in which every proper subgroup has a subgroup lattice that is a chain may clearly have more complicated structures than

cyclic groups or direct products of cyclic groups, as can be seen in the quaternion group of order 8, which is presented in Example 1.1.

Most group theoretic notation in this article is standard. We do wish to point out to the reader that for an element x of a group G, o(x) denotes the order of x. Work done on this project was completed during an independent study at King's College, Wilkes-Barre, PA under the supervision of Dr. Joseph Evan.

II. GROUPS WHOSE SUBGROUP LATTICES ARE CHAINS

This section is an in-depth discussion of groups whose subgroup lattices are chains. We first provide elementary proofs of three results, Lemmas 2.1, 2.2, and 2.3, that combine to form the proof Theorem 2.4, describing all finite groups whose subgroup lattices are chains. One might also attempt to apply Cauchy's Theorem or Sylow's Theorem in proving these results, but we aim to give efficient proofs that do not require a deep group theoretic background from the reader.

Lemma 2.1. If G is a finite group and the subgroup lattice of G is a chain, then G is cyclic.

Proof. We prove the contrapositive of this statement. Suppose G is not cyclic and finite. We wish to show that the subgroup lattice of G is not a chain. Choose x in G such that $o(x)=\max\{ o(g) \mid g \in G \}$. Then $\langle x \rangle$ is a subgroup of G with order o(x). Recall that G is not cyclic, and so there is y in G such that y is not in $\langle x \rangle$. Since $y \notin \langle x \rangle$, ,$\langle y \rangle$ is not contained in $\langle x \rangle$. So suppose $\langle x \rangle$ is properly contained in $\langle y \rangle$. Then $o(y)>o(x)$, contradicting the choice of o(x). Thus, $\langle x \rangle$ is not a subset of $\langle y \rangle$. Therefore, the subgroup lattice of G is not a chain.

Lemma 2.2. If the subgroup lattice of Z_n is a chain, then n has prime power order.

Proof. Suppose that the subgroup lattice of Z_n is a chain and n does not have prime power order. Then $n = kp^a$ and $n= mq^b$ for primes p and q and positive integers a, b, k, m such that p does not divide k and q does not divide m.

Let $Z_n = \langle x \rangle$. Then the orders of $< kx >$ and $< mx >$ are powers of p and q respectively. It follows from Lagrange's Theorem that neither of these subgroups is contained in the other, contradicting that the subgroup lattice of Z_n is a chain. Therefore, n has prime power order.

Lemma 2.3. If p is a prime and n is a natural number, then the subgroup lattice of Z_{p^n} is a chain.

Proof. For this proof consider, $Z_{p^n} = <\{0,1, \ldots p^n -1\}, + \bmod p^n >$. We first show that for any nonzero x in $\{0,1, \ldots p^n -1\}$, there is a nonnegative integer i such that $\langle x \rangle = \langle p^i \rangle$.

Choose i such that p^i divides x but p^{i+1} does not divide x. Then p^i divides x, and it is clear that $\langle x\rangle \subseteq \langle p^i\rangle$. Since these subgroups are finite it is sufficient to prove that $o(x)=o(p^i)$ in order to demonstrate that $\langle x\rangle=\langle p^i\rangle$.

Of course, $o(p^i)=p^{n-i}$. Now by the choice of i, $x=m\,p^i$ for a positive integer m where p does not divide m. As a consequence of Lagrange's Theorem, $o(x)=p^k$ for some positive integer k. Observe that $p^{n-i}x=p^{n-i}m\,p^i$ is divisible by p^n. So $k\leq n-i$. But p^n divides $p^k x=p^k m\,p^i=m\,p^{k+i}$. Since p does not divide m, $n\leq k+i$, and thus, $k\geq n-i$. Hence, k=n-i. Therefore, $o(x)=o(p^i)$, completing our proof that $\langle x\rangle=\langle p^i\rangle$.

Now the only distinct subgroups of Z_{p^n} are of the form $\langle p^i\rangle$ for nonnegative integers i, and so in proving that the subgroup lattice of Z_{p^n} is a chain, it is sufficient to consider only these subgroups. Thus, let $\langle p^i\rangle$ and $\langle p^j\rangle$ be subgroups of Z_{p^n} where j>i. Then, $p^j=p^{j-i}p^i\in\langle p^i\rangle$. Hence, $\langle p^j\rangle\subseteq\langle p^i\rangle$, completing the proof.

Lemmas 2.1 and 2.2 together form the proof of the forward direction of Theorem 2.4. Lemma 2.3 gives us the proof of the other direction.

Theorem 2.4. A finite group has a subgroup lattice that is a chain if and only if it is isomorphic to Z_{p^n}.

Of course, there is also an infinite group whose subgroup lattice is a chain. The group $G = \{k/p^n + Z|$ k,n are varying elements of Z and p is a fixed prime$\}$, which is a subgroup of Q/Z, is such a group. We leave it to the reader to prove that G is indeed a subgroup of Q/Z.

In order to prove that the subgroup lattice of this group is a chain, we will demonstrate that the proper subgroups of G are of the form $G_i = \{k/p^i + Z$: k is an element of Z$\}$ where i is a nonnegative integer. Once this is shown, one can see that the subgroup lattice of G is a chain since for any nonnegative integers i and j with j>i, we can write any k/p^i as $k\,p^{j-i}/p^j$ and hence, $G_i \subseteq G_j$.

Theorem 2.5. Let $G= \{k/p^n + Z|$ k,n are varying elements of Z and p is a fixed prime$\}$. If S is a proper subgroup of G, then for some nonnegative integer i, $S=G_i$ where $G_i = \{k/p^i + Z$: k is an element of Z$\}$.

Proof. Let S be a proper subgroup of G, and consider the set $X=\{i|$ i is a nonnegative integer and for some integer k which is not divisible by p, $k/p^i + Z$ is in S$\}$. Clearly X is nonempty. We claim that X has a maximum value.

Suppose not. We will prove that S=G. Let $k/p^j + Z$ be any element of G. It follows that there is $m\in X$ with m>j. So there is an integer r, not divisible by p, such that $r/p^m + Z$ is in S. Clearly, the order of $r/p^m + Z$ is p^m. Since the order of $1/p^m + Z$ is also

p^m, and $< r/p^m + Z >$ is contained in $<1/p^m + Z>$, we have $< r/p^m + Z > = <1/p^m + Z>$. But now $k/p^j + Z = k p^{m-j}(1/p^m + Z) \in <1/p^m + Z> = < r/p^m + Z> \subseteq S$. Hence, G=S.

Now X has a maximum value, and so we let h=max(X). We claim that $S = G_h$. Observe that $G_h = <1/p^h + Z>$. For some integer s that is not divisible by p, $s/p^h + Z$ is in S. Arguing as in the preceding paragraph, the order of $s/p^h + Z$ is clearly p^h, and since $o(1/p^h + Z) = p^h$ and $< s/p^h + Z> \subseteq <1/p^h + Z>$, we have that $< s/p^h + Z> = <1/p^h + Z>$. As a result, $G_h \subseteq S$.

On the other hand, any element of S can be written as $k/p^i + Z$ for an integer k and nonnegative integer $i \leq h$. Therefore any such $k/p^i + Z$ in S is equal to $kp^{h-i}(1/p^h + Z)$ and so $S \subseteq <1/p^h + Z> = G_h$.

III. GROUPS WHOSE SUBGROUP LATTICES ARE FORMED BY TWO CHAINS

The goal of this section is to characterize a group whose subgroup lattice is formed by two chains. We state our result in Theorem 3.1. Notice that there is no assumption regarding the finiteness of G in this result.

Theorem 3.1. If G is a group whose subgroup lattice is formed by two chains, then G is isomorphic to Z_{pq} where p and q are primes such that $p \neq q$.

In order to prove Theorem 3.1, we need to apply three well known results. Lemmas 3.2 and 3.3 follow from the study of inner automorphisms and the definition of a normal subgroup, while Lemma 3.4 is the internal characterization of a direct product [2, pg. 182-185].

Lemma 3.2. Let G be a group, and let $g \in G$. Then the function, Φg: G→G defined by $\Phi g(x) = g^{-1}xg$ is an isomorphism.

Lemma 3.3. A subgroup S of a group G is normal if and only if for all g in G, $\Phi g(S) = S$.

Lemma 3.4. If G is a group, and H and K are normal subgroups, then HK is a subgroup of G. Furthermore, if G = HK where $HK = \{hk \mid h \in H \text{ and } k \in K\}$ and $H \cap K = \{e\}$ (where e is the identity in G), then G is isomorphic to H×K.

Now we give the proof of Theorem 3.1

Proof of Theorem 3.1.

Suppose G is a group whose subgroup lattice is formed by two chains. Then there are two nonempty sets S and T of nontrivial proper subgroups of G. We claim S contains a unique subgroup of prime order. Since S is nonempty, there exists S_1 such that S_1 is an element of S. Notice that since the subgroup lattice of S_1 is a chain, the subgroup lattice

of each of its subgroups is a chain. Thus every element of S_1 generates a cyclic subgroup whose subgroup lattice is a chain.

Observe that the subgroup lattice of an infinite cyclic group is not a chain. This is true since every infinite cyclic group is isomorphic to the group of integers under addition. For any two distinct primes, p and q, $< p >$ and $< q >$ will be subgroups of the integers consisting of all multiples of p and q respectively. It is then clear that $< p >$ is not a subset of $< q >$ and $< q >$ is not a subset of $< p >$. So every element of S_1 must generate a finite cyclic subgroup whose subgroup lattice is a chain. By applying Theorem 2.4 to each of these finite cyclic subgroups, it follows that every element of S_1 generates a cyclic subgroup of prime power order.

Since S_1 is nontrivial, it has at least one nontrivial cyclic subgroup, and we have proved that this subgroup has prime power order. This nontrivial cyclic subgroup will then have a subgroup of prime order. Thus S_1 has a subgroup P of order p, where p is a prime. Observe that P is an element of S. We must now show that the subgroup P is unique. Suppose that P_1 is also an element of S that has order p. By definition, P_1 is a subset of P or P is a subset of P_1. But notice both have order p, so $P_1 = P$. Therefore, S contains a unique element of order p. By a similar argument, T contains a unique element of prime order q. Denote this subgroup by Q.

Now we will show P and Q are normal subgroups. Let g be an arbitrary element of G such that $g \neq e$. If $<g> = G$, then G is cyclic and P and Q are normal. If $<g> \neq G$, then $<g>$ is an element of S or $<g>$ is an element of T. Now either $P \leq <g>$ or $Q \leq <g>$. Suppose $P \leq <g>$. Then for all x in P, x is an element of $<g>$. Notice then that $\Phi g(x) = g^{-1} x g = x$ for all x in P, since x is a power of g. So we have that $\Phi g[P] = P$, when $P \leq <g>$.

Suppose then that $Q \leq <g>$. We need to show that $\Phi g[P] = P$. Now by similar argument $\Phi g[Q] = Q$. Since Φg is an isomorphism by Lemma 3.2, $\Phi g[P]$ is a subgroup of prime order, and thus $\Phi g[P] = P$ or $\Phi g[P] = Q$. But recall $\Phi g[Q] = Q$. Since Φg is an injection, $\Phi g[P] = P$. So for all g in G, $\Phi g[P] = P$ and P is normal by Lemma 3.3. By a similar argument, Q is normal.

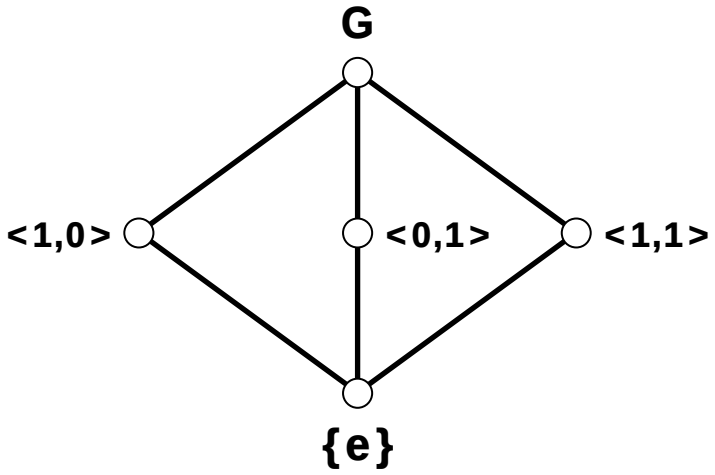
Now that P and Q are normal, by Lemma 3.4, $PQ \leq G$. We wish to show $PQ = G$. Suppose PQ is a proper subgroup of G. Then PQ is an element of S or PQ is an element of T. Suppose PQ is an element of S. Then $P \leq PQ$ and $Q \leq PQ$. But then P is an element of S and Q is an element of S. But recall Q is an element of T. This contradicts that $S \cap T$ is the empty set, and so PQ is not in S. Similarly, PQ is not an element of T. Thus, PQ is not a proper subgroup of G, and $PQ = G$. By Lemma 2.4, G is isomorphic to $P \times Q$.

Lastly, we claim $p \neq q$. Suppose $p = q$. Let $P = <x>$ and $Q = <y>$. Since x and y have order p, the subgroups $<(x,e)>$, $<(e,y)>$, and $<(x,y)>$ of $P \times Q$ have order p. But G only has two subgroups of prime order, namely P and Q, and G is isomorphic to $P \times Q$. This is a contradiction, and so $p \neq q$. Therefore, G is isomorphic to $Z_p \times Z_q$, which is isomorphic to Z_{pq}, completing the proof.

The reader should observe that we may adjust Definition 1.4 to define a *group whose subgroup lattice is formed by n chains* for any positive integer n. For example, for any prime p, $Z_p \times Z_p$ would be a group whose subgroup lattice is formed by p+1 chains.

The reason for this is that by Lagrange's Theorem, all *nontrivial* subgroups of Z_p x Z_p have order p. There are p+1 such subgroups of Z_p x Z_p. If Z_p = <{0,1,2,…, p-1}, + mod p>, then the p+1 subgroups are <(1,0)> and {<(x,1)> | x ranges over {0,1,…,p-1}}. Example 3.5 demonstrates what happens in the case that p=2.

Example 3.5. The subgroup lattice of $Z_2 \times Z_2$ is formed by three chains.



REFERENCES

1. David S. Dummit and Richard M. Foote. Abstract Algebra, Prentice Hall, 1991.
2. Joseph A. Gallian. Contemporary Abstract Algebra, Houghton Mifflin Company, 2002.
3. Roland Schmidt. Subgroup Lattices of Groups, Walter de Gruyter, 1994.