# planetmath.org

Math for the people, by the people.

# lattice of subgroups

| | |
|---|---|
| Canonical name | LatticeOfSubgroups |
| Date of creation | 2013-03-22 15:47:42 |
| Last modified on | 2013-03-22 15:47:42 |
| Owner | CWoo (3771) |
| Last modified by | CWoo (3771) |
| Numerical id | 14 |
| Author | CWoo (3771) |
| Entry type | Definition |
| Classification | msc 20E15 |
| Synonym | subgroup lattice |

Let $G$ be a group and $L(G)$ be the set of all subgroups of $G$. Elements of $L(G)$ can be ordered by the set inclusion relation $\subseteq$. This way $L(G)$ becomes a partially ordered set.

For any $H, K \in L(G)$, define $H \wedge K$ by $H \cap K$. Then $H \wedge K$ is a subgroup of $G$ and hence an element of $L(G)$. It is not hard to see that $H \wedge K$ is the largest subgroup of both $H$ and $K$.

Next, let $X = H \cup K$ and define $H \vee K$ by $\langle X \rangle$, the subgroup of $G$ generated by $X$. So $H \vee K \in L(G)$. Each element in $H \vee K$ is a finite product of elements from $H$ and $K$. Again, it is easy to see that $H \vee K$ is the smallest subgroup of $G$ that has $H$ and $K$ as its subgroups.

With the two binary operations $\wedge$ and $\vee$, $L(G)$ becomes a lattice. It is a bounded lattice, with $G$ as the top element and $\langle e \rangle$ as the bottom element. Furthermore, if $\{H_i \mid i \in I\}$ is a set of subgroups of $G$ indexed by some set $I$, then both

$$\bigwedge_{i \in I} H_i \qquad \text{and} \qquad \bigvee_{i \in I} H_i$$

are subgroups of $G$. So $L(G)$ is a complete lattice. From this, it is easy to produce a lattice which is not a subgroup lattice of any group.

Atoms in $L(G)$, if they exist, are finite cyclic groups of prime order (or $\mathbb{Z}/p\mathbb{Z}$, where $p$ is a prime), since they have no non-trivial proper subgroups.

**Remark.** Finding lattices of subgroups of groups is one way to classify groups. One of the main results in this branch of group theory states that the lattice of subgroups of a group $G$ is `http://planetmath.org/DistributiveLattice`distributive iff $G$ is locally cyclic.

It is generally not true that the lattice of subgroups of a group determines the group up to isomorphism. Already for groups of order $p^3$, $p > 2$ or $p^4$, for all primes, there are examples of groups with `http://planetmath.org/LatticeIsomorphism`isomor subgroup lattices which are not isomorphic groups.

**Example.** Note that $\operatorname{Aut} \mathbb{Z}_{p^2} \cong \mathbb{Z}_{p-1} \times \mathbb{Z}_p$. Therefore it is possible to from a non-trivial semidirect product $\mathbb{Z}_{p^2} \rtimes \mathbb{Z}_p$. The lattice of subgroups of $\mathbb{Z}_{p^2} \rtimes \mathbb{Z}_p$ is the same as the lattice of subgroups of $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$. However, $\mathbb{Z}_{p^2} \rtimes \mathbb{Z}_p$ is non-abelian while $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ is abelian so the two groups are not isomorphic.

Similarly, the groups $\mathbb{Z}_{p^i} \rtimes \mathbb{Z}_p$ and $\mathbb{Z}_{p^i} \times \mathbb{Z}_p$ for any $i > 2$ and any primes $p$ also have isomorphic subgroup lattices while one is non-abelian and the other abelian. So this is indeed a family of counterexamples.

Upon inspecting these example it becomes clear that the non-abelian

groups have a different sublattice of normal subgroups. So the question can be asked whether two groups with isomorphic subgroup lattices including matching up conjugacy classes (so even stronger than matching normal subgroups) can be non-isomorphic groups. Surprisingly the answer is yes and was the dissertation of Ada Rottländer[**?**], a student of Schur's, in 1927. Her example uses groups already discovered by Otto Hölder in his famous classification of the groups of order $p^3$, $p^2q$, and $p^4$. With the modern understanding of groups the counterexample is rather simple to describe – though a proof remains a little tedious.

Let $V = \mathbb{Z}_q^2$ where $q$ is a prime – that is $V$ is the 2-dimensional vector space over the field $\mathbb{Z}_q$. Let $p | q - 1$ be another prime. As $p | q - 1$, $\mathbb{Z}_p \le \mathbb{Z}_q^\times$ so if we write $\mathbb{Z}_p = \langle \omega \rangle$ multiplicatively so that we have for every $n \in \mathbb{Z}_q$, $n \mapsto \omega \cdot n$ is an automorphism of $\mathbb{Z}_q$. (Note that $\omega$ is often called a primitive $p$-th root of unity in $\mathbb{Z}_q$ as it spans the $\mathbb{Z}_p$ subgroup of $\mathbb{Z}_q^\times$.) Furthermore, for any $0 \le i \le p - 1$ we get an automorphism $f_i : \mathbb{Z}_q \to \mathbb{Z}_q$ given by

$$f_i(n) = \omega^i n.$$

Therefore to every $0 \le i \le p - 1$ we can define a group $G_i = \langle V, g_i \rangle$, $g_i = f_1 \oplus f_i$ as a subgroup of $AGL(V)$. That is to say, $G_i = V \rtimes \langle g_i \rangle$ where the action of $g_i$ on $V$ is given by: for every $v \in V$, $v = \begin{bmatrix} n \\ m \end{bmatrix}$ for $n, m \in \mathbb{Z}_q$ set

$$g_i(v) = \begin{bmatrix} \omega & 0 \\ 0 & \omega^i \end{bmatrix} \begin{bmatrix} n \\ m \end{bmatrix} = \begin{bmatrix} \omega n \\ \omega^i m \end{bmatrix}.$$

We are now prepared to give the Rottländer counterexample.

Now let $a$ and $b$ be integers between 2 and $p - 1$ such that $a$ is not congruent to $b$ modulo $p$. Notice this already forces $p > 3$ so our smallest example is $q = 11$ and $p = 5$. Then $G_a$ is not isomorphic to $G_b$ (compare the eigenvalues of $g_a$ to $g_b$ – they are not equal so the linear transformations are not conjugate in $GL(2, q)$.) However, $G_a$ and $G_b$ have isomorphic subgroup lattices including matching conjugacy classes.

# References

[1] Rottländer, Ada, *Nachweis der Existenz nicht-isomorpher Gruppen von gleicher Situation der Untergruppen*, Math. Z. vol. 28, 1928, 1, pp. 641–653, ISSN 0025-5874. MR MR1544982,