Soft Comput (2017) 21:2503–2505
DOI 10.1007/s00500-017-2571-1

FOCUS

An application of subgroup lattices

Yanping Chen[1] · **Yichuan Yang**[2]

Published online: 28 March 2017

Abstract We give a lattice theoretic proof of the well-known result that a finite group G is cyclic iff G has at most one subgroup of each order dividing $|G|$. Consequently, we show that a division ring D is a field iff D has at most one maximal subfield.

Keywords Subgroup lattice · Distributive lattice · Cyclic group · Division ring · Wedderburn's "little" Theorem

1 Introduction

Let G be a finite group. It is well known that G is cyclic iff it has at most one subgroup of each order dividing $|G|$ (cf., for example, Ogus 2008). This beautiful result is usually proved using a result of number theory connected with the factors of $|G|$. An interesting and natural question is, whether one can give a lattice theoretic proof of the order structure of subgroups of a cyclic group? In fact, if $|G| = n$, then for all $m|n$, G has at most one subgroup H of order m is equivalent to say that the equation $x^m = 1$ has at most m solutions.[1]

Let D be a finite division ring. J. H. M. Wedderburn first showed that D is a field, that is, the multiplicative group D^* of D is a cyclic group. This theorem is known as Wedderburn's "little" theorem with many proofs given by several dozen mathematicians. A direct and natural question is whether one can also give a lattice theoretic proof for this "easier" case, since there is two compatible operations in a division ring? It is well known that a polynomial f with degree n in a division ring has infinite roots if f has more than n roots (Lam 1991, Corollary 16.12); however, the proof of the existence of infinite roots heavily depends on Wedderburn's "little" theorem itself. Furthermore, Wedderburn's "little" theorem raises a natural question of which division rings are fields?

In the paper, we give a lattice theoretic proof of the above mentioned characterization of a finite group G to be cyclic iff G has at most one subgroup of each order dividing $|G|$. Consequently, we show that a division ring D is a field iff D has at most one maximal subfield.

2 Distributive lattices

Recall that a lattice L is a poset such that for any two elements $x, y \in L$, there exist a least upper bound (l.u.b.) denoted by $x \vee y$, and a greatest lower bound (g.l.b.) denoted by $x \wedge y$. For instance, M_5 and N_5 in Fig. 1 are lattices. A lattice L is distributive if and only if the following identity holds for all $x, y, z \in L$:

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z).$$

[1] Note that the idea is closely related to with Frobenius conjecture on characteristic subgroup of finite group.

Communicated by Y. Yang.

The work is partially supported by NSFC (Grant 11271040), and the Fundamental Research Funds for the Central Universities (Grant 302996).

✉ Yichuan Yang
ycyang@buaa.edu.cn

Yanping Chen
cypfjfz@163.com

1 Department of Foundation, Fujian Commercial College, 350012 Fuzhou, China

2 Department of Mathematics, Beihang University, 100191 Beijing, China

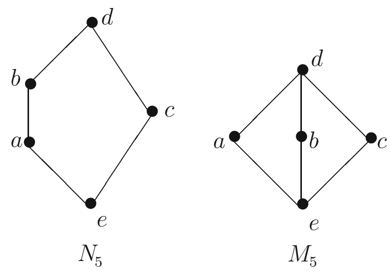

Fig. 1 *N5, M5*

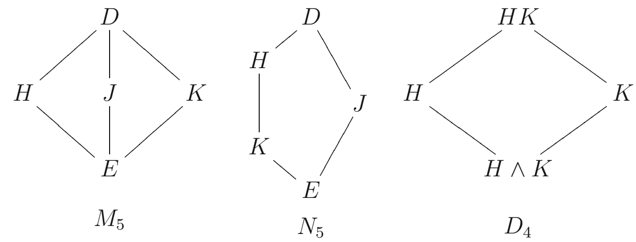

Fig. 2 M_5, N_5, D_4

It is easily seen that neither M_5 nor N_5 is distributive. Conversely, following theorem is well known since 1930's:

Lemma 1 (Burris and Sankappanavar 1981 Thm. 3.6) *A lattice is non-distributive if and only if M_5 or N_5 can be embedded into it.*

3 Subgroup lattices

Let $L(G)$ be the set of all subgroups of a group G, and let the partial order $\leq$ be the set-inclusion $\subseteq$. Then, $L(G)$ is a lattice called subgroup lattice, with respect to the meet

$$H \wedge K = H \cap K,$$

and the join

$$H \vee K = \cap_{J \in \{L(G)\}} \{H \cup K \subseteq J\}$$

for all subgroups H and K of G. It is interesting that the distributivity of the subgroup lattice of a group implies the group is commutative, the following result is well known since 1930's, too:

Lemma 2 (Birkhoff 1964 P.96, Thm. 13]) *The subgroup lattice $L(G)$ of a finite group G is distributive if and only if G is cyclic.*

Now, we give a lattice theoretic proof of the well-known theorem (cf. Ogus 2008):

Theorem 1 *A finite group G is cyclic iff G has at most one subgroup of each order dividing $|G|$.*

Proof Assume that G has at most one subgroup of each order dividing $|G|$. It is easy to verify that each subgroup H of G is normal since gHg^{-1} is a subgroup of G with the same order $|H|$ for each element g of G. Thus, for any two subgroups H, K of G, we have $H \wedge K = H \cap K$ and $H \vee K = HK = KH$. Now, let us show that the sublattice M_5 or N_5 cannot be embedded into the subgroup lattice $L(G)$ of G by the second isomorphic theorem of groups.

Case 1: If M_5 (see Fig. 2) can be embedded into $L(G)$. By $D = H \vee J = H \vee K = K \vee J$, $E = H \wedge K = H \wedge J = J \wedge K$, and $D/J \cong H/E \cong K/E$, especially, it follows $H = K$ by the uniqueness of the same order subgroups.
Case 2: If N_5 (see Fig. 2) can be embedded into $L(G)$. By $D = H \vee J = K \vee J$, $E = H \wedge J = J \wedge K$, and $D/J \cong H/E \cong K/E$, similarly, it follows that $H = K$ by the uniqueness of the same order subgroups, again.

Hence, the subgroup lattice of G is distributive by Lemma 1, and G is cyclic by Lemma 2.

Conversely, suppose that G be cyclic. If (see D_4 in Fig. 2) H and K are two subgroups of G with the same order m. Then, $HK = KH = H \vee K$ is a subgroup of G, and thus cyclic. Without loss of generality, assume that $HK = \langle s \rangle$, then the order of s must be m, since $(hk)^m = 1$ for all hk in HK. That is, $HK = H = K$. □

4 Maximal subfield semi-lattices

Let D be a division ring. It is easily seen that there always exists at least one maximal subfield. Let $M(D)$ denote the set of maximal subfields of D. Then, for any two elements $F, K \in M(D)$, $F \cap K \in M(D)$; however, the sub-division-ring generated by $F \cup K$ is not a field in general. Thus, $M(D)$ is a semi-lattice. With such an illustration, we get

Theorem 2 *A division ring D is a field iff D has a unique maximal subfield iff $M(D)$ is a lattice.*

Proof If D is a field, then D is the unique maximal subfield. Conversely, if D has a unique maximal subfield F, it remains to prove that $F = D$. Assume that $F \subsetneqq D$. Then, there exists $d \in D \backslash F$ such that the division ring extension $F(d)$ is not a field. It follows that $d \notin Z(D)$, where $Z(D)$ is the center of D. Thus, there exists another maximal subfield which contains d. This contradiction shows that $F = D$. □

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

Birkhoff G (1964) Lattice theory, Rev edn. AMS, Colloquium Publications, New York

Burris S, Sankappanavar HP (1981) A course in universal algebra, (GTM). Springer, London

Lam TY (1991) A first course in noncommutative rings. Springer, London

Ogus A (2008) Math 113—Introduction to Abstract Algebra, Cyclicity of Groups, Cyclicty. Available from http://math.berkeley.edu/~ogus/Math_113_08/supplements/cyclicity