On the Uniqueness of the Cyclic Group of Order n

Dieter Jungnickel

The American Mathematical Monthly, Vol. 99, No. 6. (Jun. - Jul., 1992), pp. 545-547.

Stable URL:
http://links.jstor.org/sici?sici=0002-9890%28199206%2F07%2999%3A6%3C545%3AOTUOTC%3E2.0.CO%3B2-M

The American Mathematical Monthly is currently published by Mathematical Association of America.

On the Uniqueness of the Cyclic Group of Order n

Dieter Jungnickel

When is there a unique group of order n? (Such a group, of course, must be cyclic.) When teaching a beginning course in group theory, we point out there is a unique group when n is a prime. Usually, we go on to discuss the Sylow theorems and apply them to groups of order pq ($p < q$ primes). Such a group is unique, we show, if and only if p does not divide $q - 1$. It is natural, therefore, to ask when the group of order n is unique. The answer is "well known", but not widely known, and seldom mentioned in such classes. Here is a simple proof that is suitable for even an elementary class in group theory.

Theorem. *Let n be a positive integer. Then the cyclic group $C(n)$ of order n is the only group of order n if and only if one has $(n, \phi(n)) = 1$, where ϕ denotes the Euler phi function.*

Proof: We first note that both conditions imply that n is square-free. For assume that $n = mp^a$, where p is a prime not dividing m and where $a \geqslant 2$. Then both n and $\phi(n) = p^{a-1}(p - 1)\phi(m)$ are divisible by p. Also, the group $C(m) \times C(p)^a$ is clearly not isomorphic to $C(n)$. From now on, let n be square-free. Then

$$(*)\ n = p_1 \cdots p_k \text{ is a product of distinct primes and}$$

$$\phi(n) = (p_1 - 1) \cdots (p_k - 1).$$

Thus $(n, \phi(n)) \neq 1$ implies the existence of primes p and q dividing $n = pqm$, say, for which p divides $q - 1$. Then there exists a non-abelian group H of order pq (a semidirect product), and so $H \times C(m)$ is a non-abelian group of order n.

It thus remains to assume $(n, \phi(n)) = 1$ and to show that there is only one group of order n in this case. Assume the contrary, and let n be the least positive integer for which a counter-example G exists. We shall now reach a contradiction in the following steps.

Step 1. One has $(m, \phi(m)) = 1$ for every divisor m of n.
This follows immediately from $(*)$ above.

Step 2. Every proper subgroup and every non-trivial factor group of G are cyclic.
This is clear from Step 1 and the minimality of n.

Step 3. The center $Z(G)$ is trivial.

Otherwise $G/Z(G)$ would be cyclic by Step 2, and therefore G would be abelian and hence cyclic.

Step 4. Let $x \neq 1$ be an element of a maximal subgroup U of G. Then U is the centralizer $C_G(x)$ of x in G.

For $C_G(x)$ is a proper subgroup of G by Step 3, and U is cyclic and therefore contained in $C_G(x)$ by Step 2; thus the maximality of U shows $U = C_G(x)$.

Step 5. Any two distinct maximal subgroups U and V of G have trivial intersection.

For assume that $x \neq 1$ is in $U \cap V$. Then Step 4 would give the contradiction $U = C_G(x) = V$.

Step 6. Any maximal subgroup U equals its own normalizer $N_G(U)$.

To see this, let $x \neq 1$ be any element in $N_G(U)$. Then the conjugation with x induces an automorphism α of the cyclic group U. If U has order m, then the automorphism group of U has order $\phi(m)$ which divides $\phi(n)$ because of $(*)$. Since x and hence α have order dividing n, Step 1 shows that α has to have order 1. Thus x centralizes U and by Step 3 belongs to U.

Step 7. Let U be a maximal subgroup of order u of G. Then the conjugates of U contain exactly $n - n/u$ elements $\neq 1$.

Note that the number of conjugates of U is the index of the normalizer of U in G. By Step 6, this index is n/u. By Step 5, any two distinct conjugates of U intersect trivially. Thus the conjugates of U contain altogether $(u-1)n/u$ elements $\neq 1$.

Step 8. Now let U be as in Step 7 and choose an element x not contained in any of the conjugates of U. Let V be a maximal subgroup containing x and therefore not conjugate to U. Then any conjugate of V and any conjugate of U intersect trivially by Step 5. Applying Step 7 also to V, we obtain $n - n/v$ elements $\neq 1$ in the conjugates of V. But there are only $n - 1$ elements $\neq 1$, giving the inequality

$$n - n/u + n - n/v < n$$

which results in the contradiction $uv < u + v$. □

Some historical remarks: The preceding theorem is a special case of a result due to Dickson [**1**] who determined those n for which every group of order n is abelian; his 1905 paper is, as far as the author knows, the earliest reference for our theorem. Simpler proofs were given by Szele [**4**] and Szep [**5**] who seem not to have been aware of Dickson's result. Regarding further reading, the reader might be interested to go on to study related questions, e.g. for which orders n every group is abelian or nilpotent; for these and similar questions, we recommend Pazderski [**3**]. Another problem that is suggested by the proof given above is the determination of those non-abelian groups for which all proper subgroups are abelian; this problem was considered by Miller and Moreno [**2**].

REFERENCES

1. L. E. Dickson, Definitions of a group and a field by independent postulates, *Trans. Amer. Math. Soc.* 6 (1905), 198–204.
2. G. A. Miller and H. C. Moreno, Non-abelian groups in which every subgroup is abelian, *Trans. Amer. Math. Soc.* 4 (1903), 398–404.

3. G. Pazderski, Die Ordnungen, zu denen nur Gruppen mit gegebener Eigenschaft gehören, *Archiv Math.* 10 (1959), 331–343.
4. T. Szele, Über die endlichen Ordnungszahlen, zu denen nur eine Gruppe gehört, *Comm. Math. Helv.* 20 (1947), 265–267.
5. J. Szep, On finite groups which are necessarily commutative, *Comm. Math. Helv.* 20 (1947), 223–224.

Mathematisches Institut
Justus Liebig Universität Giessen
Arndtstr. 2, D-6300 Giessen
Germany

THE PARADOX OF FAIRNESS

Let's say the coin is fair
And we toss it in the air.

Heads or Tails?
Who's the first to pick?
Shall we toss another?
To avoid a Diaconis trick.

But then what side
Will decide
The options on which
Our game does ride?

Let a third person toss it in the air!
And we'll call it while it's there.

But who's first to call it—
While it's there?
Again we shout
All is still unfair!

Play until fortunes tie.
Won't that now satisfy?

Might as well play for fun
Or never start the run
Than await boring ties
And even triter lies.

Cooperation is what's fair.
You cut the cake...
I'll pick from the pair.

But Beware!
Let not Tarski make the tear!
Otherwise, and it's okay—
The Game is Solitaire—
With its fun and lonely fare
Free of all competing dare.