Abstract Algebra

August, Evelyn, revised *

9/28/2021

$\boxed{19}$ What are the cyclic subgroups of $U(30)$.

$\boxed{\text{answer}}$ Finding the cyclic subgroups of $u(30)$ can be done easily by making a simple program in python. Using the following simple program:

```python
import math

u30 = set()

for x in range(30):
  if math.gcd(30,x) == 1:
    u30.add(x)
    print(x)
cycle = set()
for e in u30:
  cycle = set()
  done = False
  n = 1
  while not done:
    a = e**n % 30
    if a in cycle:
      done = True
    cycle.add(a)
    n += 1
  print(cycle)
```

, we obtain the following cyclic subgroups, $< 1 >= \{1\}$, $< 7 >=< 13 >= \{1, 7, 13, 19\}$, $< 11 >= \{1, 11\}$, $< 17 >=< 23 >= \{1, 17, 19, 23\}$ $< 19 >= \{1, 19\}$, and $< 29 >= \{1, 29\}$. In total, this is 6 distinct cyclic subgroups of $U(30)$, including the trivial subgroup.

$\boxed{\text{20, proposition}}$ Let G be an Abelian group of order 35 such that every element in G satisfies the equation $x^{35} = e$. Then G is cyclic.

$\boxed{\text{proof}}$ Suppose G is an Abelian group of order 35 with the property that for every element $x \in G$ $x^{35} = e$. Let x be an arbitrary element in G. By corollary 2 of theorem 4.1, $|x||35$. Then for all elements $x \in G$, $|x|$ can be $1, 5, 7$, or 35. By a corollary to theorem 4.4, we know that the number of elements in G of order d must be a non-negative (a negative number wouldn't make sense) multiple of $\phi(d)$. Considering all of our possible orders, and since the identity is the only element of order 1 which must be unique, we have the equation $1+\phi(5)a+\phi(7)b+\phi(35)c = 35 : a, b, c \in \mathbb{N}_0$. This equation simplifies to $2a + 3b + 12c = 17$. Since 2,3,12 are not divisors of 17, at least two of these coefficients must be nonzero. Hence we have four options for zero coefficients: a, b or c zero or none. If the first three options hold and c is not zero, we're done (at least to the step of showing there is an element with order 35). Assume then that c is zero. Then there exist some elements x of order 5 and y of order 7. Furthermore, by the closure property of groups $xy \in G$. By a previously proven theorem, and since G is Abelian, the order of xy must divide $|x||y| = 35$. If $|xy| = 5$, we have $x^5 y^5 = y^5 \neq e$, hence $|xy| \neq 5$. Likewise, $|xy| = 7$ implies that $x^7 y^7 = x^7 = x^2 \neq e$, hence $|xy| \neq 7$. Finally $|xy| \neq 1$, as this would imply that $xy = e$, but then $x = y^{-1}$, and by a previously proven theorem (in the homeworks) it would follow that x and y have the same order, and by supposition they do not. Hence $|xy| = 35$. Furthermore, by theorem it follows that $| < xy > | = |G|$, hence $< xy >= G$, so G is cyclic. Q.E.D.

remark! Additionally, the proof also works after replacing 35 by 33.

remark!!! Does this work so long as we have exactly 2 prime factors for our replacement integer? Are there any other integers that work?

lemma Let $x, y \in G$ such that $xy = yx$, then $|xy| = \mathrm{lcm}(|x|, |y|)$.

proof Let x, y be as stated. Let $a = |x|$ and $b = |y|$. Then

proposition Let G be an Abelian group of order 35 such that every element in G satisfies the equation $x^{35} = e$. If n is square free and has 2 prime factors, then G is cyclic.

49, proposition For each $n \in \mathbb{N}$, there are exactly $\phi(n)$ elements of order n in $\mathbb{C}^*$.

proof * (forgot to specify that n is a positive divisor of n) Let n be some arbitrary natural number. Let x be an arbitrary element of $\mathbb{C}^*$ such that $x^n = 1$.. Then this becomes the equation for the roots of unity, $x^n - 1 = 0$. The n the roots of unity. Hence we have the set $\{x : x = e^{2\pi k i/n}\}$ for $k = 1, \ldots, n$. Simple calculation reveals that this is a cyclic group generated by $e^{2\pi i/n}$, which has order n, call it $< 1^{1/n} >$. Then since $n|n$, by theorem 4.4 the number of elements of order n in $1^{1/n}$ (this notation is used in our complex analysis textbook) is $\phi(n)$. Hence the number of elements in $\mathbb{C}^*$ with order n is exactly $\phi(n)$.

Q.E.D.

remark This example shows that there can be an element in a group of infinite order with finite order! That seems strange and amazing!

58, question How many solutions are there to the equation $x^{15} = e$ in a cyclic group G where $15||G|$?.

thoughts By the fundamental theorem of finite cyclic groups, we know that there must be exactly one subgroup of G with order 15, as 15 must be a positive divisor of $|G|$. Call it $< x >$ for some $x \in G$. By another theorem, each set of elements whose orders divide 15 must be a subgroup of this group. So there are exactly 15 elements in G which satisfy this equation.

Actually, since G is cyclic it follows that for each divisor of the order of G, d, the number of elements whose orders are d is $\phi(d)$. If $x^{15} = e$, then by another theorem it follows that $|x||15$. So to account for each $x \in G$ which satisfies this condition we should also account the divisors, which, since divisibility is "transative," are also divisors of $|G|$ (in this case 15). The positive divisors of 15 are $1, 3, 5, 15$. Hence the number of solutions in G to the equation $x^{15} = e$ is $\phi(1) + ...\phi(15) = 1 + 2 + 4 + 8 = 15$.

Also, from number theory we have a theorem that says that the sum of $\phi(d)$ for all positive divisors such that $d|n$ is n. In summation notation,

$$\sum_{d|n} \phi(n) = n.$$

So we can generalize the statement as follows:
$\boxed{\text{proposition: 58}}$ If G is a cyclic subgroup and n is a natural number such that $n||G|$, then the number of elements $x \in G$ such that $x^n = e$ is exactly n.

$\boxed{\text{proof}}$ Let G be as stated in the proposition. Since G is cyclic, by a previously proven theorem (theroem 4.4) it follows that since n is a positive divisor of the order of G, there exists $\phi(n)$ elements in G whose order are n, hence these satisfy the condition that $x^n = e$. But by another previously proven theorem, $x^n = e$ if and only if $n||x|$. Hence for each positive divisor d of n, we have $\phi(d)$ more solutions. In other words, we have

$$\sum_{d|n} \phi(n)$$

elements x in G such that $x^n = e$. By a result from number theory, this is just n. Q.E.D.

$\boxed{\text{36, proposition}}$ Suppose that G is a group that has exactly one nontrivial proper subgroup. Prove that G is cyclic and $|G| = p^2$, where p is prime.

$\boxed{\text{proof}}$ Suppose that G is a group. Let H be its only nontrivial proper subgroup. Then there exists a $x \in G$ that is not in H. Next, consider the cyclic subgroup that is generated by x: $< x >$. This subgroup cannot be another proper subgroup, nor is it the trivial subgroup. Hence, $< x >$ must be G, which implies that G is cyclic.
Furthermore, by Theorem 4.3 there exists exactly one subgroup for every divisor of $|G|$. Since G has only one proper nontrivial subgroup, this means that $|G|$ has only one divisor that is not 1 and not itself. Thus, it follows that $|G| = p^2$, which can only be divided by 1, p and p^2.