Abstract Algebra

August, Evelyn

9/21/2021

$\boxed{\text{Ch3, 4, proposition}}$ In any group, an element an its inverse have the same order.

$\boxed{\text{"lemma"}}$ Let x be an arbitrary element of a group. Let n be an arbitrary positive integer such that $x^n = e$. Then it follows that $(x^{-1})^n = e$.

$\boxed{\text{proof}}$ By the associative law of groups it follows that $x^n = xx^{n-1} = e$. Hence by definition of the inverse, $x^{n-1} = x^{-1}$. Hence we have $(x^{-1})^n = (x^{n-1})^n = x^{n(n-1)} = (x^n)^{n-1} = e^{n-1} = e$.

$\boxed{\text{proof}}$ Let G be an arbitrary group, and let x be an arbitrary element in G. This proof will be broken up into two cases: infinite and finite order.

Suppose that $|x| = \infty$. By the inverse property of groups (do I have to say this, or could I jump right to it and let this be implied by the fact that G is a group), there exists some $x^{-1} \in G$ such that $xx^{-1} = e$. Suppose by way of contradiction that $x^{-1} = x^n$ for some positive integer n. Then we have $xx^n = e$. But it follows then that $x^{n+1} = e$, contradicting the supposition that $|x| = \infty$.

Suppose then that $|x| = n$ for some positive integer n. Then it follows that $x^n = e$. Furthermore, by the associative law of groups it follows that $x^n = xx^{n-1} = e$. Hence by definition of the inverse, $x^{n-1} = x^{-1}$. Hence we have $(x^{-1})^n = (x^{n-1})^n = x^{n(n-1)} = (x^n)^{n-1} = e^{n-1} = e$.

Having shown that n is a positive integer such that $(x^{-1})^n = e$, it remains to be shown that it is the smallest such integer. Suppose then by way of contradiction that there exists some positive integer $m > n$ such that $(x^{-1})^m = e$. By the lemma it follows that $x^m = e$. But this is a contradiction.

$\boxed{\text{Ch 3, 77, proposition}}$ Let x be an arbitrary element of a group, G, such that $|x| = m$. Let n be an arbitrary positive integer. If $\gcd(m, n) = 1$, then $x = y^n$ for some $y \in G$.
$\boxed{\text{proof}}$ Let x be an arbitrary element of an arbitrary group G. Suppose that $|x| = m$, and let n be a positive integer such that $\gcd(m, n) = 1$. By Bazout's identity it follows that $1 = ma + nb$ for integers a and b. Hence we have $x = x^1 = x^{ma+nb} = x^{ma}x^{nb} = (x^m)^a(x^b)^n = (e)^a(x^b)^n = (x^b)^n$. Call $x^b = y$. To be extra meticulous, applying the closure property it follows that $y \in G$. Since x is arbitrary, it follows that for all x in a group, there exists some positive integer n such that $gcd(n, m) = 1$ and $x = y^m$.

$\boxed{\text{Ch 4, 39, find a group with exactly six subgroups}}$. Try $\mathbb{Z}_6$ under addition? There is of course the trivial subgroup, $\{0\}$. Then there is itself. Then there $\{2, 4, 0\} =< 2 >$. Then there is $< 3 >= \{0, 3\}$ Nope, that is only four. How about I try $\mathbb{Z}_{2^5}$ under addition. Yep, then I'd have $< 0 = 32 >, < 1 >, < 2 >, < 4 >, < 8 >$ and $< 16 >$. This is six. Here's my generalization: cyclic groups with orders which have n divisors must have exactly n subgroups. This is a direct corollary of the fundamental theorem of cyclic subgroups.

$\boxed{\text{Ch 4, 40, thoughts}}$ We want to find a generator for $< m > \cap < n >$ given arbitrary $m, n \in \mathbb{Z}$. Try this, $\text{lcm}(m,n)$. This seems to follow intuitively, because this will have less things relatively prime to it, hence less things "asseccible" to it. Let's try it out.

$\boxed{\text{proposition}}$ Let $m, n \in \mathbb{Z}$ under addition. Let $\text{lcm}(m,n) = a$. Consider the cyclic subgroup $< a >$. The rest of this proof shall be a sort of set-equality proof (as the operation is inherited and these are groups by definition of cyclic groups), to show that $< a > \leq < m > \cap < n >$ and $< m > \cap < n > \leq < a >$. Let $g = pa$ for some integer p be an arbitrary element of $< a >$. Definition of the least common multiple, $m|a$ and $n|a$. Hence there exist integer q, r such that $qm = a$ and $rn = a$. Then by definition of $< a >$ and $< m >$, it follows that $a \in < m >$ and $a \in < n >$. Furthermore, also by the definition of cyclic groups, since p is an integer, $g = pa \in < m >$ and $g = pa \in < n >$. Then by definition of intersection, $g \in < m >$ and $g \in < n >$. Since g is arbitrary, this applies to all g, hence $< \text{lcm}(m,n) > \subseteq < m > \cap < n >$

Now let x be an arbitrary element in $< m > \cap < n >$. Then it follows by definition of intersection that $x \in < m >$ and $x \in < n >$. By definition of cyclic groups, there exists integers p and q such that $pn = x = qm$. By definition of division, it follows that $n|x$ and $m|x$. By definition of the least common multiple (and the easily proven property that anything which divides both of the numbers whose least common multiple is common to must also be a multiple of the least common multiple), it follows that $a|x$. By definition of divisibility, there exists some integer y such that $ya = x$. By definition of $< a >$, it follows that $x \in < a >$. Since x is arbitrary, this applies to all elements of $< m > \cap < n >$, hence $< m > \cap < n > \leq \mathbb{Z}$.

By set equality and the fact that both of these things are groups, it follows that

$$< m > \cap < n > = < \text{lcm}(m,n) > .$$

$\boxed{\text{remark}}$ So then, is it true that $< m > \cup < n > = < \gcd(m,n) >$?

$\boxed{\text{proof}}$ This proof is left as an exercise for the reader.

$\boxed{\text{Ch 4, 82, proposition}}$ Let $G = \{ax^2 + bx + c : a, b, c \in \mathbb{Z}_3\}$. Under addition (mod 3), assume that G is a group. Then $|G| = 27$ and G not cyclic.

$\boxed{\text{proof}}$ First I shall prove that $|G| = 27$. Since there are three possible values for each respective coefficient, we have $3^3 = 27$ different possibilities, hence $|G| = 27$.

Suppose that G is cyclic. By the fundamental theorem of cyclic groups, there must be exactly one subgroup of order k. Now let g be an arbitrary element of G. By definition of G, $g = [a]x^2 + [b]x + [c]$ for some $[a], [b], [c] \in \mathbb{Z}/(3)$. Consider $3g = ([a] + [a] + [a])x^2 + ([b] + [b] + [b])x + ([c] + [c] + [c])$. By properties of addition of modular congruence classes, $g = [3a]x^2 + [3b]x + [3c] = [3][a]x^2 + [3][b]x + [3][c] = [0]$, which is the identity element in G. Since g is arbitrary, it follows that $3g = e$ for all $g \in G$. But by the fundamental theorem there must exist some $h \in G$ such that $|h| = 27$. Since 3 is less than 27, and since by what we have just shown, $3h = e$, 27 cannot be the order of h. Hence we arrive at a contradiction, so G must not be cyclic.