Abstract Algebra

August, Evelyn

9/14/2021

$\boxed{\text{Ch2, 37}}$ Let G be a finite group. Then the number of elements x such that $x^3 = e$ is odd, and the number of elements y such that $y^2 \neq e$ is even.

$\boxed{\text{proof}}$ Let G be an arbitrary group and let $|G|$ be the order of G.

- Let S be the set of all elements x in G such that $x^3 = e$. Clearly $e \in S$, as by definition $e^3 = e$. This proof will first show that each element besides e has a distinct inverse in S. Adding e into the mix would show that $|S| = 2n + 1$ for some non-negative integer n, hence n would be odd. To show this, we will break this into two steps.
  - First we shall show that for each element in $x \in S$, $x^{-1} \in S$. By the group axiom of associativity, it follows that $x^3 = x(x^2) = (x^2)x = e$. By definition of inverses, $x^{-1} = x^2$. Furthermore, observe that $(x^{-1})^3 = (x^2)^3 = (x^3)^2 = e^2 = e$.
    Hence $x^{-1} \in S$.
  - Now we shall show that for all $x \in S$ such that $x \neq e$, $x^{-1} \neq x$. We shall proceed by contraction. Suppose by way of contradiction that $x \neq e$ and $x = x^{-1}$. Then by supposition $e = x^{-1}x = x^2$. Operating on both sides, we have $ex = x = x^3 = e$. But by supposition, $x \neq e$, hence a contradiction. Thus it follows by way of contradiction that whenever an element $x \in S$ is not e, then x is distinct from x^{-1}.

  Having shown that for every x in S not equal to e, there exists another element x^{-1} in S, it follows that $|S - \{e\}| = 2n$ for some non-negative integer n. Adding in e, $|S| = 2n + 1$, hence by definition of S the number of elements $x \in G$ such that $x^3 = e$ is odd. Q.E.D.

- Let S be a subset of G such that each element $x \in S$ has the property that $x^2 \neq e$. Note that S could be empty, in which case the proposition holds. Suppose then that S is not empty. Let x be an arbitrary element of S. First we shall show that each element $x \in S$, $x^{-1} \in S$. Then we shall show that if each $x \in S$ is distinct from its inverse.
  - Let x be an arbitrary element in S. By the inverse property of groups, $x^{-1} \in G$. By the associative property of groups, it is clear that $(x^{-1})^2 x^2 = x^{-1}x^{-1}xx = x^{-1}(x^{-1}x = e)x = e$, hence $(x^{-1})^2 = (x^2)^{-1}$. Furthermore, since $x^2 \neq e$, it follows that $(x^{-1})^2 x^2 \neq (x^{-1})^2 e$, hence $e \neq (x^{-1})^2$. By definition of S, it follows that $x^{-1} \in S$.
  - Once again, let x be an arbitrary element in S. Now to show that x^{-1} is distinct from x, suppose that the contrary is true. Then we have $x = x^{-1}$. It would follows by the associative and inverse properties of groups that $x^2 = xx^{-1} = e$, contradicting the supposition that $x \in S$. Hence it follows that for all x in S, the inverse of x is distinct from x.

  By the uniqueness property of inverses in a group, it follows that for every element in S there is exactly one other element in S (it's inverse). In other words, $|S| = 2n$ for some nonzero integer n, so there is an even number of elements x in G such that $x^2 \neq e$. Q.E.D.

$\boxed{\text{Ch 3, 31}}$ For each divisor k>1 of n, let $U_k(n) = \{x \in U(n) | x \mod k = 1\}$.
a) List the elements of $U_4(20), U_5(20), U_5(30)$, and $U_{10}(30)$.
b) Prove that $U_k(n)$ is a subgroup of $U(n)$.
c) Let $H = \{x \in U(10) | xmod3 = 1\}$. Is H a subgroup of U(10)?

a)

$$U(n) = \{[x]_n : gcd(x, n) = 1\}$$

$$U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$$

$$U(30) = \{1, 7, 11, 13, 17, 19, 23, 29\}$$

$$U_4(20) = \{1, 9, 13, 17\}$$

$$U_5(20) = \{1, 11\}$$

$$U_5(30) = \{1, 11\}$$

$$U_{10}(30) = \{1, 11\}$$

b)

$$U_k(n) \leq U(n)$$

(finite subgroup test)
Let n be an arbitrary positive integer greater than 1. Let $k > 1$ be an arbitrary divisor of n.
We know that $U(n)$ is a finite group, which implies that the subset $U_k(n)$ is also finite. Furthermore, the identity element, 1, is an element of U(n), since $\gcd(k, 1) = 1$ for all $1 < k \in \mathbb{N}$. Furthermore, 1 is also an element of $U_k(n)$, since $1 \in U(n)$ and $1 \mod k = 1$ for all $k \in \mathbb{N}$. Thus, the subset is non-empty.

Let a and b be arbitrary elements of $U_k(n)$. We know, by definition, that $amodk = 1$ and $b \mod k = 1$. Since $[a] \cdot [b] = [a \cdot b]$, we know that $ab \mod k = 1$. Thus, $ab \in U_k(n)$ for all $a, b \in U_k(n)$.

c)

$$U(10) = \{1, 3, 7, 9\}$$

$$H = U_k(10) = \{1, 7\}$$

Yes, H is a subgroup of U(10). This can be seen by showing that $[7][7] = [1][1] = [1]$. Also we can use the previously proven result.

$\boxed{\text{Ch 3, 32: proposition}}$ If G is a group, and H and K are subgroups of G, then it follows that $H \cap K$ is a subgroup of G.

$\boxed{\text{proof}}$ Let G be an arbitrary group, and let H and K be arbitrary subgroups of G. First we must show that $H \cap K$ is nonempty. By definition of a subgroup, H and K must share the identity element. Hence $H \cap K \neq \emptyset$. Let a be an arbitrary element of $H \cap K$. By intersection, it follows that $a \in H$ and $a \in K$. Furthermore, by the group axioms it follows that there is an inverse, a^{-1} in both H and K. Hence the inverse property is satisfied.
Now let $a, b \in H \cap K$ be arbitrary elements. By intersection it follows that $a, b \in H$ and $a, b \in K$. Furthermore, since H and K are subgroups, by the group axioms it follows that $ab \in H$ and $ab \in K$. By intersection, it follows that $ab \in H \cap K$. Since a and b are arbitrary, it follows that this works for all elements in $H \cap K$, hence $H \cap K$ is closed under the group operation of G. By the two step subgroup test it follows that $H \cap K$ is a subgroup of G. Q.E.D.

$\boxed{\text{proposition}}$ Given any number of subgroups of G, the intersection of all of these subgroups is also a subgroup.
$\boxed{\text{proof}}$
Let H and K be subgroups of G for some group G. By the previously proven result, $H \cap K \leq G$. We shall proceed by induction, so let this be the base case.
Now for the induction hypothesis, suppose that for some $n \in \mathbb{N}$,

$$H = \bigcap_{i \leq n} H_i : \text{for } H_i \leq G$$

such that $H \leq G$. For the induction step, we have for subgroups of G, $H_1, \ldots, H_{n+1}$,

$$\bigcap_{i \leq n+1} H_i = H \cap H_{n+1}.$$

By the previously proven result, this is a subgroup of G. Hence by way of induction, it follows that the intersection of any collection of subgroups in a group is also a subgroup. Q.E.D. (Induction may have been overkill).

$\boxed{\text{Ch3, 68: proposition}}$ Let $H = \{A \in GL(2, \mathbb{R}) : \det A = 2^p, \exists p \in \mathbb{Z} \text{ ; for } m, n = 1, 2; \}$. Then $H \leq GL(2, \mathbb{R})$.
$\boxed{\text{proof}}$ Consider the identity matrix I_4. Clearly $\det I_4 = 1 = 2^0$, and $0 \in \mathbb{Z}$. Hence by definition of H, $I_4 \in H$ and H is nonempty. Let A be an arbitrary element in H. By definition of H, since 0 is not an integer power of 2, the determinate of A cannot be zero, hence by the results of linear algebra there must exist some A^{-1} in $GL(2, \mathbb{R})$. Furthermore, by definition of H, there must exist some integer $n \in \mathbb{Z}$ such that $\det A = 2^p$. Furthermore, by the results of linear algebra, $\det A^{-1} = 1/2^p = 2^{-p}$. Since $\mathbb{Z}$ is a group, $-p \in \mathbb{Z}$:). By definition of H, it follows that $A^{-1} \in H$.
Now let A and B be arbitrary elements in H. By definition of H, we know $\det A = 2^m$ and $\det B = 2^n$ for some $m, n \in \mathbb{Z}$. Applying the results of linear algebra, $\det(AB) = \det A \det B = 2^m 2^n = 2^{m+n}$. Since $\mathbb{Z}$ is a group, it follows by the closure property of groups that $m, n \in \mathbb{Z}$. Hence by definition of H $AB \in H$. Since A and B are arbitrary elements in H, it follows that H is closed under the group operation.
By the two step subgroup test, it follows that since each element in H has an inverse, and since H is closed under the group operation, $H \leq GL(2, \mathbb{R})$.

$\boxed{\text{Ch 3, 70}}$ Let $(G, \cdot)$, (from now on call it G), be a group real valued functions under multiplication $f : \mathbb{R} \to \mathbb{R}^*$ for some set $\mathbb{R}^* \subseteq \mathbb{R}$, where multiplication is defined $f \cdot g : \mathbb{R} \to \mathbb{R}^*$ such that $f \cdot g(x) = f(x)g(x)$. Let H be a subset of G defined $H = \{f \in G | f(2) = 1\}$.

$\boxed{\text{proof}}$ Let H be an arbitrary subset of G. First, we must show that H is nonempty. Consider the function $e(n) = 1$ for all $e \in \mathbb{R}$. By definition $f \in H$Let f, g be arbitrary elements in H. By definition of H, $f(2) = 1 = g(2)$. Furthermore, since by definition of function multiplication, $f \cdot g(2) = f(2)g(2) = (1)(1) = 1$, we find that the function $f \cdot g$ is also in H. Hence H is closed under the group operation of G.
Now let f be an arbitrary element in H. Since $f \in G$, by the group axioms f must have an inverse f^{-1}. Confusingly, this will not be the identity map on the reals, as our group operation here is not function composition but function multiplication. Hence f^{-1} is the function defined $f^{-1}(x) = 1/f(x)$. Furthermore, observe that $1/f(2) = 1/1 = 1$, hence $f^{-1} \in H$. Since f is arbitrary, it follows that each element in H has an inverse.
By the two step subgroup test, $H \leq G$. Q.E.D.