TheNumbersBook.com 2010

Dummit & Foote 1.1 # 8, 22, 25, 26, 27, 31

1.1.8 Let $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$.

(a) Prove that G is a group under multiplication (called the group of *roots of unity* in $\mathbb{C}$).

(b) Prove that G is not a group under addition.

(a) First, note that for any $z, z' \in G$ such that $z^m = 1, z'^n = 1$, then $(zz')^{nm} = (z^m)^n(z'^n)^m = 1 * 1 = 1$. Thus $zz' \in G$ (closure under multiplication). Furthermore, $1 \in G$ is the identity and for any $z \in G$, we also have $z^{n-1} \in G$ (because $(z^{n-1})^n = (z^n)^{n-1} = 1$). But $z * z^{n-1} = z^n = 1$ so z^{n-1} is the inverse of z. Finally, note that for $z, z', z'' \in G$ we have $(zz')z'' = z(z'z'')$ because $z, z', z'' \in \mathbb{C}$ (associativity holds under complex numbers).

(b) The additive identity in $\mathbb{C}$ is 0. But $0 \notin G$ as there is no natural number n such that $0^n = 1$.

■

1.1.22 If x and g are elements of the group G, prove that $|x| = |g^{-1}xg|$. Deduce that $|ab| = |ba|$ for all $a, b \in G$.

Let $g^{-1}, x, g \in G$. Assume $|g^{-1}xg| = n$, then $(g^{-1}xg)^n = e$, by definition. We want to show that $|x| = n$. Then,

$$\begin{aligned}
e &= (g^{-1}xg)^n \\
&= (g^{-1}xg)(g^{-1}xg)\cdots(g^{-1}xg) \\
&= g^{-1}xgg^{-1}xg\cdots g^{-1}xg \\
&= g^{-1}x(gg^{-1})x(g\cdots g^{-1})xg \\
&= g^{-1}x^n g \\
g &= x^n g \\
e &= x^n
\end{aligned}$$

This shows that $|x| = n$. We now want to deduce that $|ab| = |ba|$. Let $a = g^{-1}x$ and $b = g$. Then,

$$|ab| = |(g^{-1}x)g| = |x| = |(gg^{-1}x)| = |g(g^{-1}x)| = |ba|$$

■

1.1.26 Assume H is a nonempty subset of $(G, \star)$ which is closed under the binary operation on G and is closed under inverses, i.e., for all h and $k \in H$, hk and $h^{-1} \in H$. Prove that H is a group under the operation $\star$ restricted to H (such a subset H is called a *subgroup* of G).

If $h, h^{-1} \in H$, then $hh^{-1} = 1 \in H$ because it is closed under operation of G. Thus, H has an identity element. Finally, for any $h, k, j \in H$, we have $(hk)j = h(kj)$ since $h, k, j \in G$ and H is closed under operation of G. Thus, H is associative. The three axioms of a group are satisfied, so H is a *subgroup* of G. ■

1.1.27 Prove that if x is an element of the group G then $\{x^n \mid n \in \mathbb{Z}\}$ is a subgroup (cf. the preceding exercise) of G (called the *cyclic subgroup* of G generated by x).

From previous problem, it is sufficient to show H is non-empty, closed under operation and under inverses. H is clearly non-empty. Consider two $x^n, x^m \in H$. Then $x^n x^m = x^{n+m} \in H$ as $n + m \in \mathbb{Z}$. Also, for $x^n \in H$, $x^{-n} \in H$ (which is the inverse of x^n. ■

1.1.31 Prove that any finite group G of even order contains an element of order 2. [Let $t(G)$ be the set $\{g \in G \mid g \neq g^{-1}\}$. Show that $t(G)$ has an even number of elements and every nonidentity element of $G - t(G)$ has order 2.]

Let $t(G) = \{g \in G \mid g \neq g^{-1}\}$. Since $g \neq g^{-1}$ then, similarly, $(g^{-1})^{-1} \neq g$ so $t(G)$ creates a parity of elements that do not equal their own inverses. So $t(G)$ is of even order. Since G is a finite group of even order, then $G - t(G)$ is also a finite group of even order. Since $G - t(G) = \{g \in G \mid g = g^{-1}\}$ then $g = g^{-1}$ or $g^2 = e$ for a non-identity element g. This means that $|g| = 2$, as desired. Alternatively: we could have proved this problem using indeces. ■