Mathematics 243 – Algebraic Structures, section 1
Selected Solutions – Problem Set 6
November 14, 2003

3.2/11. Let H be a subgroup of a group G, let $a \in G$ be a fixed element, and let

$$K = \{x \in G | x = aha^{-1}, \text{ some } h \in H\}$$

We must show K is a subgroup of G. First, $e \in K$, since $e = aea^{-1}$, and $e \in H$ because H is a subgroup. Next, if $x, y \in K$, we must show that $xy \in K$. Saying $x \in K$ means $x = aha^{-1}$ for some $h \in H$. Similarly $y \in K$ means $y = aka^{-1}$ for some $k \in H$. Then

$$xy = (aha^{-1})(aka^{-1}) = ah(a^{-1}a)ka^{-1} = aheka^{-1} = ahka^{-1}$$

Since H is a subgroup and $h, k \in H$, we have $hk \in H$. Therefore $xy \in K$. Finally, we must show that if $x \in H$, then $x^{-1} \in H$ too. But note by the "reverse order law",

$$x^{-1} = (aha^{-1})^{-1} = (a^{-1})^{-1}h^{-1}a^{-1} = ah^{-1}a^{-1}$$

Since H is a subgroup of G and $h \in H$, $h^{-1} \in H$. This says $x^{-1} \in K$. We have verified all three of the conditions of Theorem 3.9 in the text, so K is a subgroup of G.

3.2/12. Let G be an abelian group (i.e. the group operation is commutative), and let $H = \{x \in G | h^{-1} = h\}$. In other words, H is the set of elements in G that *are their own inverses*. We want to show that H is a subgroup of G. First, since $e^{-1} = e$ for the identity e in G, $e \in H$, so H is nonempty. Next, if $h, k \in H$, so $h = h^{-1}$ and $k = k^{-1}$, then by the reverse order law and commutativity,

$$hk = h^{-1}k^{-1} = (kh)^{-1} = (hk)^{-1}.$$

Hence $hk \in H$ (because it is its own inverse). Finally, since $h^{-1} = h$ for all $h \in H$, every element in H has an inverse in H (itself!!). We have verified all three of the conditions of Theorem 3.9 in the text, so H is a subgroup of G.

3.12/17. Let G be a group, and let

$$Z(G) = \{a \in G | ax = xa, \text{ all } a \in G\}$$

We must show $Z(G)$ is a subgroup of G. First, $e \in Z(G)$, since $ex = xe = x$. Next, if $a, b \in Z(G)$, we must show that $ab \in Z(G)$. Saying $a \in Z(G)$ means $ax = xa$ for all $x \in G$. Similarly $b \in Z(G)$ means $bx = xb$ for all $x \in G$. Then using associativity and these properties we have for any $x \in G$:

$$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$$

Hence ab also commutes with every x in G, so $ab \in Z(G)$. Finally, we must show that if $a \in Z(G)$, then $a^{-1} \in Z(G)$ too. From the equation $ax = xa$, if we multiply on both

sides on the left and right by a^{-1} we have $a^{-1}(ax)a^{-1} = a^{-1}(xa)a^{-1}$. Regrouping by associativity, and cancelling when we can this gives $xa^{-1} = a^{-1}x$ for all x in G. Hence $a^{-1} \in Z(G)$. We have verified all three of the conditions of Theorem 3.9 in the text, so $Z(G)$ is a subgroup of G.

3.3/13a. First, we show by induction on n that

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^n = \begin{pmatrix} \cos n\theta & -\sin n\theta \\ \sin n\theta & \cos n\theta \end{pmatrix}$$

for all $n \geq 1$. The base case is completely obvious (nothing to prove). So assume that

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^k = \begin{pmatrix} \cos k\theta & -\sin k\theta \\ \sin k\theta & \cos k\theta \end{pmatrix}$$

and consider

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^{k+1} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^k \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

By the induction hypothesis, this is

$$\begin{pmatrix} \cos k\theta & -\sin k\theta \\ \sin k\theta & \cos k\theta \end{pmatrix} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} =$$

$$\begin{pmatrix} \cos k\theta\cos\theta - \sin k\theta\sin\theta & -\cos k\theta\sin\theta - \sin k\theta\cos\theta \\ \cos k\theta\cos\theta + \sin k\theta\sin\theta & \cos k\theta\cos\theta - \sin k\theta\sin\theta \end{pmatrix}$$

Using the trig identities

$$\cos(A+B) = \cos(A)\cos(B) - \sin(A)\sin(B), \quad \sin(A+B) = \sin(A)\cos(B) + \sin(B)\cos(A)$$

this last matrix equals

$$\begin{pmatrix} \cos(k\theta+\theta) & -\sin(k\theta+\theta) \\ \sin(k\theta+\theta) & \cos(k\theta+\theta) \end{pmatrix} = \begin{pmatrix} \cos(k+1)\theta & -\sin(k+1)\theta \\ \sin(k+1)\theta & \cos(k+1)\theta \end{pmatrix}$$

which is what we wanted to show. To be complete, to finish part a, we should also show that the negative powers of $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ have the same form. To see this note by our general formula for 2×2 inverse matrices, since $\det \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = \cos^2\theta + \sin^2\theta = 1$, we have

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^{-1} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} \cos -\theta & -\sin -\theta \\ \sin -\theta & \cos -\theta \end{pmatrix}$$

because of the identities $\sin(-\theta) = -\sin\theta$ and $\cos(-\theta) = \cos(\theta)$. Hence the negative powers of $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ will come from the matrices of the same form with negative integer multiples of θ.

3.3/14 and 15. We can show both of these simultaneously by showing that the set G of all $[a]$ in $\mathbf{Z}_n$ with $\gcd(a, n) = 1$ is a group under multiplication mod n. We know that multiplication mod n is associative in all cases, so it is associative on the subset of classes which have multiplicative inverses. We are including exactly the elements in $\mathbf{Z}_n$ that do have multiplicative inverses, so every element of G has an inverse for multiplication and that inverse is also an element of G. The element $[1] \in G$ is an identity for multiplication. So the only thing that must be proved is that G is closed under multiplication. If $\gcd(a, n) = \gcd(b, n) = 1$, then we know there exist equations $am + n\ell = 1 = bp + nq$ for some integeres m, ℓ, p, q. If we multiply, we get

$$1 = (am + n\ell)(bp + nq) = (ab)pm + n(\ell p + qa + n\ell q)$$

This implies that $\gcd(ab, n) = 1$ also. Hence $[ab]$ also has a multiplicative inverse in $\mathbf{Z}_n$.