Correction of the Second Midterm Math 120B (Fall 1994)

Ali Nesin

July 21, 2002

1. Let A be an abelian group. Let $B := \{a \in A : a$ has finite order$\}$.
1a. Show that B is a subgroup of A.

Recall that $a \in A$ has finite order if and only if $a^n = 1$ for some natural number $n > 0$. Thus,

$$B := \{a \in A : a^n = 1 \text{ for some natural number } n > 0\}.$$

Since $1^1 = 1$, 1 is in B.

Assume a is in B. We want to show that a^{-1} is also in B. Since a is in B, $a^n = 1$ for some $n > 0$. Since $(a^{-1})^n = (a^n)^{-1} = 1^{-1} = 1$ (the first equality has been proved in class), a^{-1} is also in B.

Assume $a_1, a_2 \in B$. We want to show that $a_1a_2 \in B$. Since a_1 and a_2 are in B, there are positive integers n_1 and n_2 such that $a_1^{n_1}$ and $a_2^{n_2} = 1$. Now,

$$(a_1a_2)^{n_1n_2} = a_1^{n_1n_2}a_2^{n_1n_2} = (a_1^{n_1})^{n_2}(a_2^{n_2})^{n_1} = 1^{n_2}1^{n_1} = 1 \cdot 1 = 1.$$

Therefore a_1a_2 has finite order and it is in B.

1b. Show that in the group A/B, the order of every nonidentity element is infinite.

Let $aB \in A/B$ be an element of finite order. We want to show that aB is the identity element of the group A/B, i.e. we want to show that $aB = B$, i.e. we want to show that $a \in B$. Since aB has finite order, $(aB)^n$ is equal to the identity element of A/B, which is B. So, $(aB)^n = B$. But $(aB)^n = a^nB$. Hence $a^nB = B$. This means that $a^n \in B$. Note that, till now, we did not use the definition of B. Since $a^n \in B$, from the definition of B, it follows that $(a^n)^m = 1$ for some positive integer m. Hence $a^{nm} = 1$ and a has finite order. Therefore $a \in B$.

2. We consider $\mathbb{R}$ as a group under addition. Since $\mathbb{Z} \le \mathbb{R}$, we can consider the group $G := \mathbb{R}/\mathbb{Z}$.

2a. Show that every element of G can be written as $r + \mathbb{Z}$ for some unique $r \in \mathbb{R}$ with $0 \le r < 1$.

Let $a + \mathbb{Z}$ be an element of $\mathbb{R}/\mathbb{Z}$. We can write

$$a = r + z$$

for some $z \in \mathbb{Z}$ and $r \in [0, 1)$. For example, if $a = 3.14$, we can take $z = 3$ and $r = 0.14$. If $a = -5, 4$, we can take $z = -6$ and $r = 0.6$. In general z is equal to the integer part [a] of a and $r = a - [a]$. Now $a + \mathbb{Z} = r + z + \mathbb{Z} = r + \mathbb{Z}$. This shows that every element of $\mathbb{R}/\mathbb{Z}$ can be written as $r + \mathbb{Z}$ for some $r \in [0, 1)$.

We now show the uniqueness. Assume that for $0 \leq r, s < 1$, $r + \mathbb{Z} = s + \mathbb{Z}$. We want to show that $r = s$. Since $r + \mathbb{Z} = s + \mathbb{Z}$, $r - s \in \mathbb{Z}$. But $r - s \in (-1, 1)$. Therefore $r - s = 0$ and $r = s$.

2b. Show that if $q \in \mathbb{Q}$, then $q + \mathbb{Z}$ is an element of finite order of G.

Let $q = m/n$. Then $n(q + \mathbb{Z}) = nq + \mathbb{Z} = m + \mathbb{Z} = \mathbb{Z}$. Therefore the order of $q + \mathbb{Z}$ is finite (it divides n).

2c. Find all elements of order 2, 3 and 6 of G.

Let $r + \mathbb{Z}$ be an element of order 6 of G. By part (a), we may assume that $r \in [0.1)$. Since the order of the element $r + \mathbb{Z}$ of $\mathbb{R}/\mathbb{Z}$ is 6,

$$\mathbb{Z} = 6(r + \mathbb{Z}) = 6r + \mathbb{Z}.$$

Therefore, $6r \in \mathbb{Z}$ and r is equal to one of 0/6, 1/6, 2/6, 3/6, 4/6, 5/6. But it is easy to see that

$0/6 + \mathbb{Z}$	has order 1
$2/6 + \mathbb{Z}$	has order 3
$3/6 + \mathbb{Z}$	has order 2
$4/6 + \mathbb{Z}$	has order 3

Therefore only $1/6 + \mathbb{Z}$ and $5/6 + \mathbb{Z}$ have order 6.

Similarly, the only element of order 2 is $1/2 + \mathbb{Z}$ and the elements of order 3 are $1/3 + \mathbb{Z}$ and $2/3 + \mathbb{Z}$.

2d. For a fixed integer $n > 0$, find all elements of order n of G.

The calculations above suggest and one can prove in a similar way that the set of elements of order n is $\{n/m + \mathbb{Z} : n \text{ and } m \text{ are prime to each other}\}$.

3. Let G be a group and let $H \lhd G$ be a normal subgroup of G.

3a. Show that $C_G(H) := \{g \in G : gh = hg$ for all $h \in H\}$ is a normal subgroup of G.

We have seen in the first midterm that $C_G(H)$ is a subgroup of G for any **subset** H of G. Thus we only need to prove that $C_G(H)$ is normal in G. We have to show that for any $g \in G$,

$$g^{-1} C_G(H) g \subseteq C_G(H).$$

Let $c \in C_G(H)$. Thus c commutes with every element of H. We want to show that

$$g^{-1}cg \in C_G(H).$$

Thus we want to show that $g^{-1}cg$ commutes with every element of H. Accordingly, let h be any element of H and try to show that $g^{-1}cg$ and h commute with each other, i.e. that

$$g^{-1}cg \cdot h = h \cdot g^{-1}cg. \tag{1}$$

We know that $ghg^{-1} \in H$, because H is normal in G. Since $ghg^{-1} \in H$ and since c commutes with every element of H, c commutes with ghg^{-1}. Thus

$$c \cdot ghg^{-1} = ghg^{-1} \cdot c.$$

(1) follows from this easily.

3b. For $x \in G$, define $B(x) := \{g \in G : g^{-1}x^{-1}gx \in H\}$. Show that $B(x)$ is a subgroup of G that contains H.

Since $1^{-1}x^{-1}1x = 1 \in H$, 1 is in $B(x)$.

Let g be an element of $B(x)$. Thus

$$g^{-1}x^{-1}gx \in H \tag{2}$$

We want to show that g^{-1} is also in $B(x)$, i.e. that

$$gx^{-1}g^{-1}x \in H.$$

By (2), $(g^{-1}x^{-1}gx)^{-1} \in H$, i.e. $x^{-1}g^{-1}xg \in H$. Now using the fact that H is normal in G, we get $g(x^{-1}g^{-1}xg)g^{-1} \in H$, i.e. $gx^{-1}g^{-1}x \in H$. This is what we wanted to prove.

Let g_1, g_2 be two elements of $B(x)$. Thus

$$g_1^{-1}x^{-1}g_1x \in H \quad \text{and} \quad g_2^{-1}x^{-1}g_2x \in H. \tag{3}$$

We want to show that $g_1g_2 \in B(x)$, i.e. that $(g_1g_2)^{-1}x^{-1}(g_1g_2)x \in H$, i.e. that

$$g_2^{-1}g_1^{-1}x^{-1}g_1g_2x \in H. \tag{4}$$

Since

$$g_2^{-1}g_1^{-1}x^{-1}g_1g_2x = g_2^{-1}(g_1^{-1}x^{-1}g_1x)g_2 \cdot (g_2^{-1}x^{-1}g_2x),$$

by formulas in (3) and by the fact that H is normal in G, (4) follows.