INF 240 - Exercise problems - 2
Solutions

Nikolay Kaleyski

Exercise 1. *To show that H is a subgroup of G if and only if equation (1) holds, we have to show two things:*

- *if H is a subgroup of G, then equation (1) holds;*
- *if equation (1) holds, then H is a subgroup of G.*

We begin with the first implication, so we assume that H is a subgroup of G. Suppose we are given two elements $a, b \in H$. Since H is a subgroup, b must have an inverse b^{-1} in H. But since $a, b^{-1} \in H$ and H (as a subgroup) is closed under the group operation, we have $ab^{-1} \in H$. Thus, equation (1) holds.

Now we prove the second point, so we assume that (1) holds and we want to prove that H is a sub-group. First, we will show that the neutral element e of the group G belongs to H. Let $a \in H$ be some arbitrary element of H. Consider all powers $a^1 = a$, $a^2 = a \cdot a$, $a^3 = a \cdot a \cdot a$, etc. Since H is a finite, eventually this sequence will loop, i.e. we will have $a^k = a^n$ for some $k < n$. We thus have

$$\underbrace{a \cdot a \cdot a \cdot \cdots \cdot a}_{k \text{ times}} = \underbrace{a \cdot a \cdot a \cdot \cdots \cdot a}_{n \text{ times}}.$$

Since $a \in G$ and G is a group, a has an inverse a^{-1} such that $a^{-1} \cdot a = e$. Multiplying both sides of the above equation by a^{-1} n times, we obtain

$$a^{k-n} = e,$$

i.e. the neutral element e can be expressed as a power of a. But by equation (1) which we have assumed to be true, for any $a, b \in H$ we have $ab \in H$ (note that a and b do not have to be different elements here); we thus have $a^2 \in H$ (with $a = a$, $b = a$), $a^3 \in H$ (with $a = a^2, b = a$), etc. Ultimately, $a^k = e \in H$, so H contains the neutral element.

From equation (1), we already know that H is closed with respect to the group operation. So it only remains to show that for every element $a \in H$, its inverse a^{-1} also belongs to H. Just like we did above, for any element a, we can find some integer k such that $a^k = e$. Then a^{k-1} is the inverse of a since $a \cdot a^{k-1} = a^{k-1} \cdot a = a^k = e$.

Exercise 2. *1. By definition, $\varphi(p^s)$ is the number of integers a in the range $1 \leq a \leq p^s$ that are co-prime with p^s. Clearly, there are p^s integers in this range; if we determine how many of them are not co-prime with p^s, we merely have to subtract their number from p^s in order to arrive at the result.*

Recall that every integer k can be written as a product of powers of primes, and that this product is unique (up to rearrangement). This is referred to as the prime factorization of k. For instance, we can write $132 = 2^2 \cdot 3 \cdot 11$.

If a number a is not co-prime with p^s, then a and p^s must have a common divisor; in particular, they must both contain the same prime in their prime factorization. But since p^s is a power of a prime, this means that a must contain p (or some power of p) in its prime factorization. Thus, a must be of the form $a = p \cdot b$ for some integer b between 1 and p^{s-1}. Since we have p^{s-1} choices for b, the number of integers a that are not co-prime with p^s is exactly p^{s-1}. Hence

$$\varphi(p^s) = p^s - p^{s-1} = p^s \left(1 - \frac{1}{p}\right).$$

2. Since m and n are prime, we immediately have $\varphi(m) = m - 1$ and $\varphi(n) = n - 1$. As above, we want to calculate the number of integers a with $1 \leq a \leq mn$ that are not co-prime with mn. An integer a is not co-prime with mn if it divides m or if it divides n; and since by assumption $\gcd(m, n) = 1$, it cannot divide both m and n at the same time (unless $a = 1$).

The integers a that are not co-prime with mn must have the form bm or cn for somec, m. In the first case, we have $m, 2m, 3m, 4m, \ldots, nm$, and in the second case we have $n, 2n, 3n, 4n, \ldots, mn$: thus, we have n integers in the first case, and m it the second case. We have to subtract 1 to account for double-counting since mn appears in both lists. Thus, the number of integers a in $1 \leq a \leq mn$ that are not co-prime with mn is $(m + n - 1)$, and hence

$$\varphi(mn) = mn - (m + n - 1) = mn - m - n + 1.$$

On the other hand, we have

$$\varphi(m)\varphi(n) = (m - 1)(n - 1) = mn - n - m + 1,$$

so that the two qualities are indeed equal.

Exercise 3. *Here we have to be very careful that we interpret the symbols properly and only use the rules prescribed in the axioms from the definition of a ring. For instance, one has to remember that there is no subtraction in a ring, and $(-a)$ denotes the additive inverse of a, i.e. the inverse of a with respect to the additive operation.*

Since $a + (-a) = (-a) + a = b + (-b) = (-b) + b = 0$, we have

$$(a + (-a))(-b) = a((-b) + b).$$

Using the distributive property of the ring, we have

$$a(-b) + (-a)(-b) = a(-b) + ab.$$

By adding the additive inverse of $a(-b)$ to both sides of the above equation, the former cancels out, and we obtain

$$(-a)(-b) = ab$$

as desired.

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	7	0	1	2	3	4	5	6
2	6	7	0	1	2	3	4	5
3	5	6	7	0	1	2	3	4
4	4	5	6	7	0	1	2	3
5	3	4	5	6	7	0	1	2
6	2	3	4	5	6	7	0	1
7	1	2	3	4	5	6	7	0

Table 1: Cayley table for $(\mathbb{Z}_8, +)$

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	9	0	1	2	3	4	5	6	7	8
2	8	9	0	1	2	3	4	5	6	7
3	7	8	9	0	1	2	3	4	5	6
4	6	7	8	9	0	1	2	3	4	5
5	5	6	7	8	9	0	1	3	2	4
6	4	5	6	7	8	9	0	1	2	3
7	3	4	5	6	7	8	9	0	1	2
8	2	3	4	5	6	7	8	9	0	1
9	1	2	3	4	5	6	7	8	9	0

Table 2: Cayley table for $(\mathbb{Z}_{10}, +)$

Exercise 4. *1. The Cayley tables simply express addition modulo 8, resp. addition modulo 8, and take the form*

and

2. Since $(\mathbb{Z}_n, +)$ is a commutative group for any positive integer n, we can use the fact that any subgroup of a commutative group is normal, and simply concentrate on finding a subgroup of $\mathbb{Z}_8$, resp. $\mathbb{Z}_{10}$.

We can take $H = \{0, 2, 4, 6\}$ to be the subgroup of $\mathbb{Z}_8$ consisting of even numbers. By the statement we proved in Exercise 1, it is clear that H is indeed a subgroup of $\mathbb{Z}_8$ since the sum of two even integers is always even, and modulation by an even integer (in this case, 8) does not change the parity.

For $\mathbb{Z}_{10}$, we could also take N to be the sub-group of even integers, but we can also take e.g. $N = \{0, 5\}$. It is clear that this is a subgroup.

3. The elements of the factor groups are simply the cosets of the normal subgroup. In the case of $\mathbb{Z}_8/H$, the cosets are

$$[0] = \{0, 2, 4, 6\}$$

and

$$[1] = \{1, 3, 5, 7\}.$$

In the case of $\mathbb{Z}_{10}/N$, the cosets are

$$[0] = \{0, 5\},$$

$$[1] = \{1, 6\},$$

$$[2] = \{2, 7\},$$

$$[3] = \{3, 8\},$$

and

$$[4] = \{4, 9\}.$$

4. Since H has 4 elements, its order is 4, and its index is $8/4 = 2$. Since N has 2 elements, its order is 2 and its index is $10/2 = 5$.

5. It is easy to see that e.g. 2 generates H and 5 generates N.

6. Since $\mathbb{Z}_n$ is commutative for every positive integer n, its center is $\mathbb{Z}_n$ itself, and each element of $\mathbb{Z}_n$ lies in its own conjugacy class consisting only of itself.