

Math 417

Problem Set 2

Solutions

Work all of the following problems. Remember, you are encouraged to work together on Problem Sets, but each student must turn in his or her own write-up. Be sure to adhere to the Rules and Expectations outlined in the Course Information Sheet.

1 Traditional Problems

1. Prove that if H is a group of order 3, then H is cyclic.

Solution: If H is a group with $|H| = 3$, then $H = \{1_H, a, b\}$. Consider the element ab . If $ab = a$ then multiplying by a^{-1} on the left gives $b = 1$, a contradiction. So $ab \neq a$. Similarly, $ab \neq b$. Thus, $ab = 1$ and $b = a^{-1}$. Now consider the element a^2 . If $a^2 = a$ then $a = 1$, a contradiction. If $a^2 = 1$ then $a = a^{-1} = b$, another contradiction. Therefore $a^2 = b$ and we see that $H = \{1, a, a^2\} = \langle a \rangle$ is cyclic.

2. Let G be a group that has exactly 8 elements of order 3. How many subgroups of order 3 does G have? Explain carefully.

Solution: There will be exactly 4 subgroups of order 3. To see this, note that if $a \in G$ has order 3, then $\langle a \rangle = \{1_G, a, a^2 = a^{-1}\}$ and that a^{-1} has order 3 as well. Hence every cyclic subgroup of order 3 contains exactly 2 elements of order 3. Further, no two cyclic subgroups of order 3 can contain the same element of order 3 since then they'd both contain that element, its inverse, and, of course, the identity. Thus, since the group has 8 elements of order 3, it must contain exactly 4 cyclic subgroups of order 3. By the previous problem, every group of order 3 is cyclic, and so G must contain exactly 4 subgroups of order 3.

3. Let G be a group of even order. Prove that G has an element of order 2. (Hint: Divide the elements of G into those which are their own inverses and those which are not their own inverses. What is the parity of the latter set?)

Solution: Let S be the set of elements of G which are their own inverses and T the set of elements which are not. Then $|G| = |S| + |T|$ since S and T are disjoint. Note that $1 \in S$ since 1 is its own inverse. If $a \in S$ and $a \neq 1$ then a is an element of order 2. So all we have to show is that $|S| \geq 2$. Now note that if $x \in T$ then $x^{-1} \in T$ also. (Since if $x \in T$ then $x \neq x^{-1}$ and $x = (x^{-1})^{-1} \neq x^{-1}$.) Thus, the elements in T come in pairs, which means $|T|$ is even. Since $|G|$ is even (by hypothesis), we must have $|S|$ is even as well. Hence, $|S| \geq 2$.

4. Let G be a group and let n be a positive integer. Define the subset G^n of G by

$$G^n = \{g^n \mid g \in G\}.$$

- (a) Prove that if G is abelian, then G^n is a subgroup of G .

Solution: Note that $1_G = 1_G^n$ and so $G^n \neq \emptyset$. Let $a, b \in G^n$. Then $a = x^n$ and $b = y^n$ for some $x, y \in G$. Since G is abelian, we have $ab = x^n y^n = (xy)^n \in G^n$. Further, $a^{-1} = (x^n)^{-1} = (x^{-1})^n \in G^n$. So, by the subgroup test, we have that G^n is a subgroup of G .

- (b) Give an example of a nonabelian group G and a positive integer n such that G^n is not a subgroup of G . Explain.

Solution: Take $G = D_3$, the dihedral group of order 6. (This is the group of rigid motions of an equilateral triangle.) Then G^3 is the collection of flips, plus the identity. Since the product of two distinct flips is a nontrivial rotation, G^3 is not closed under the group operation and hence is not a subgroup of G .

5. Let H and K be subgroups of the group G . Prove that $H \cap K$ is a subgroup of G .

Solution: Since $1_G \in H$ and $1_G \in K$, we know $1_G \in H \cap K$, and so $H \cap K \neq \emptyset$. Now let $x, y \in H \cap K$. Then $xy \in H$ since H is a subgroup of G and $xy \in K$ since K is a subgroup of G . Hence $xy \in H \cap K$. Similarly, $x^{-1} \in H \cap K$. Therefore, by the subgroup test, $H \cap K$ is a subgroup of G .

2 Computer Problems

1. Use the GAP commands `ulist` and `cyclic` (see Chapter 3 of the lab manual) to determine whether the group $U(\mathbb{Z}_n)$ (or, using the book's notation, $U(n)$) is cyclic for various values of n of the form p^a where p is an odd prime and a is a positive integer. Do enough examples so that you feel comfortable making a conjecture, carefully state your conjecture, and then do a few more examples to make sure you believe it. (You do not need to prove your conjecture.) Then use GAP to decide whether your conjecture applies also to the group $U(\mathbb{Z}_{2^a})$ where a is a positive integer. Explain.

Solution: We start by putting in the function `cyclic`.

```
gap> cyclic:= function(n,a)
> local x, b, o ;
> x:= [];
> b:= 1;
> o:= One(Integers mod n);
> if Gcd(n,a) = 1 then
>   repeat
>     b:= b*a mod (n);
>     Add(x,b);
>   until b=1;
> fi;
> return x*o;
> end;
function( n, a ) ... end
```

We know that

```
Size(ulist(p^a))
```

outputs the order of the group $U(\mathbb{Z}_{p^a})$ and

```
Size(cyclic(p^a,x))
```

outputs the order of the cyclic subgroup $\langle x \rangle$ of $U(p^a)$. So if we find an x such that

```
Size(ulist(p^a))
```

is the same as

```
Size(cyclic(p^a,x))
```

, then we know that $U(\mathbb{Z}_{p^a})$ is cyclic (generated by x). Start with examples:

```
gap> Size(ulist(\mathbb{Z}_{3^2})); 6 gap> Size(cyclic(3^2,2)); 6
gap> Size(ulist(\mathbb{Z}_{3^4})); 54 gap> Size(cyclic(3^4,2)); 54
gap> Size(ulist(\mathbb{Z}_{25})); 20 gap> Size(cyclic(25,2)); 20
gap> Size(cyclic(81,2)); 54 gap> Size(ulist(81)); 54
```

So it seems to be true. It even seems in our examples that $x = 2$ always works as a generator, but I'm not willing to conjecture this in general. (Actually, it's false.) My conjecture is: For every odd prime p and every positive integer a , the group $U(\mathbb{Z}_{p^a})$ is cyclic. Now we check if it's true for $p = 2$.

```
gap> Size(ulist(8)); 4 gap> ulist(8); [ ZmodnZObj( 1, 8 ),  
ZmodnZObj( 3, 8 ), ZmodnZObj( 5, 8 ), ZmodnZObj( 7, 8 ) ] gap>  
Size(cyclic(8,1)); 1 gap> Size(cyclic(8,3)); 2 gap>  
Size(cyclic(8,5)); 2 gap> Size(cyclic(8,7)); 2
```

These commands show that $U(\mathbb{Z}_8) = \{1, 3, 5, 7\}$ but no element of $U(\mathbb{Z}_8)$ generates all of $U(\mathbb{Z}_8)$ as a cyclic subgroup. Hence $U(\mathbb{Z}_8)$ is not cyclic. (We actually already knew this from class.)