

HOMEWORK 6

Let G be a group.

- (1) Define a map $\varphi : G \rightarrow G$ by sending any $g \in G$ to g^2 . Show that φ is a homomorphism of groups if and only if G is a abelian.

Sol'n φ is a group homomorphism if and only if for all $a, b \in G$ we have $\varphi(ab) = \varphi(a)\varphi(b)$ which means

$$(ab)^2 = a^2b^2 \Leftrightarrow$$

$$abab = aabb \Leftrightarrow$$

$$bab = abb \Leftrightarrow$$

$$ba = ab \Leftrightarrow$$

G is a abelian.

- (2) Define a map $I : G \rightarrow G$ by sending any $g \in G$ to g^{-1} . Show that φ is a homomorphism of groups if and only if G is a abelian.

Sol'n The content of this statement is exactly the same as a problem given in the second homework assignment. This is because $I(ab) = (ab)^{-1}$ and $I(a)I(b) = a^{-1}b^{-1}$ and so I is a homomorphism if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$ which as we showed holds if and only if G is abelian. (recall: the proof of this went as follows:

$$(ab)^{-1} = a^{-1}b^{-1} \Leftrightarrow$$

$$aba^{-1}b^{-1} = 1_G \Leftrightarrow$$

$$aba^{-1} = b \Leftrightarrow$$

$$ab = ba \Leftrightarrow$$

G is abelian).

- (3) Show that if a homomorphism from \mathbb{Z} to itself has a non-trivial kernel, then it must be the zero map.

Sol'n If $f : \mathbb{Z} \rightarrow \mathbb{Z}$ is a homomorphism, then $f(n) = f(1 + \dots + 1) = nf(1)$. So if n is a nontrivial element of the kernel of f , then $f(n) = 0$ which implies that $0 = f(n) = nf(1)$ which implies that $f(1) = 0$. Hence for any other integer m , we have $f(m) = mf(1) = m0 = 0$ and f is the zero map.

- (4) Make a table which lists every element of \mathbb{Z}_{12} along with its order. **Sol'n**

element	0	1	2	3	4	5	6	7	8	9	10	11
order	1	12	6	4	3	12	2	12	3	4	6	12

- (5) In this problem we will explore the set of units (i.e. invertible elements) of (\mathbb{Z}_n, \cdot) .

- (a) Show that the set of elements of \mathbb{Z}_n which have a multiplicative inverse (i.e. the set of elements of $x \in \mathbb{Z}_n$ so that there exists an element $y \in \mathbb{Z}_n$ so that $xy = 1$) forms an abelian group under the operation of multiplication mod n which we will denote $U(\mathbb{Z}_n)$.

Sol'n The element $1 \in U(\mathbb{Z}_n)$ since $1 \cdot 1 = 1$ and clearly acts as the identity element of $U(\mathbb{Z}_n)$.

If $a \in U(\mathbb{Z}_n)$, then $(a^{-1})^{-1} = a$ implies that a^{-1} has a multiplicative inverse (namely a) which implies that $a^{-1} \in U(\mathbb{Z}_n)$.

Now if $x, y \in U(\mathbb{Z}_n)$ with inverses x' and y' resp., then $(xy)(x'y') = xx'y'y' = 1 \cdot 1 = 1 \pmod n$ which implies that xy has a multiplicative inverse (namely $x'y'$) which implies that $xy \in U(\mathbb{Z}_n)$. Thus multiplication in \mathbb{Z}_n restricts to a well defined binary operator in $U(\mathbb{Z}_n)$.

$U(\mathbb{Z}_n)$ is associative and abelian since the larger set \mathbb{Z}_n is.

- (b) Prove the following are equivalent
- (i) $a \pmod n \in U(\mathbb{Z}_n)$
 - (ii) a is relatively prime to n
 - (iii) a generates the additive group \mathbb{Z}_n
 - (iv) a has order n in the additive group \mathbb{Z}_n .

Sol'n

These were all in some form or another proven in class and the organizational task is left to the student (that would be YOU!)

- (c) Look up the Euler totient function either online or in a textbook. State its formula and its relevance to this sequence of problems.

Sol'n

The Euler totient function, φ is a function from the set of positive integers to itself which assigns m the number of integers less than that number which is relatively prime to m . By the previous problem we have that $\varphi(n) = |U(\mathbb{Z}_n)|$. The formula for $\varphi(n)$ is

$$\varphi(n) = n \cdot \prod_{\{p \text{ is prime}, p|n\}} \left(1 - \frac{1}{p}\right).$$

¹Technically, we only showed that $(a^{-1})^{-1} = a$ holds in a group which (\mathbb{Z}_n, \cdot) is not. However the same proof works equally well. An interesting exercise at this point for the reader to undertake is to go back to the basic lemmas concerning group theory, e.g. inverses are unique, the 1 step subgroup test, the two step subgroup test, etc and see which carry over if we only assume that our binary operator is associative or is associative with identity, etc

For example $1320 = 2^3 \cdot 3 \cdot 5 \cdot 11$ and so

$$\begin{aligned} \varphi(1320) &= 1320 \cdot \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \left(1 - \frac{1}{11}\right). \\ &= 1320 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{10}{11} \\ &= \frac{2^3 \cdot 3 \cdot 5 \cdot 11}{2 \cdot 3 \cdot 5 \cdot 11} 2 \cdot 4 \cdot 10 \\ &= 2^2 \cdot 2 \cdot 4 \cdot 10 \\ &= 2^6 \cdot 5 \\ &= 64 \cdot 5 \\ &= 320. \end{aligned}$$

- (d) Show that $U(\mathbb{Z}_5)$, $U(\mathbb{Z}_7)$, $U(\mathbb{Z}_{11})$ and $U(\mathbb{Z}_{13})$ are cyclic by explicitly finding an element of order equal to the order of the group. Make a conjecture about $U(\mathbb{Z}_p)$ (interestingly one needs a little bit of field theory in order to prove this conjecture).

Sol'n We exhibit an explicit generator in each case.

n	1	2	3	4
$2^n \pmod{5}$	2	4	3	1

So that the (multiplicative) order of the element 2 in $U(\mathbb{Z}_5)$ is 4, which is the order of that group, so $U(\mathbb{Z}_5)$ is cyclic.

n	1	2	3	4	5	6
$3^n \pmod{7}$	3	2	6	4	5	1

So that the (multiplicative) order of the element 3 in $U(\mathbb{Z}_7)$ is 6, which is the order of that group, so $U(\mathbb{Z}_7)$ is cyclic.

n	1	2	3	4	5	6	7	8	9	10
$2^n \pmod{11}$	2	4	8	5	10	9	7	3	6	1

So that the (multiplicative) order of the element 2 in $U(\mathbb{Z}_{11})$ is 10, which is the order of that group, so $U(\mathbb{Z}_{11})$ is cyclic.

n	1	2	3	4	5	6	7	8	9	10	11	12
$2^n \pmod{13}$	2	4	8	3	6	12	11	9	5	10	7	1

So that the (multiplicative) order of the element 2 in $U(\mathbb{Z}_{13})$ is 12, which is the order of that group, so $U(\mathbb{Z}_{13})$ is cyclic. From these examples the most natural conjecture one can make is that $U(\mathbb{Z}_p)$ is cyclic whenever p is prime. (Actually this is true even if p is either prime or the power of an odd prime. However, any conjecture that one can make about what an actual generator is is more than likely false.)

- (e) Show that $U(\mathbb{Z}_9)$ is cyclic but $U(\mathbb{Z}_8)$ is not.

Sol'n We refer to the problem below to see that $U(\mathbb{Z}_8)$ is not cyclic. More concretely, $U(\mathbb{Z}_8) = \{1, 3, 5, 7\}$ and the (multiplicative) order of every non-identity element is 2 ($3^2 = 9 \equiv 1 \pmod{8}$, $5^2 = 25 = 8 \cdot 3 + 1 \equiv 1 \pmod{8}$ and $7^2 = 49 = 8 \cdot 6 + 1 \equiv 1 \pmod{8}$). Since no element has order equal to the order of the group, the group is not cyclic.

On the other hand $U(\mathbb{Z}_9) = \{1, 2, 4, 5, 7, 8\}$ and

n	1	2	3	4	5	6
$2^n \pmod{9}$	2	4	8	7	5	1

- (f) More generally show that $U(\mathbb{Z}_{2^n})$ is never cyclic for n an integer ≥ 3 (**hint** show that it has too many elements of order 2).

Sol'n From class we know that any cyclic group contain at most subgroup of order 2. Since every subgroup of order 2 contains a unique element of order 2 this means that a cyclic group can contain at most one element of order 2. Now $-1 = 2^n - 1 \pmod{2^n} \in U(\mathbb{Z}_{2^n})$ has order 2 (since $(-1)^2 = 1$), and I also claim that $2^{n-1} + 1$ also has order 2. Indeed a direct calculation shows that

$$\begin{aligned} (2^{n-1} + 1)^2 &= (2^{n-1})^2 + 2 \cdot 2^{n-1} + 1 \\ &= 2^{2n-2} + 2^n + 1 \\ &\equiv 1 \pmod{2^n}. \end{aligned}$$

where the last equality holds since $2n - 2 \geq n$ (since $n \geq 3$). Lastly if

$$\begin{aligned} 2^{n-1} + 1 &= 2^n - 1 \Leftrightarrow \\ 2^{n-1} + 2 &= 2 \cdot 2^{n-1} \Leftrightarrow \\ 2 &= 2^{n-1} \Leftrightarrow \\ n - 1 &= 1 \Leftrightarrow \\ n &= 2 \end{aligned}$$

which is contrary to the assumption that $n \geq 3$. Hence $2^{n-1} + 1$ and $2^n - 1$ are two distinct elements of order 2 in $U(\mathbb{Z}_{2^n})$ and hence $U(\mathbb{Z}_{2^n})$ is not cyclic.

- (6) Let G be a group and H a subgroup of G . Suppose that m is relatively prime to the order of some element $g \in G$ and that $g^m \in H$. Then show that $\langle g \rangle \subset H$, that is every power of g is in H .

Sol'n Since m is relatively prime to the order of g , m is a generator for $\mathbb{Z}_{|g|}$. Thus there exists an integer r so that $mr \equiv 1 \pmod{|g|}$. Thus any $g^n = (g^m)^{rn}$ which is a power of an element in H and is hence in H .

- (7) Complete (with a one word answer) and prove the following: $|a| = |a^2|$ if and only if $|a|$ is ...

Sol'n The one word answer is "odd". To see why this theorem is true we as usual think of $\langle a \rangle$ as \mathbb{Z}_n where n is the order of a . Then the statement $|a| = |a^2|$ translates as the order of $1 \bmod n$ equals the order of $2 \bmod n$. This happens if and only if 2 is a generator of $\mathbb{Z}_n \Leftrightarrow 2$ is relatively prime to $n \Leftrightarrow n$ is odd.