

1. (4points) Suppose p, n, m are integers.

(a) n divides m iff $\exists k \in \mathbb{Z} \ m = kn$.

(b) p is a prime number iff $p \geq 2$ and there exists no $k \in \mathbb{Z}$ with $1 < k < n$ and k divides p .

(c) $\gcd(n, m) = d$ iff d is the largest integer which divides both n and m

(d) n and m are relatively prime iff $\gcd(n, m) = 1$.

2. (6points)(Euclid's Lemma)

The idea of this proof is to use that if p does not divide a then since p is prime, $\gcd(a, p) = 1$ and so there exists $k, l \in \mathbb{Z}$ such that $ka + lp = 1$.

3. (4points) Define $(G, *)$ is a group.

4. (7points) Suppose $(G, \cdot)$ is a group and $a \in G$.

(a) G is abelian iff $\forall x, y \in G \ xy = yx$.

(b) $|G|$ is the number of elements in G .

(c) $|a|$ is the least positive integer n such that $a^n = e$, if there is no such n then $|a|$ is infinite. Equivalently, $|a| = |\langle a \rangle|$.

(d) $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$

(e) $Z(G) = \{x \in G : \forall y \in G \ xy = yx\}$.

(f) $C(a) = \{x \in G : xa = ax\}$.

(g) $b = a^{-1}$ iff $ab = ba = e$.

5. (4points) Let $(G, \cdot)$ be any group. Prove that for any $a, b \in G$,

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

proof:

$$abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = e$$

and similarly $b^{-1}a^{-1}ab = e$.

6. (5points) Let $(G, \cdot)$ be any group. Suppose that for every a and b in G that $a^2b^2 = (ab)^2$. Prove that G is abelian.

proof: $aabb = a^2b^2 = (ab)^2 = abab$ so by multiplying on the left by a^{-1}

$$a^{-1}aabb = a^{-1}abab$$

and so

$$abb = bab$$

Multiplying on the right with b^{-1} gives

$$abbb^{-1} = babb^{-1}$$

and so $ab = ba$.

7. (3points) H is a subgroup of G if and only if

- (0) H is a nonempty subset of G .
- (1) for every $x \in H$ we have that $x^{-1} \in H$.
- (2) for every $x, y \in H$ we have that $xy \in H$.

8. (6points) Let $(G, \cdot)$ be any group and a and b elements of G such that $ab = ba$. Define

$$H = \{x \in G : axb = bxa\}$$

Prove that H is a subgroup of G using the two step method.

$axb = bxa$ implies

$$x(ba^{-1}) = (a^{-1}b)x$$

Since $ab = ba$ it follows that $ba^{-1} = a^{-1}b$. Hence $H = C(a^{-1}b)$.

9. (5points) Prove that any finite group with more than one element contains an element of prime order.

Proof: Let $a \in G$ be any element not equal to the identity. Suppose $|a| = n$. If n is prime we are done, otherwise by the Prime Factorization Theorem n has a prime divisor p . Suppose that $n = pk$. Then if $b = a^k$ we have that $b^p = a^{kp} = a^n = e$. So $|b| \leq p$. If $|b| = l < p$ then $e = b^l = a^{kl}$ which would contradict $|a| = n > kl$. Hence the order of b is p .

10. (3points) Define $\approx$ is an equivalence relation on the set X .

$\approx$ is a binary relation on X satisfying:

- (a) $\forall x \in X \quad x \approx x$
- (b) $\forall x, y \in X \quad x \approx y \Rightarrow y \approx x$
- (c) $\forall x, y, z \in X \quad (x \approx y \text{ and } y \approx z) \Rightarrow x \approx z$

11. (3points) $a \equiv_n b$ iff $\exists k \in \mathbb{Z} \quad a = b + kn$

12. (5points) Suppose $a, b, a', b', n \in \mathbb{Z}$ and $n > 1$. Prove that $a \equiv_n a'$ and $b \equiv_n b'$ implies that $ab \equiv_n a'b'$.

Proof. $a \equiv_n a'$ implies there exists $k \in \mathbb{Z}$ such that $a = a' + kn$ and $b \equiv_n b'$ implies there exists $l \in \mathbb{Z}$ such that $b = b' + ln$. Hence

$$ab = (a' + kn)(b' + ln) = a'b' + (a'l + b'k + kln)n$$

So $ab \equiv_n a'b'$.

13. (4points) Prove that 7 divides $3^{3n} + 1$ for all positive odd integers n .

Equivalently $3^{3n} + 1 \equiv_7 0$ for all odd n or $3^{3n} \equiv_7 -1$. For $n = 1$ we get that $3^3 = 27 \equiv_7 -1$. By induction assume that $3^{3n} \equiv_7 -1$ for n an odd integer and prove that the same is true for the next odd integer $n + 2$.

$$3^{3(n+2)} = 3^{3n}3^33^3 \equiv_7 (-1)(-1)(-1) = -1$$

14. (2points) Define Z_n and $\oplus_n$ where n a positive integer.

Z_n is either the set $\{0, 1, \dots, n-1\}$ or the group with this underlying set.

$\oplus_n$ is the binary operation on the set $\{0, 1, \dots, n-1\}$ defined by

$a \oplus_n b = c$ iff $a, b, c \in \{0, 1, \dots, n-1\}$ and $a + b \equiv_n c$.

15. (4points) Draw the lattice of subgroups of $(Z_{12}, \oplus_{12})$.

The subgroups of Z_n are generated by the divisors of n (including the trivial group $\langle 0 \rangle$ corresponding to the divisor n). So for Z_{12} this would be

$$\langle 0 \rangle, \langle 6 \rangle, \langle 4 \rangle, \langle 3 \rangle, \langle 2 \rangle, \langle 1 \rangle$$

For the divisors k, l we have that $\langle k \rangle$ is a subgroup of $\langle l \rangle$ iff k is a multiple of l .

16. (2points) Define the group U_n . (The set and operation.)

The underlying set is $U_n = \{k \in Z_n : \gcd(k, n) = 1\}$. The binary operation is $\otimes_n$ defined by

$a \otimes_n b = c$ iff $a, b, c \in U_n$ and $ab \equiv_n c$.

Note: U_n is a subset of Z_n but not a subgroup.

17. (4points) Write out the Cayley table for U_{12} .

$\oplus_{12}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Take Home 4-56 (5points)

The generators of Z_n are precisely the elements of U_n . For any $k < \frac{n}{2}$ we have that $\gcd(n, k) = 1$ iff $\gcd(n, n-k) = 1$. Since $n/2$ cannot be relatively prime to n it follows that the elements of U_n can be paired up and so there is an even number of them.

Take Home 4-62 (5points)

Let a be in the center of G and have prime order p . Suppose b is any element of G with prime order q . Suppose for contradiction the $p \neq q$. Then since a and b commute we have that

$$(ab)^{pq} = (a^p)^q (b^q)^p = e$$

Now since the order of ab is prime and must divide pq it must have order p or order q . But if it has order p then

$$e = (ab)^p = a^p b^p = eb^p = b^p$$

which would imply the q divides p contradicting that p and q are distinct primes. Similar if ab has order q we get a contradiction. Hence every nontrivial element of G must have order p .

18. (Extra Credit Optional Problems)

(a) Suppose G has a unique element of order 2. Prove it must be in the center of G .

(b) Prove that U_{2^n} is not cyclic.

(c) Let a, b be elements of some group and suppose $aba^{-1} = b^{-1}$ and a has odd order. Prove that $b^2 = e$.

Extra Credit is still available for these problems.

Also Extra Credit:

Prove or disprove: For any group G if for all $x \in G$ $x^3 = e$ then G is abelian.