Midterm 2

Abstract Algebra 1

MATH 3140

Fall 2022

Friday October 28, 2022

UPLOAD THIS COVER SHEET!

NAME: ______________________________

PRACTICE EXAM

SOLUTIONS

Question:	**1**	**2**	**3**	**4**	**5**	Total
Points:	20	20	20	20	20	100
Score:						

- The exam is closed book. You **may not use any resources** whatsoever, other than paper, pencil, and pen, to complete this exam.
- You **may not discuss the exam** with anyone except me, in any way, under any circumstances.
- You **must explain your answers**, and you will be **graded on the clarity of your solutions**.
- You must upload your exam as a single **.pdf** to **Canvas**, with the questions in the correct order, etc.
- You have 45 minutes to complete the exam.

1. (a) (5 points) • *Is the permutation* $\sigma = (1,6,4)(2,5) \in S_6$ *even or odd?*

SOLUTION:

$$\boxed{\sigma \text{ is odd.}}$$

We have

$$\sigma = (1,6,4)(2,5) = (1,6)(6,4)(2,5)$$

is the product of an odd number of transpositions.

(b) (5 points) *Is the permutation* σ^2 *even or odd?*

SOLUTION:

$$\boxed{\sigma^2 \text{ is even.}}$$

The square of any permutation is even.

(c) (5 points) *Compute* $|\sigma|$; i.e., the order of the element σ in the group S_6.

SOLUTION:

$$\boxed{|\sigma| = 6}$$

The order of $(1,6,4)$ is 3 and the order of $(2,5)$ is 2. As σ is equal to the product of these disjoint cycles, it follows that $|\sigma| = \operatorname{lcm}(3,2) = 6$.

(d) (5 points) *With* σ *as above and* $\tau = (5,3,2)$, *compute* $\sigma\tau$ *(as a product of disjoint cycles).*

SOLUTION:

$$\boxed{\sigma\tau = (1,6,4)(3,5)}$$

We have

$$\sigma\tau = (1,6,4)(2,5)(5,3,2) = (1,6,4)(3,5).$$

1
20 points

2. • Consider the dihedral group D_n, with $n \geq 3$. Recall the notation we have been using: D_n has identity element I, and is generated by elements R and D, satisfying the relations $R^n = D^2 = I$ and $RD = DR^{-1}$. Consider the cyclic subgroup $\langle R^2 \rangle$.

(a) (10 points) *Show that $\langle R^2 \rangle$ is a normal subgroup of D_n.*

SOLUTION:

Solution. To show that $\langle R^2 \rangle$ is normal in D_n, it suffices to check for all $g \in D_n$ that $g\langle R^2 \rangle g^{-1} \subseteq \langle R^2 \rangle$. (For a subgroup H of a group G, we have seen that H is normal if and only if $gHg^{-1} \subseteq H$ for all $g \in G$.) So let $D^a R^b \in D_n$ and let $R^{2k} \in \langle R^2 \rangle$. Then

$$D^a R^b R^{2k} (D^a R^b)^{-1} = D^a R^b R^{2k} R^{-b} D^a = D^a R^{2k} D^a = D^a D^a R^{(-1)^a 2k} = R^{(-1)^a 2k} \in \langle R^2 \rangle.$$

Thus $\langle R^2 \rangle$ is normal in D_n. □

(b) (10 points) *Find the order of the group $D_n / \langle R^2 \rangle$.* [*Hint:* this may depend on the parity of n.]

SOLUTION:

Solution.

$$\boxed{|D_n / \langle R^2 \rangle| = 2 \text{ if } n \text{ is odd, and } 4 \text{ if } n \text{ is even}}$$

To see this, we note that the order of R in D_n is n. Consequently, if n is odd, then $\langle R^2 \rangle = \langle R \rangle$, which has order n. If n is even, then $\langle R^2 \rangle \neq \langle R \rangle$ and the order of $\langle R^2 \rangle$ is $n/2$. By Lagrange's Theorem, the order of $D_4 / \langle R^2 \rangle$ is then either $2n/n = 2$ (if n is odd) or $2n/(n/2) = 4$ (if n is even). (Note that in the latter case, the quotient is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, and not to $\mathbb{Z}_4$, since the quotient has two elements of order 2, namely, the cosets $R\langle R^2 \rangle$ and $D\langle R^2 \rangle$.) □

2
20 points

3. • Recall that for a commutative ring R with unity $1 \neq 0$, we define $R[x]$ to be the ring of polynomials in x with coefficients in R. Consider the map

$$\phi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_4[x]$$

$$\sum_{k=0}^{n} a_k x^k \mapsto \sum_{k=0}^{n} [a_k] x^k,$$

where $[a_k] = a_k \pmod 4$.

(a) (10 points) *Show that ϕ is a homomorphism of rings.*

SOLUTION:

Solution. First we must show for all $p(x), q(x) \in \mathbb{Z}[x]$ that

$$\phi(p(x) + q(x)) = \phi(p(x)) + \phi(q(x)) \quad \text{and} \quad \phi(p(x)q(x)) = \phi(p(x))\phi(q(x)).$$

To do this, let us suppose that $p(x) = \sum_{k=0}^{n} a_k x^k$ and $q(x) = \sum_{j=0}^{m} b_j x^j$; since addition and multiplication are commutative, we may assume that $n \leq m$, and in fact, taking $a_k = 0$ for $k > n$, we may assume $n = m$. Then

$$\phi(p(x) + q(x)) = \phi\left(\sum_{k=0}^{n} a_k x^k + \sum_{j=0}^{n} b_j x^j\right) = \phi\left(\sum_{k=0}^{n} (a_k + b_k) x^k\right) = \sum_{k=0}^{n} [a_k + b_k] x^k$$

$$= \sum_{k=0}^{n} [a_k] x^k + \sum_{j=0}^{n} [b_j] x^j = \phi(p(x)) + \phi(q(x)).$$

Similarly,

$$\phi(p(x) \cdot q(x)) = \phi\left(\sum_{k=0}^{n} a_k x^k \cdot \sum_{j=0}^{n} b_j x^j\right) = \phi\left(\sum_{i=0}^{2n} \sum_{k=0}^{i} (a_k b_{i-k}) x^i\right) = \sum_{i=0}^{2n} \sum_{k=0}^{i} [a_k][b_{i-k}] x^i$$

$$= \sum_{k=0}^{n} [a_k] x^k \cdot \sum_{j=0}^{n} [b_j] x^j = \phi(p(x)) \cdot \phi(q(x)).$$

Thus ϕ is a homomorphism of rings. □

(b) (10 points) *Describe the kernel of ϕ.* (Do not just write down the definition; you need to describe an explicit subset of $\mathbb{Z}[x]$.)

SOLUTION:

Solution. We can describe the kernel as

$$\boxed{\ker \phi = 4\mathbb{Z}[x]}$$

Indeed, suppose that $p(x) = \sum_{k=0}^{n} a_k x^k \in \ker \phi$. Then $[a_k] = 0$ for all $k = 0, \ldots, n$. Thus $a_k \in 4\mathbb{Z}$ for all $k = 0, \ldots, n$. $\square$

3
20 points

4. (20 points) • In a commutative ring with unity, *show that* $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.

SOLUTION:

Solution. Since we are in a commutative ring with unity, when writing out

$$(a+b)^n = (a+b)(a+b)\cdots(a+b)$$

one can deduce that the number of monomials of the form $a^k b^{n-k}$ in the expansion will be $\binom{n}{k}$, corresponding to choosing k of the n factors above from which to take an a, and then taking a b from the remaining $n-k$ factors. $\square$

Here is another argument using induction. First observe that

$$\binom{n}{k-1} + \binom{n}{k} = \frac{n!}{(n-k+1)!(k-1)!} + \frac{n!}{(n-k)!k!} = \frac{n!k}{(n-k+1)!k!} + \frac{n!(n-k+1)}{(n-k+1)!k!}$$

$$= \frac{(n+1)!}{(n+1-k)!k!} = \binom{n+1}{k}.$$

Now, using this, we will prove the assertion of problem using induction. We start with the case $n=1$, and we check that

$$\sum_{k=0}^{1} \binom{1}{k} a^k b^{1-k} = b + a = (a+b)^1.$$

We now perform the inductive step. We assume that $(a+b)^m = \sum_{k=0}^{m} \binom{m}{k} a^k b^{m-k}$ for all $m \le n$ for some $n \ge 1$. We then show that

$$(a+b)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}.$$

Here is the computation:

$$(a+b)^n(a+b) = \left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\right)(a+b) = \left(\sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k}\right) + \left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k}\right)$$

$$= \binom{n}{0} b^{n+1} + \sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k}\right) a^k b^{n+1-k} + \binom{n}{n} a^{n+1}$$

$$= \binom{n+1}{0} b^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^k b^{n+1-k} + \binom{n+1}{n+1} a^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}.$$

4
20 points

5. • **TRUE** or **FALSE**. For this problem, and this problem only, **you do not need to justify your answer**.

(a) (4 points) **TRUE** or **FALSE** (circle one). The order of an element of a finite group divides the order of the group.

SOLUTION: TRUE. This follows from Lagrange's Theorem (see Thm. 10.12, p.101).

(b) (4 points) **TRUE** or **FALSE** (circle one). The symmetric group S_n is not cyclic for any $n \geq 1$.

SOLUTION: FALSE. The symmetric groups S_1 and S_2 are cyclic (of order 1 and 2, respectively).

(c) (4 points) **TRUE** or **FALSE** (circle one). Every abelian group of order divisible by 5 contains a cyclic subgroup of order 5.

SOLUTION: TRUE. By the FTFGAG, the group G is isomorphic to $\cdots \times \mathbb{Z}_{5^s} \times \cdots$ for some natural number s, and then the element $(\ldots, 0, 5^{s-1}, 0, \ldots)$ has order 5, and so generates a cyclic subgroup of order 5. (As an aside, which is not necessary for our class, one can drop the hypothesis that the group be abelian, but then the proof is harder – if you're interested, see Cauchy's Theorem, p.322.)

(d) (4 points) **TRUE** or **FALSE** (circle one). Every quotient group ("factor group") of a cyclic group is cyclic.

SOLUTION: TRUE. Under the homomorphism $\pi : G \mapsto G/N$, a generator g of G will map to the generator gN of G/N.

(e) (4 points) **TRUE** or **FALSE** (circle one). If F is a field, and R is a subring of F with unity 1_R in R equal to unity 1_F in F, then R is a field.

SOLUTION: FALSE. Take $\mathbb{Z} \subseteq \mathbb{Q}$.

5
20 points