In-Class Final

Abstract Algebra 1

MATH 3140

Summer 2021

Friday July 2, 2021

NAME: ______________________________

PRACTICE EXAM

SOLUTIONS

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

- You must have your **camera** on, and a working **microphone**, for the **duration of the exam** in order to receive credit.
- 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 60 minutes to complete the exam.

1. • 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 $R^{a_1}D^{b_1} \in D_n$ and let $R^{2k} \in \langle R^2 \rangle$ (here $k \in \mathbb{Z}$). Then

$$R^{a_1}D^{b_1}R^{2k}(R^{a_1}D^{b_1})^{-1} = R^{a_1}D^{b_1}R^{2k}D^{b_1}R^{-a_1} = R^{a_1}D^{b_1}D^{b_1}R^{(-1)^{b_1}2k}R^{-a_1} = R^{(-1)^{b_1}2k} \in \langle R^2 \rangle.$$

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.

$$|D_4/\langle R^2 \rangle| = 2 \text{ if } n \text{ is odd, and } 4 \text{ if } n \text{ is even.}$$

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 $D_n/\langle R^2 \rangle$ is then either $2n/n = 2$ or $2n/(n/2) = 4$. (Note that in the case where the quotient $D_n/\langle R^2 \rangle$ has order 4, it is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, not $\mathbb{Z}_4$, since the quotient has three elements of order 2, namely, the cosets for R, D, and RD.) □

1
20 points

2. • Consider the map (or "function") of polynomial rings

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

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

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 is commutative in $\mathbb{Z}[x]$ and $\mathbb{Z}_4[x]$, we may assume that $n \leq m$, and in fact, taking $a_k = 0$ for $k > n$, we may assume $n = m$. Then

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

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

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.

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

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 $k = 0, \ldots, n$. $\square$

2
20 points

3. (20 points) • *Show that for a prime p, the polynomial $x^p + a \in \mathbb{Z}_p[x]$ is not irreducible for any $a \in \mathbb{Z}_p$.*

SOLUTION

Solution. By Fermat's Little Theorem (see Fraleigh Corollary 20.2), we know that $b^p = b$ for all $b \in \mathbb{Z}_p$. Thus $-a$ is a root of $x^p + a$ in $\mathbb{Z}_p$. It follows from the Factor Theorem (Fraleigh Corollary 23.3) that $x + a$ is a factor of $x^p + a$. Thus, since $p \geq 2$, we have that $x^p + a$ is not irreducible for any $a \in \mathbb{Z}_p$. □

3
20 points

4. (20 points) • *Prove that the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$ is not a finite extension of $\mathbb{Q}$.*

SOLUTION

Solution. Let $\overline{\mathbb{Q}} \subseteq \mathbb{C}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. Then for each positive integer n, we have $\sqrt[n]{2} \in \overline{\mathbb{Q}}$ ($\sqrt[n]{2}$ is a root of $x^n - 2 \in \mathbb{Q}[x]$). Thus for each n we have extensions $\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q}$. If $\overline{\mathbb{Q}}$ were a finite extension of $\mathbb{Q}$, this would imply that $[\overline{\mathbb{Q}} : \mathbb{Q}] \geq [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}]$ for every n (Fraleigh Theorem 31.4). Using Eisenstein's Criterion (Fraleigh Theorem 23.15) applied to the prime $p = 2$, one can show that $x^n - 2$ is irreducible, so that $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$. In other words, if $\overline{\mathbb{Q}}$ were a finite extension of $\mathbb{Q}$, then we would have $[\overline{\mathbb{Q}} : \mathbb{Q}] \geq [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$ for every positive integer n, which is impossible. Thus $\overline{\mathbb{Q}}$ is not a finite extension of $\mathbb{Q}$. □

4
20 points

5. (20 points) • Find the degree and a basis for the field extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$.

SOLUTION

Solution. The field extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$ has degree 4, with a basis given by $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$.

To see this, we start with the extension $\mathbb{Q}(\sqrt{2})$. By Eisenstein's Criterion applied to the prime $p = 2$ (or using the fact that $\sqrt{2}$ is not rational), we see that $x^2 - 2 \in \mathbb{Q}[x]$ is irreducible, so that the extension $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ has degree 2, with basis given by $1, \sqrt{2}$ (see Theorem 29.18 or Theorem 30.23 of Fraleigh).

Next I claim that the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}(\sqrt{2})$ has degree 2, with basis given by $1, \sqrt{3}$. To prove this, it suffices to show (again, see Theorem 29.18 or Theorem 30.23) that $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2})$. Since this quadratic polynomial can only possibly factor into linear terms, it is equivalent to show that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ (see Corollary 23.3).

To show $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ assume for the sake of contradiction that $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. Then since $1, \sqrt{2}$ give a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$, we could write $\sqrt{3} = \frac{a}{b} + \frac{c}{d}\sqrt{2}$ with $a, b, c, d \in \mathbb{Z}$, and $b, d \neq 0$. Clearly $c \neq 0$, since otherwise $\sqrt{3}$ would be rational, which we know is not the case. On the other hand, I claim that $c \neq 0$, either. Otherwise, squaring both sides we would have $3 = \frac{c^2}{d^2}2$, or, rearranging, $3d^2 = 2c^2$; but the left hand side has an even number of factors of 2, while the right hand side has an odd number of factors of 2, giving a contradiction. Thus we may assume $a, c \neq 0$. Squaring both sides of $\sqrt{3} = \frac{a}{b} + \frac{c}{d}\sqrt{2}$ gives $3 = \left(\frac{a^2}{b^2} + \frac{2c^2}{d^2}\right) + 2\frac{ac}{bd}\sqrt{2}$, but since a, c are assumed not to be zero, it would follow that $\sqrt{2}$ is rational, giving a contradiction. Thus $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.

For the degree of the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$, we then conclude (Theorem 31.4) that

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

For a basis, we can use the elements $1 \cdot 1$, $1 \cdot \sqrt{3}$, $\sqrt{2} \cdot 1$, $\sqrt{2}\sqrt{3}$ (see the proof of Theorem 31.4; we are taking the product of each element of the basis for $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ with each element of the basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})$). In other words, a basis for the field extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$ is $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$.

□

5
20 points