In-Class Final

Abstract Algebra 1

MATH 3140

Fall 2021

Sunday December 12, 2021

NAME: ______________________________

PRACTICE EXAM

SOLUTIONS

Question:	**1**	**2**	**3**	**4**	Total
Points:	25	25	25	25	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 to **Canvas** as a **single .pdf** file with the questions in the correct order.
- You have 60 minutes to complete the exam.

1. (25 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 $a \in \mathbb{Z}_p$. □

1
25 points

2. (25 points) • Let R be a commutative ring and let I be an ideal of R. The *radical of* I is the set

$$\sqrt{I} := \{a \in R : a^n \in I \text{ for some } n \in \mathbb{Z}^+\}.$$

Show that $\sqrt{I}$ *is an ideal of* R.

SOLUTION

Solution. First we will show that $\sqrt{I}$ a subgroup of R. The first observation is that $0 \in I \subseteq \sqrt{I}$, so that $\sqrt{I}$ is nonempty. Now, let $a, b \in \sqrt{I}$, we will show that $(a - b) \in \sqrt{I}$. To do this, suppose that $a, b \in \sqrt{I}$, so that there are $\alpha, \beta \in \mathbb{Z}^+$ such that $a^\alpha, b^\beta \in I$. Let n be an integer such that $n \geq \alpha + \beta$. Then

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

since either $k \geq \alpha$ or $n - k \geq \beta$ (otherwise $n = k + (n - k) < \alpha + \beta$). In other words, each term in the sum is in I since $a^k \in I$ or $b^{n-k} \in I$ (use the definition of an ideal), and since I is a subgroup, the sum of elements of I is in I. Thus $\sqrt{I}$ is a subgroup.

To show that it is an ideal, let $r \in R$ and $a \in \sqrt{I}$. Suppose that $a^n \in I$. Then $(ra)^n = r^n a^n \in I$, so that $ra \in \sqrt{I}$. □

2
25 points

3. (25 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 $\sqrt[n]{2} \in \overline{\mathbb{Q}}$, since $\sqrt[n]{2}$ 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 positive integer n (Fraleigh Theorem 31.4). Using Eisenstein's Criterion (Fraleigh Theorem 23.15) applied to the prime $p = 2$, one has that $x^n - 2$ is irreducible in $\mathbb{Q}[x]$, 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 $\mathbb{Q}$. □

3
25 points

4. (25 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 $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$.

We start with the extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. 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 $a \neq 0$, 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 (solve for $\sqrt{2}$), giving a contradiction. Thus $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, completing the proof of the claim that the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}(\sqrt{2})$ has degree 2, with basis given by $1, \sqrt{3}$.

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

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

as claimed.

For a basis of $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$, we can use the elements $1 \cdot 1$, $1 \cdot \sqrt{3}$, $\sqrt{2} \cdot 1$, $\sqrt{2} \cdot \sqrt{3}$ (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 $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$, as claimed. □

4
25 points