Solutions for the Midterm Exam for Math 404A–Spring, 2018

QUESTION 1. In each part of this question, you should find a polynomial $f(x)$ with certain properties. The polynomial $f(x)$ should be in $\mathbf{Q}[x]$ and have degree 4. The polynomial $f(x)$ should be monic and irreducible over $\mathbf{Q}$. Please note that your answer in each part should be an example of a polynomial $f(x)$ having the above properties as well as one additional property. We repeat that we want $deg\big(f(x)\big) = 4$ and we want $f(x)$ to be irreducible over $\mathbf{Q}$. Your answers should be justified.

We will let K denote the field $\mathbf{Q}(\theta)$ where θ is one of the roots of $f(x)$ in $\mathbf{C}$.

(a) The field K is the splitting field over $\mathbf{Q}$ for the polynomial $f(x)$.

SOLUTION: We will let $f(x) = x^4 + x^3 + x^2 + x + 1$. The roots of this polynomial are $\{\omega^i \bigm| 1 \leq i \leq 4\}$ where $\omega = cos(\frac{2\pi}{5}) + sin(\frac{2\pi}{5})i$. We proved in class that $f(x)$ is irreducible over $\mathbf{Q}$. It obviously is monic and has degree 4. The splitting field for $f(x)$ over $\mathbf{Q}$ is

$$\mathbf{Q}(\omega, \omega^2, \omega^3, \omega^4) \ = \ \mathbf{Q}(\omega) = \ K$$

if we take $\theta = \omega$. It actually doesn't matter which root θ of $f(X)$ we choose. The reason is that if θ' is any one of the other roots of $f(x)$ in $\mathbf{C}$, then $\theta' \in K$ and hence $\mathbf{Q}(\theta') \subseteq K$. Thus, $\mathbf{Q}(\theta') \subseteq \mathbf{Q}(\theta)$. But both θ and θ' have the same minimal polynomial over $\mathbf{Q}$, namely $f(x)$. Hence both of the fields $\mathbf{Q}(\theta')$ and $\mathbf{Q}(\theta)$ are extensions of $\mathbf{Q}$ of degree 4. Therefore, the inclusion must be an equality. That is, $\mathbf{Q}(\theta') = \mathbf{Q}(\theta)$.

(b) The field K is not the splitting field over $\mathbf{Q}$ for the polynomial $f(x)$.

SOLUTION:. For this part, let $f(x) = x^4 - 2$. Then $f(x)$ is monic and has degree 4 and is also irreducible over $\mathbf{Q}$. The irreducibility over $\mathbf{Q}$ follows immediately from the Eisenstein Criterion for $p = 2$. One root is $\theta = \sqrt[4]{2}$ which is a real number. But $K = \mathbf{Q}(\theta)$ is a subfield of $\mathbf{R}$ and therefore cannot contain all the roots of $f(x)$ in $\mathbf{C}$. The reason is that $\sqrt[4]{2}i$ is another root of $f(x)$ in $\mathbf{C}$ and is obviously not in $\mathbf{R}$. Therefore, that root of $f(x)$ cannot be in K. Therefore, K is not the splitting field for $f(x)$ over $\mathbf{Q}$.

QUESTION 2. This question concerns the following polynomial:

$$g(x) \ = \ x^{35} - 12x^{26} - 9x^{24} + 39x^{16} + 21x^{11} - 27x^4 + 3x + 6 \quad .$$

Let θ denote one of the roots of $g(x)$ in $\mathbf{C}$. Let $K = \mathbf{Q}(\theta)$.

(a) Consider K as a vector space over $\mathbf{Q}$. Give a basis for this vector space. Justify your answer.

SOLUTION: Note that the polynomial $g(x)$ is monic and irreducible over $\mathbf{Q}$. This follows immediately from the Eisenstein criterion for $p = 3$. Therefore, $g(x)$ must be the minimal polynomial for θ over $\mathbf{Q}$. Hence

$$[K : \mathbf{Q}] \;=\; deg\big(g(x)\big) \;=\; 35 \;\;.$$

Thus, K is a vector space over $\mathbf{Q}$ of dimension 35. As discussed in class, the following set is a basis for K as a vector space over $\mathbf{Q}$:

$$\{1,\; \theta,\; .\,.\,.,\theta^{34}\} \;=\; \{\theta^i \;\big|\; 0 \le i \le 34\;\} \;\;.$$

(b) Suppose that $\beta \in K$. Let $h(x)$ be the minimal polynomial for β over $\mathbf{Q}$. Without knowing anything else about β, what can you say (if anything) about the degree of the polynomial $h(x)$? Justify your answer.

SOLUTION:. Let $F = \mathbf{Q}(\beta)$. Since $\beta \in K$, we have $\mathbf{Q} \subseteq F \subseteq K$. Consequently,

$$35 \;=\; [K : \mathbf{Q}] \;=\; [K : F][F : \mathbf{Q}]$$

and therefore $[F : \mathbf{Q}]$ must divide 35. We know that $[F : \mathbf{Q}] = deg\big(h(x)\big)$. Therefore, $deg\big(h(x)\big)$ must divide 35. The possible values of $deg\big(h(x)\big)$ are $1,\ 5,\ 7$, or 35.

(c) Carefully prove that there exists a polynomial $f(x) \in \mathbf{Q}[x]$ such that $f(\theta^3) = \theta$.

SOLUTION:. Let $\beta = \theta^3$. Then $\beta \in K$. As in part (b), let $F = \mathbf{Q}(\beta)$. The argument in part (b) makes it clear that $[K : F]$ must divide 35. Thus, $[K : F] = 1,\ 5,\ 7$, or 35. Now notice that

$$K \;=\; \mathbf{Q}(\theta) \;\subseteq\; F(\theta) \;\subseteq\; K$$

It follows that $K = F(\theta)$. Let $m(x)$ be the minimal polynomial for θ over F. Hence $[K : F] = deg\big(m(x)\big)$. We make the following observation. Since $\beta = \theta^3$, it follows that θ is a root of $x^3 - \beta$. Since $\beta \in F$, the polynomial $x^3 - \beta$ is in $F[x]$. Since θ is a root of $x^3 - \beta$, it therefore follows that $m(x)$ divides $x^3 - \beta$ in $F[x]$. Therefore, it is clear that

$$deg\big(m(x)\big) \;\le\; deg\big(x^3 - \beta\big) \;=\; 3 \;\;.$$

Therefore, $[K : F] \leq 3$. Combining that with the fact that $[K : F] = 1,\ 5,\ 7$, or 35, it follows that $[K : F] = 1$. Therefore, we must have $F = K$.

We have proved that $K = \mathbf{Q}(\beta)$. Since K is a finite extension of $\mathbf{Q}$, we know that β is algebraic over $\mathbf{Q}$ and therefore that $K = \mathbf{Q}(\beta) = \mathbf{Q}[\beta]$. Since $\theta \in K$, there must exist a polynomial $f(x) \in \mathbf{Q}[x]$ such that $f(\beta) = \theta$. Therefore, $f(\theta^3) = \theta$.

QUESTION 3. (35 points) Consider the polynomial $g(x) = x^5 - 2$. We know that $g(x)$ is irreducible over $\mathbf{Q}$ by the Eisenstein criterion for $p = 2$. Thus, $g(x)$ has five distinct roots in $\mathbf{C}$. We can write

$$g(x) \ = \ (x - \theta_1)(x - \theta_2)(x - \theta_3)(x - \theta_4)(x - \theta_5)$$

where $\theta_i \in \mathbf{C}$ for $1 \leq i \leq 5$. For each such i, let $F_i = \mathbf{Q}(\theta_i)$. Let $K = \mathbf{Q}(\theta_1, \theta_2, \theta_3, \theta_4, \theta_5)$.

(a) Prove that the five fields $F_1,\ \ldots, F_5$ are all distinct.

SOLUTION:. Suppose that we take $\theta_1 = \sqrt[5]{2}$. Then $F_1 = \mathbf{Q}(\theta_1)$ is a subfield of $\mathbf{R}$. The other four roots of $g(x)$ in $\mathbf{C}$ are obviously not in $\mathbf{R}$. Hence the fields $F_2,\ F_3,\ F_4,\ F_5$ are not subfields of $\mathbf{R}$. Hence those four fields are not equal to F_1. It will be useful to remark that F_1 contains only one root of the polynomial $g(x)$, namely the root θ_1.

We now show that those four fields are distinct from each other. To show this, assume that $F_i = F_j$ where $2 \leq i,\ j \leq 4$. We will show that $i = j$. As we discussed in class, the five fields $F_1, \ldots, F_5$ are all isomorphic to each other over $\mathbf{Q}$. In particular, there is an isomorphism $\sigma : F_i \to F_1$ over $\mathbf{Q}$ with the property that $\sigma(\theta_i) = \theta_1$. Since we are assuming that $F_j = F_i$, it follows that $\theta_j \in F_i$. Since $g(\theta_j) = 0$ and $g(x) \in \mathbf{Q}[x]$, it follows that

$$g\big(\sigma(\theta_j)\big) \ = \ \sigma\big(g(\theta_j)\big) \ = \ \sigma(0) \ = \ 0 \ \ .$$

Of course, this is a familiar observation that we discussed in class. Now $\sigma(\theta_j) \in F_1$ and so $\sigma(\theta_j)$ is a root of $g(x)$ in F_1. As remarked above, it follows that $\sigma(\theta_j) = \theta_1$. But $\sigma(\theta_i) = \theta_1$ too. Since σ is an isomorphism, it is an injective map, and hence we must have $\theta_i = \theta_j$. This implies that $i = j$.

(b) Prove that $[K : \mathbf{Q}] = 20$.

SOLUTION: Let $\zeta_5 = e^{\frac{2\pi i}{5}}$. We know that $L = \mathbf{Q}(\zeta_5)$ is a subfield of K since both $\theta_1 = \sqrt[5]{2}$ and $\zeta_5\theta_1 = \zeta_5\sqrt[5]{2}$ are roots of $g(x)$. Their ratio ζ_5 must be in K. Since K contains L and

K contains θ_1, it is clear that K contains $\mathbf{Q}(\zeta_5, \theta_1)$. However, the five roots of $x^5 - 2$ are $\{\zeta_5^i \theta_1 \bigm| 0 \le i \le 4\}$, all of which are in $\mathbf{Q}(\zeta_5, \theta_1)$. It follows that K is contained in $\mathbf{Q}(\zeta_5, \theta_1)$. These remarks show that $K = \mathbf{Q}(\zeta_5, \theta_1)$.

Since $x^5 - 2$ is irreducible over $\mathbf{Q}$ by the Eisenstein criterion for $p = 2$, it is clear that $x^5 - 2$ is the minimal polynomial for θ_1 over $\mathbf{Q}$. Let $F_1 = \mathbf{Q}(\theta_1)$ as above. It follows that $[F_1 : \mathbf{Q}] = 5$. Also, we proved in class that $[L : \mathbf{Q}] = 4$. Since $\mathbf{Q} \subseteq L \subseteq K$ and $\mathbf{Q} \subseteq F_1 \subseteq K$, it therefore follows that

$$[K : \mathbf{Q}] \;=\; [K : L][L : \mathbf{Q}] \;=\; 4[K : L] \qquad \textit{and} \qquad [K : \mathbf{Q}] \;=\; [K : F_1][F_1 : \mathbf{Q}] \;=\; 5[K : F_1] \;\; .$$

Thus, $[K : \mathbf{Q}]$ must be divisible by both 4 and 5, and hence divisible by 20.

On the other hand $K = \mathbf{Q}(\zeta_5, \theta_1) = L(\theta_1)$. Since θ_1 is a root of $x^5 - 2 \in L[x]$, it follows that the minimal polynomial for θ_1 over L has degree at most 5. Hence $[K : L] \le 5$. Therefore,

$$[K : \mathbf{Q}] \;=\; [K : L][L : \mathbf{Q}] \;=\; 4[K : L] \;\le\; 4 \cdot 5 \;=\; 20 \;\; .$$

Thus, we have shown that $[K : \mathbf{Q}] = 20q$ for some positive integer q and that $[K : \mathbf{Q}] \le 20$. Combining these observations, we see that $[K : \mathbf{Q}] = 20$

(c) What can you say (if anything) about the order of the group $Aut(K/\mathbf{Q})$

SOLUTION:. By definition, K is the splitting field over $\mathbf{Q}$ for the polynomial $x^5 - 2$. It follows that K is a finite Galois extension of $\mathbf{Q}$. Therefore,

$$\bigl|Aut(K/\mathbf{Q})\bigr| \;=\; \bigl|Gal(K/\mathbf{Q})\bigr| \;=\; [K : \mathbf{Q}] \;=\; 20 \;\; .$$