MATH 210B

Name: Quin Darcy **Due Date:** 3/11/20
Instructor: Dr. Shannon **Assignment:** Homework 6

4. Let ζ be a primitive 6^{th} root of unity. Find (with explanation) all 1-1 homomorphisms of $\mathbb{Q}(\sqrt[3]{5}, \zeta)$ to $\mathbb{C}$, and all 1-1 homomorphisms from $\mathbb{Q}(\sqrt{2}, i)$ to $\mathbb{C}$.

Solution. *Let $\zeta = \frac{1}{2} + i\frac{\sqrt{3}}{2}$. Then ζ is equal to one of the 2 primitive 6^{th} roots of unity. The minimal polynomial of $\sqrt[3]{5}$ over $\mathbb{Q}$ is $x^3 - 5$. The minimal polynomial of ζ over $\mathbb{Q}$ is $x^2 - x + 1$. Since $\sqrt[3]{5} \notin \mathbb{Q}(\zeta)$ and $\zeta \notin \mathbb{Q}(\sqrt[3]{5})$, then $[\mathbb{Q}(\sqrt[3]{5}, \zeta) \colon \mathbb{Q}] = 6$. Note that $x^3 - 5$ splits over $\mathbb{Q}(\sqrt[3]{5}, \zeta)$ as*

$$(x - \sqrt[3]{5})(x - \zeta^2\sqrt[3]{5})(x - \zeta^4\sqrt[3]{5}).$$

Similarly, $x^2 - x + 1$ splits over $\mathbb{Q}(\sqrt[3]{5}, \zeta)$ as

$$(x - \zeta)(x - \zeta^5).$$

Since $\mathbb{Q}(\sqrt[3]{5}, \zeta) \subseteq \mathbb{C}$, then both polynomials split over $\mathbb{C}$. Thus, if $\psi \colon \mathbb{Q}(\sqrt[3]{5}, \zeta) \to \mathbb{C}$ is a 1-1 homomorphism, then by Exam 1 and HW5 we have 6 possibilities

$$\psi_1 := \begin{cases} \sqrt[3]{5} \mapsto \sqrt[3]{5} \\ \zeta \mapsto \zeta \end{cases} \qquad \psi_2 := \begin{cases} \sqrt[3]{5} \mapsto \zeta^2\sqrt[3]{5} \\ \zeta \mapsto \zeta \end{cases} \qquad \psi_3 := \begin{cases} \sqrt[3]{5} \mapsto \zeta^4\sqrt[3]{5} \\ \zeta \mapsto \zeta \end{cases}$$

$$\psi_4 := \begin{cases} \sqrt[3]{5} \mapsto \sqrt[3]{5} \\ \zeta \mapsto \zeta^5 \end{cases} \qquad \psi_5 := \begin{cases} \sqrt[3]{5} \mapsto \zeta^2\sqrt[3]{5} \\ \zeta \mapsto \zeta^5 \end{cases} \qquad \psi_6 := \begin{cases} \sqrt[3]{5} \mapsto \zeta^4\sqrt[3]{2} \\ \zeta \mapsto \zeta^5. \end{cases}$$

As above, we see that the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$ which factors as $(x - \sqrt{2})(x + \sqrt{2})$ over $\mathbb{Q}(\sqrt{2})$. The minimal polynomial of i over $\mathbb{Q}$ is $x^2 + 1$, which factors as $(x - i)(x + i)$ over $\mathbb{Q}(i)$. Thus, there are 4 possible 1-1 homomorphisms from $\mathbb{Q}(\sqrt{2}, i)$ to $\mathbb{C}$. We have:

$$\psi_1 := \begin{cases} \sqrt{2} \to \sqrt{2} \\ i \to i \end{cases} \qquad \psi_2 := \begin{cases} \sqrt{2} \to -\sqrt{2} \\ i \to i \end{cases}$$

$$\psi_3 := \begin{cases} \sqrt{2} \to \sqrt{2} \\ i \to -i \end{cases} \qquad \psi_4 := \begin{cases} \sqrt{2} \to -\sqrt{2} \\ i \to -i. \end{cases}$$

5. For each of the following fields, and mappings, φ, determine if φ is an automorphism of the field, and if so, then find F_φ, and find $[E \colon F_\varphi]$.

   (a) $\mathbb{Q}(i)$, $\varphi(i) = -i$.

Solution. This is an automorphism. Since $\mathbb{Q}(i)$ is the splitting field for $x^2+1=(x-i)(x+i)$, then all we need is that i be mapped to itself or $-i$. We also know that φ is the identity over $\mathbb{Q}$ and thus for any $a+bi\in\mathbb{Q}(i)$, we have $\varphi(a+bi)=a-bi$ and so $\mathbb{Q}\subseteq F_\varphi$. Moreover, since i is the only element which does not map to itself, then $F_\varphi=\mathbb{Q}$ and so $[\mathbb{Q}(i)\colon\mathbb{Q}]=2$.

(b) $\mathbb{Q}(\omega)$, $\varphi(\omega)=\omega^2$.

Solution. This is an automorphism. Since $x^2+x+1=(x-\omega)(x-\omega^2)$ is the minimal polynomial associated with ω, then all we need is that $\varphi(\omega)\in\{\omega,\omega^2\}$, which it is. From the definition, it follows that $\varphi(\omega^2)=\omega$. Thus, the only fixed elements of this automorphism are those in $\mathbb{Q}$ and so $F_\varphi=\mathbb{Q}$ and $[\mathbb{Q}(\omega)\colon\mathbb{Q}]=2$.

(c) $\mathbb{Q}(\omega)$, $\varphi(\omega)=-\omega$.

Solution. This is not an automorphism, since $-\omega$ is not a root of x^2+x+1.

(d) $\mathbb{Q}(x)$, $\varphi(x)=1/x$.

Solution. φ is an automorphism and so $\varphi(x+\frac{1}{x})=\varphi(x)+\varphi(\frac{1}{x})=\frac{1}{x}+x$. Thus, $\mathbb{Q}(x+\frac{1}{x})\subseteq F_\varphi$. Note that x is a root of $z^{-}(x+\frac{1}{x})z+1$. And so the minimal polynomial for x has degree ≤ 2. However, if it had degree 1, then $[\mathbb{Q}(x)\colon\mathbb{Q}(x+\frac{1}{x})]=1$ which would imply that $\mathbb{Q}(x)=\mathbb{Q}(x+\frac{1}{x})$. This is not true since not every element of $\mathbb{Q}(x)$ is fixed. Thus, $[\mathbb{Q}(x)\colon\mathbb{Q}(x+\frac{1}{x})]=2$. Since for any $f(x)\in F_\varphi$ such that $f(x)\notin\mathbb{Q}(x+\frac{1}{x})$ we would have $[\mathbb{Q}(x+\frac{1}{x})\colon\mathbb{Q}(x+\frac{1}{x})]>1$ and so $[\mathbb{Q}(x)\colon\mathbb{Q}(x+\frac{1}{x},f(x))]=1$, but this is not possible. Therefore, $F_\varphi=\mathbb{Q}(x+\frac{1}{x})$ and $[\mathbb{Q}(x)\colon F_\varphi]=2$.

(e) $GF(2^n)$, $\varphi(a)=a^2$.

Solution. φ is an automorphism. Since it is 1-1, then for any $a\in GL(2^n)$ such that $\varphi(a)=a^2=a$, it follows that $a=1$ or $a=0$. However, $a\neq 1$ since if $1\in GF(2^n)$, then $\varphi(1+1)=1+1=2$, but we know $\varphi(2)=4$. Thus, $F_\varphi=\{0\}$ and $[GL(2^n)\colon F_\varphi]=2^n$.

6. For each of the fields, and subsets, S, of the automorphism group of the field, find F_S, and find $[E\colon F_S]$. For (b)-(e), the φ's are defined in the solution to HW5.

(a) $\mathbb{Q}(i)$, $S=\{\text{identity},\varphi(i)=i\}$.

Solution. Clearly, with the identity automorphism we have that all of $\mathbb{Q}(i)$ is fixed, however, with $\varphi(i)=-i$, only $\mathbb{Q}$ is fixed. Thus, $F_S=\mathbb{Q}(i)\cap\mathbb{Q}=\mathbb{Q}$ and so $[\mathbb{Q}(i)\colon\mathbb{Q}]=2$.

(b) $\mathbb{Q}(\sqrt[3]{2},\omega)$, $S=\{\varphi_1,\varphi_2\}$.

Solution. Here we have that the fixed field of φ_1 is $\mathbb{Q}(\sqrt[3]{2},\omega)$ and for φ_2 it is just $\mathbb{Q}(\omega\sqrt[3]{2}$. Thus, $F_S=\mathbb{Q}(\sqrt[3]{2})$ and, by HW5, $[\mathbb{Q}(\sqrt[3]{2},\omega)\colon\mathbb{Q}]=2$.

(c) $\mathbb{Q}(\sqrt[3]{2},\omega)$, $S=\{\varphi_1,\varphi_3\}$.

Solution. With φ_1, the fixed field is all of $\mathbb{Q}(\sqrt[3]{2},\omega)$ and since with φ_3, we have that $\varphi(\sqrt[3]{2})=\sqrt[3]{2}$, then only ω has changed. Thus, $F_S=\mathbb{Q}(\sqrt[3]{2})$. Additionally, since $\omega\notin\mathbb{Q}(\sqrt[3]{2})$, then the minimal polynomial of ω over $\mathbb{Q}(\sqrt[3]{2})$ is x^2+x+1 and thus $[\mathbb{Q}(\sqrt[3]{2},\omega)\colon\mathbb{Q}(\sqrt[3]{2})]=2$.

(d) $\mathbb{Q}(\sqrt[3]{2}, \omega)$, $S = \{\varphi_1, \varphi_4, \varphi_5\}$.

Solution. The fixed field for the identity map is all of $\mathbb{Q}(\sqrt[3]{2}, \omega)$. The fixed field for φ_4 is $\mathbb{Q}(\omega)$ since $\varphi(\sqrt[3]{2}) = \omega\sqrt[3]{2}$ and $\varphi_4(\omega) = \omega$. Similarly, φ_5 leaves ω unchanged while $\varphi_5(\sqrt[3]{2}) = \omega^2\sqrt[3]{2}$ and so the fixed field for φ_5 is $\mathbb{Q}(\omega)$. Thus, $F_S = \mathbb{Q}(\omega)$ and $[\mathbb{Q}(\sqrt[3]{2}, \omega) \colon \mathbb{Q}(\omega)] = 3$ since $x^3 - 2$ is the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}(\omega)$.

(e) $\mathbb{Q}(\sqrt[3]{2}, \omega)$, $S = \{\varphi_1, \varphi_2, \varphi_6\}$.

Solution. In this case both φ_2 and φ_6 map $\sqrt[3]{2}$ and ω to elements different from themselves. However, $\varphi_6(\omega^2\sqrt[3]{4})$. And so $F_S = \mathbb{Q}(\omega^2\sqrt[3]{4})$ and $[\mathbb{Q}(\sqrt[3]{2}, \omega) \colon \mathbb{Q}(\omega^2\sqrt[3]{4})] = 3$.

7. Prove that $f(x)$ has a multiple root in its splitting field iff f and f' have a common factor of degree ≥ 1.

Proof. Let E denote the splitting field of $f(x)$ and assume $\alpha \in E$ is a root of multiplicity $k > 1$. Then by definition, $(x - \alpha)^k \mid f(x)$ and so we may write

$$f(x) = (x - \alpha)^k \sum_{i=0}^{m} a_i x^i.$$

Taking the derivative of both sides we get

$$\begin{aligned}
\big(f(x)\big)' &= \left((x - \alpha)^k \sum_{i=0}^{m} a_i x^i\right)' \\
&= k(x - \alpha)^{k-1} \sum_{i=0}^{m} a_i x^i + (x - \alpha)^k \sum_{i=1}^{m} i a_i x^{i-1} \\
&= (x - \alpha)^{k-1} \left(k \sum_{i=0}^{m} a_i x^i + (x - \alpha) \sum_{i=1} i a_i x^{i-1}\right).
\end{aligned}$$

Thus, $(x - \alpha)^{k-1} \mid f'(x)$ and $(x - \alpha)^{k-1} \mid f(x)$. Since $k > 1$, then $k - 1 \geq 1$. Hence, $f(x)$ and $f'(x)$ have a common factor of degree ≥ 1. Now to argue the contrapositive, assume that $f(x)$ does not have a multiple root in its splitting field. Then letting α be a root of $f(x)$, we can write $f(x) = (x - \alpha)g(x)$, where $(x - \alpha) \nmid g(x)$. From here we see that the derivative of f is $f'(x) = g(x) + (x - \alpha)g'(x)$. Thus, $(x - \alpha) \nmid f'(x)$ and since α was any root of $f(x)$, then it follows that $f(x)$ and $f'(x)$ do not share any common factors. $\square$

8.

(a) Assume that $\mathrm{char}(F) = 0$, $f(x) \in F[x]$, and $f(x)$ is irreducible over F. Prove that f cannot have any roots of multiplicity greater than 1.

Proof. Assume for contradiction that $f(x)$ has a root of multiplicity greater than 1. Then by 7., $f(x)$ and $f'(x)$ have a common factor. Thus, if a is the root of multiplicity, then the minimal polynomial of a over F is $f(x)$ since $f(x)$ is irreducible (assuming it is monic). However, since a is also a root of $f'(x)$, then it must be the case that $f(x) \mid f'(x)$. This is a contradiction as $\deg(f'(x)) < \deg(f(x))$. $\square$

(b) Assume that $\text{char}(F) = p$, $f(x) \in F[x]$, $f(x)$ is irreducible over F. Prove that if f has a multiple root then there exists $g(x) \in F[x]$ such that $f(x) = g(x^p)$.

Proof. Assume that f has a multiple root. Then by 7., f and f' share a common factor. Since f is irreducible, then $\gcd(f, f') = f$. This implies that $f'(x) = 0$. Thus, for some $g(x) \in F[x]$, $f(x) = g(x^p)$. In other words, if we let $f(x) = a_0 + a_1 x^p + \cdots a_n x^{np}$, then $f'(x) = pa_1 x^{p-1} + \cdots npa_n x^{np-1}$ and since $\text{char}(F) = p$, then every term in $f'(x)$ vanishes. $\square$

9.

(a) Prove that if p is prime, $p \nmid n$, then $x^n - 1$ has n distinct roots over $\mathbb{Z}_p$.

Proof. Let $f(x) = x^n - 1$, then $f'(x) = nx^{n-1}$. Since $p \nmid n$, then $f'(1) \neq 0$. Seeing that the only root of $f'(x)$ is 0 and $f(0) \neq 0$, then it follows that $f(x)$ and $f'(x)$ share no common roots and thus no common factors. Thus, $f(x)$ has no roots of multiplicity. Thus, $x^n - 1$ has n distinct roots over $\mathbb{Z}_p$. $\square$

(c) Assume that ζ is a primitive n^{th} root of unity. Determine $[\mathbb{Q}(\zeta) \colon \mathbb{Q}]$.

Solution. By part (b) we know that if $f(x) \mid x^n - 1$ and ζ is a root of $f(x)$ then ζ^p, where p prime and $p \nmid n$, is also a root. Thus, the total number of roots of such an $f(x)$ is given by $\phi(n)$. Thus, the minimal polynomial of ζ has degree $\phi(n)$ and therefore, $[\mathbb{Q}(\zeta) \colon \mathbb{Q}] = \phi(n)$.