MATH 210B

Name: Quin Darcy **Due Date:** 3/4/20
Instructor: Dr. Shannon **Assignment:** Homework 5

4. Assume that in the equation of a line, $y = mx + b$, $m, b \in \mathbb{Q}$, and that in the equation of a circle $(x-h)^2 + (y-k)^2 = r^2$, $h, k, r \in \mathbb{Q}$. Assuming that the line and the circle intersect, explain why the coordinates of the points of intersection are elements of an extension, $\mathbb{Q}(\sqrt{g})$, of $\mathbb{Q}$, where $[\mathbb{Q}(\sqrt{g})\colon \mathbb{Q}] = 2$ or $= 1$.

   Solution. Given that $y = mx + b$, we can substitute this in for the equation of the circle. Obtaining,

$$\begin{aligned}(x-h)^2 + (y-k)^2 - r^2 &= \left[x^2 - 2hx + h^2\right] + \left[y^2 - 2ky + k^2\right] - r^2 \\ &= \left[x^2 - 2hx + h^2\right] + \left[(mx+b)^2 - 2k(mx+b) + k^2\right] - r^2 \\ &= (1+m^2)x^2 + (2mb - 2mk - 2h)x + (h^2 - 2bk + k^2 - r^2) \\ &= 0.\end{aligned}$$

   Using the quadratic formula to solve for x we get

$$x = \frac{-(2mb - 2mk - 2h) \pm \sqrt{(2mb - 2mk - 2h)^2 - 4(1+m^2)(h^2 - 2bk + k^2 - r^2)}}{2(1+m^2)}.$$

   Let $g = (2mb - 2mk - 2h)^2 - 4(1+m^2)(h^2 - 2bk + k^2 - r^2)$. Then if $\sqrt{g} \in \mathbb{Q}$, we have that $x \in \mathbb{Q}$ and $[\mathbb{Q}(\sqrt{g})\colon \mathbb{Q}] = 1$. Otherwise, we have that $\sqrt{g} \in \mathbb{Q}(\sqrt{g})$ and since

$$\frac{-(2mb - 2mk - 2h)}{2(1+m^2)} = \frac{-mb + mk + h}{1+m^2} \in \mathbb{Q}$$

   and $2(1+m^2) \in \mathbb{Q}$, then both of these rational numbers are elements of $\mathbb{Q}(\sqrt{g})$. Hence, $x \in \mathbb{Q}(\sqrt{g})$. Moreover, if $\sqrt{g} \notin \mathbb{Q}$, then $[\mathbb{Q}(\sqrt{g})\colon \mathbb{Q}] = 2$ since $\{1, \sqrt{g}\}$ is a basis for $\mathbb{Q}(\sqrt{g})$ over $\mathbb{Q}$. By the same argument we can show that $y \in \mathbb{Q}(\sqrt{g})$. Therefore, the coordinates of the two intersection points of the line with the circle are elements of $\mathbb{Q}(\sqrt{g})$.

5. Recall that an automorphism of F is an isomorphism of F onto F. Find all the automorphisms of $\mathbb{Q}(\sqrt[3]{2}, \omega)$.

Solution. We have that $\sqrt[3]{2}$ is algebraic over $\mathbb{Q}$ since it is a root of $x^3 - 2$. Thus, $\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}[x]/(x^3-2)_i$. Now note that a basis for $\mathbb{Q}[x]/(x^3-2)_i$ is $\{(x^3-2)_i+1, (x^3-2)_i + x, (x^3-2)_i + x^2\}$. It follows from this that $[\mathbb{Q}(\sqrt[3]{2})\colon \mathbb{Q}] = 3$. Additionally, a basis for this extension is $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$. Similarly, ω is algebraic over $\mathbb{Q}$ since it is a root of x^2+x+1 and by the same reasoning as above, it follows that $[\mathbb{Q}(\omega)\colon \mathbb{Q}] = 2$ and a basis for this extension is $\{1, \omega\}$. Thus, $[\mathbb{Q}(\sqrt[3]{2}, \omega)\colon \mathbb{Q}] = 6$ and a basis for this extension is $\{1, \sqrt[3]{2}, \sqrt[3]{4}, \omega, \omega\sqrt[3]{2}, \omega\sqrt[3]{4}\}$. Now consider some $\alpha \in \mathbb{Q}(\sqrt[3]{2}, \omega)$. Given our basis, it can be expressed as

$$\alpha = a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\omega + e\omega\sqrt[3]{2} + f\omega\sqrt[3]{4},$$

for $a, b, c, d, e, f \in \mathbb{Q}$. Now let $\sigma\colon \mathbb{Q}(\sqrt[3]{2}, \omega) \to \mathbb{Q}(\sqrt[3]{2}, \omega)$ be an automorphism. Since $\mathbb{Q}$ is a subfield of $\mathbb{Q}(\sqrt[3]{2}, \omega)$ and σ is an automorphism, then it follows that $\mathbb{Q} \cong \sigma(\mathbb{Q})$. However, by HW1, σ can only be the identity map on $\mathbb{Q}$. In other words, $\sigma(q) = q$ for all $q \in \mathbb{Q}$. From this it follows that

$$\begin{aligned}\sigma(\alpha) &= \sigma(a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\omega + e\omega\sqrt[3]{2} + f\omega\sqrt[3]{4}) \\ &= a + b\sigma(\sqrt[3]{2}) + c\sigma(\sqrt[3]{4}) + d\sigma(\omega) + e\sigma(\omega\sqrt[3]{2}) + f\sigma(\omega\sqrt[2]{4}).\end{aligned}$$

Thus, any such automorphism is uniquely determined by where it sends the basis elements. Now if we consider the polynomial $x^3 - 2 = (x - \sqrt[3]{2})(x - \omega\sqrt[3]{2})(x - \omega^2\sqrt[3]{2})$, and let $\theta\colon \mathbb{Q}(\sqrt[3]{2}, \omega)[x] \to \mathbb{Q}(\sqrt[3]{2}, \omega)[x]$ be the isomorphism given on Exam 1, then given any root, call it α, of $x^3 - 2$ must give that $\sigma(\alpha)$ is a root of $\theta(x^3 - 2)$. Similarly, each root, α, of $x^2 + x + 1 = (x - \omega)(x - \omega^2)$ must correspond to a root $\sigma(\alpha)$ of the same polynomial. With these restrictions, we can conclude that there are 6 possible automorphisms:

$$\sigma_1 := \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \omega \mapsto \omega \end{cases} \qquad \sigma_2 := \begin{cases} \sqrt[3]{2} \mapsto \omega\sqrt[3]{2} \\ \omega \mapsto \omega \end{cases} \qquad \sigma_3 := \begin{cases} \sqrt[3]{2} \mapsto \omega^2\sqrt[3]{2} \\ \omega \mapsto \omega \end{cases}$$

$$\sigma_4 := \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \omega \mapsto \omega^2 \end{cases} \qquad \sigma_5 := \begin{cases} \sqrt[3]{2} \mapsto \omega\sqrt[3]{2} \\ \omega \mapsto \omega^2 \end{cases} \qquad \sigma_6 := \begin{cases} \sqrt[3]{2} \mapsto \omega^2\sqrt[3]{2} \\ \omega \mapsto \omega^2. \end{cases}$$

6. Find (with proof) γ such that $\mathbb{Q}(\gamma) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$.

Proof. Consider $\mathbb{Q}(\sqrt{2}\sqrt[3]{5})$. Since $\sqrt{2}, \sqrt[3]{5} \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$ and this set is closed under multiplication, then $\sqrt{2}\sqrt[3]{5} \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$. Thus, $\mathbb{Q}(\sqrt{2}\sqrt[3]{5}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$. Next, we note that $(\sqrt{2}\sqrt[3]{5})^3 = 10\sqrt{2}$ and so $\sqrt{2} \in \mathbb{Q}(\sqrt{2}\sqrt[3]{5})$. Similarly, $(\sqrt{2}\sqrt[3]{5})^4 = 20\sqrt[3]{5}$ and so $\sqrt[3]{5} \in \mathbb{Q}(\sqrt{2}\sqrt[3]{5})$. Thus, $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$. Therefore, $\mathbb{Q}(\sqrt{2}\sqrt[3]{5}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$. $\square$

7. Assume that K/F, K/E, K/F'. Assume that F'/F is algebraic and E/F. Let E' be the smallest subfield of K which contains E and F'. Prove that E'/E is algebraic.

   Proof. Let $M = \cup\{E(a_1, \dots, a_n) \colon a_i \in F', n \in \mathbb{Z}^+\}$. Then since for every $n \in \mathbb{Z}^+$, $E(a_1, \dots, a_n) \subseteq E'$ for $a_i \in F'$. Thus, $M \subseteq E'$. Now let $c, d \in M$. Then for some $i, j \in \mathbb{Z}^+$, $c \in E(a_1, \dots, a_i)$ and $d \in E(b_1, \dots, b_j)$. If c and d are in the same extension, then $c - d$ and cd are in that extension as well. Otherwise, we let $c = t_1a_1 + \cdots + t_ia_i$ and $d = r_1b_1 + \cdots + r_jb_j$, where $t_i, r_i \in E$. Then (assuming $j \geq i$) $c - d = (t_1a_1 - r_1b_1) + \cdots + (t_ia_i - r_ib_i) - \cdots - r_jb_j$. It follows that $c - d \in E(a_1, \dots, a_i, b_1, \dots, b_j)$ and thus $c - d \in M$. Similarly, $cd \in E(a_1b_1, a_1b_2, \dots, a_1b_j, \dots, a_ib_j)$ and so $cd \in M$. Note commutativity of addition and multiplication, multiplicative inverses, and no zero divisors are all inherited from the fields over which M is the union. Thus, M is a field. Finally, since $E \subseteq M$ and $F' \subseteq M$, then $E' \subseteq M$ because E' is the smallest subfield which contains E and F'. Now let $s \in E'$, then for some $k \in \mathbb{Z}^+$, $s \in E(a_1, \dots, a_k)$. Then $(x - s) \in E(a_1, \dots, a_k)[x]$ and thus s is algebraic over E since $E \subseteq E(a_1, \dots, a_k)$. Therefore, E'/E is algebraic. $\square$

8.

   (a) Determine, with explanation, if the following are splitting fields for $x^3 - 2$ over $\mathbb{Q}$:

      (i) $\mathbb{Q}(\sqrt[3]{2}, \omega)$

      Solution. Note that $x^3 - 2 = (x - \sqrt[3]{2})(x - \omega\sqrt[3]{2})(x - \omega^2\sqrt[3]{2})$ and so any splitting field must contain these roots. Clearly, $\sqrt[3]{2}, \omega \in \mathbb{Q}(\sqrt[3]{2}, \omega)$ and so $\omega\sqrt[3]{2}, \omega^2\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2}, \omega)$. Now note that $\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$ is a splitting field for $x^3 - 2$ since its the smallest field containing all the roots. Then $[\mathbb{Q}(\sqrt[3]{2}) \colon \mathbb{Q}] = 3$ since $\sqrt[3]{2}$ is a root of the third degree irreducible polynomial $x^3 - 2$. And $[\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}) \colon \mathbb{Q}(\sqrt[3]{2})] = 2$ since ω is a root of the irreducible polynomial $x^2 + x + 1 \in \mathbb{Q}(\sqrt[3]{2})[x]$. Finally, $[\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}) \colon \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2})] = 1$ since $\omega^2\sqrt[3]{2}$ can be generated from $\sqrt[3]{2}$ and $\omega\sqrt[3]{2}$. Thus, the degree of the splitting field is $[\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}) \colon \mathbb{Q}] = 6$. From problem 5. we saw that $[\mathbb{Q}(\sqrt[3]{2}, \omega) \colon \mathbb{Q}] = 6$ and so $\mathbb{Q}(\sqrt[3]{2}, \omega)$ is a splitting field for $x^3 - 2$ over $\mathbb{Q}$.

      (ii) $\mathbb{Q}(\omega\sqrt[3]{2}, \omega)$

      Solution. This is a splitting field. Since ω is an element, then ω^{-1} is an element and so $\sqrt[3]{2}$ is therefore an element. Thus, $\mathbb{Q}(\sqrt[3]{2}, \omega) \subseteq \mathbb{Q}(\omega\sqrt[3]{2}, \omega)$. Similarly, $\omega\sqrt[3]{2}, \omega \in \mathbb{Q}(\sqrt[3]{2}, \omega)$ and so $\mathbb{Q}(\omega\sqrt[3]{2}, \omega)$. Therefore, $\mathbb{Q}(\omega\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2}, \omega)$.

      (iii) $\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$.

      Solution. This is a splitting field. As mentioned in part (i), this is, by definition, the smallest field which contains $\mathbb{Q}$ and all the roots of $x^3 - 2$ and is therefore the splitting field of $x^3 - 2$.

(iv) $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$.

Solution. This is a splitting field. Since $i\sqrt{3}$ is an element, then $-1/2 + i\sqrt{3}/2$ is an element. Thus, $\omega \in \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ and since $\sqrt[3]{2}$ is also an element, then $\mathbb{Q}(\sqrt[3]{2}, \omega) \subseteq \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$. Similarly, from ω we can add $1/2$ and multiply by 2 to obtain $i\sqrt{3}$ and thus $i\sqrt{3} \in \mathbb{Q}\sqrt[3]{2}, \omega)$ and since $\sqrt[3]{2}$ is also an element, then $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega)$. Therefore, $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) = \mathbb{Q}(\sqrt[3]{2}, \omega)$.

(b) Find, with explanation, the splitting field of $x^6 + 1$ over $\mathbb{Q}$, and find the degree of the splitting field over $\mathbb{Q}$.

Solution. Consider $x^{12} - 1 = (x^6 + 1)(x^6 - 1)$. This shows that $x^{12} - 1$ contains the roots of $x^6 + 1$. Using De Moivere's Theorem, we can obtain the 12^{th} roots of unity. However, we will first look at the roots of $x^6 - 1$ since these roots are distinct from those in $x^6 + 1$. We have: $1, \frac{1}{2} + i\frac{\sqrt{3}}{2}, \omega, -1, \omega^2$. Thus, the roots of $x^6 + 1$ are $e^{2k\pi/12}$, where k is odd. However, letting $\zeta = \frac{\sqrt{3}}{2} + \frac{i}{2}$, then we observe that ζ generates all 12 roots. Thus, and extension of $\mathbb{Q}$ which contains ζ allows $x^12 - 1$ and thus x^6+1 to split completely. Now note that $x^6+1 = (x^2+1)(x^4-x^2+1)$ and so the minimal polynomial associated with the desired splitting field is of degree 2 or 4. It cannot be degree 2 since $x^2 + 1$ has roots i and $-i$, but $x^6 + 1$ does not split over $\mathbb{Q}(i)$. Thus, $x^4 - x^2 + 1$ is the minimal polynomial. Moreover, since the splitting field must contain ζ and ζ generates all 12 roots, then the splitting field is $\mathbb{Q}(\zeta)$ and $[\mathbb{Q}(\zeta) \colon \mathbb{Q}] = 4$.