

**Math 395**  
**Homework 7**  
**Due: 4/18/2024**

**Name:** Avinash Iyer

**Collaborators:** Antonio Cabello, Timothy Rainone, Nate Hall, Nora Manukyan, Jamie Perez-Schere

### Problem 1

We say a field  $K/F$  is normal if  $K$  is the splitting field of a collection of polynomials. Equivalently, every polynomial in  $F[x]$  that has a root in  $K$  splits into linear factors over  $K$ . Let  $\alpha \in \mathbb{R}$  such that  $\alpha^4 = 5$ . We will show that  $\mathbb{Q}(\alpha + i\alpha)$  is normal over  $\mathbb{Q}(i\alpha^2)$ , but  $\mathbb{Q}(\alpha + i\alpha)$  is not normal over  $\mathbb{Q}$ .

Note that  $(\alpha + i\alpha)^2 = 2i\alpha^2$ . Thus,  $\mathbb{Q}(\alpha + i\alpha) = \text{Spl}_{\mathbb{Q}(i\alpha^2)}(x^2 - 2i\alpha^2)$ , so  $\mathbb{Q}(\alpha + i\alpha)$  is normal over  $\mathbb{Q}(i\alpha^2)$ .

Suppose toward contradiction that  $\mathbb{Q}(\alpha + i\alpha)$  is normal over  $\mathbb{Q}$ . Notice that  $(\alpha + i\alpha)^4 = -20$ , as is  $(\alpha - i\alpha)^4$ . Thus,  $\alpha + i\alpha$  and  $\alpha - i\alpha$  are roots of  $x^4 + 20$ . Since  $\alpha, i, i\alpha \in \mathbb{Q}(\alpha + i\alpha)$ , it is the case that  $\mathbb{Q}(\alpha, i) \subseteq \mathbb{Q}(\alpha + i\alpha)$ . However, we have

$$\begin{aligned} [\mathbb{Q}(\alpha, i) : \mathbb{Q}] &= [\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \\ &= (2)(4) \\ &= 8, \end{aligned}$$

and  $[\mathbb{Q}(\alpha + i\alpha) : \mathbb{Q}] = 4$ , as  $m_{\alpha+i\alpha, \mathbb{Q}}(x) = x^4 + 20$ .  $\perp$

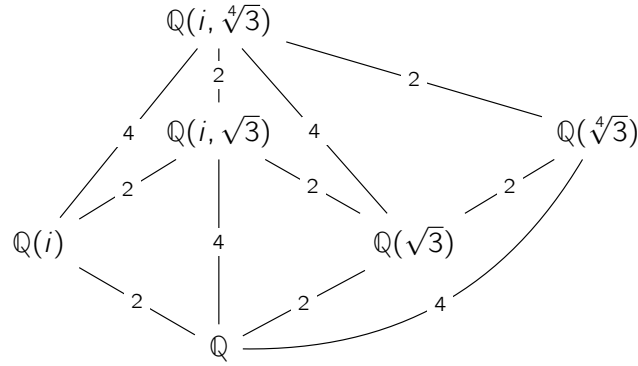
### Problem 2

The roots of  $f(x) = (x^5 - 2)(x^2 - 2)$  are  $\pm\sqrt{2}, \zeta_5^k \sqrt[5]{2}$  for  $k = 0, 1, 2, 3, 4$ . We can see that  $\mathbb{Q}(\zeta_5, \sqrt{2}, \sqrt[5]{2})$  contains the roots of  $(x^5 - 2)(x^2 - 2)$ , so  $\text{Spl}_{\mathbb{Q}}(f(x)) \subseteq \mathbb{Q}(\zeta_5, \sqrt{2}, \sqrt[5]{2})$ . Additionally, we see that  $\sqrt[5]{2} \in \text{Spl}_{\mathbb{Q}}(f(x))$ ,  $\zeta_5 = \frac{\zeta_5 \sqrt[5]{2}}{\sqrt[5]{2}} \in \text{Spl}_{\mathbb{Q}}(f(x))$ , and  $\sqrt{2} \in \text{Spl}_{\mathbb{Q}}(f(x))$ . Thus,  $\mathbb{Q}(\zeta_5, \sqrt[5]{2}, \sqrt{2}) = \text{Spl}_{\mathbb{Q}}(f(x))$ .

For  $x^6 + x^3 + 1$ , we have that  $x^6 + x^3 + 1 = \frac{x^9 - 1}{x^3 - 1}$ . Therefore, the roots of  $x^6 + x^3 + 1$  are  $\zeta_9^d$ , where  $\gcd(d, 9) = 1$  (since  $9 = 3^2$ , every  $n \neq 0, 3, 6$  is a root of  $x^6 + x^3 + 1$ ). Therefore, we can see that  $x^6 + x^3 + 1 = \Phi_9(x)$ , meaning  $\text{Spl}_{\mathbb{Q}}(x^6 + x^3 + 1) = \mathbb{Q}(\zeta_9)$ .

### Problem 6

To find the subfields of  $\mathbb{Q}(i, \sqrt[4]{3})$ , we see that the basis of  $\mathbb{Q}(i, \sqrt[4]{3})$  over  $\mathbb{Q}$  is  $\{1, \sqrt[4]{3}, \sqrt{3}, \sqrt[4]{27}, i, i\sqrt[4]{3}, i\sqrt{3}, i\sqrt[4]{27}\}$ , meaning  $[\mathbb{Q}(i, \sqrt[4]{3}) : \mathbb{Q}] = 8$ . Finding subspaces of  $\mathbb{Q}(i, \sqrt[4]{3})$ , we arrive at the following diagram.



For any subfield  $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}(i, \sqrt[4]{3})$ , it must be the case that  $[F : \mathbb{Q}] = 2^k$  for some  $k = 0, 1, 2, 3$ . Therefore, it must be the case that all subfields are of degree 1, 2, 4, 8.

Suppose there is any subfield  $\mathbb{Q} \subseteq E \subseteq \mathbb{Q}(i)$ . Then, it must be the case that  $[E : \mathbb{Q}] = 1$  or  $[E : \mathbb{Q}] = 2$ , meaning  $E = \mathbb{Q}$  or  $E = \mathbb{Q}(i)$ . The same argument applies for all degree 2 extensions in the above diagram.

## Problem 7

Let  $n = p^k m$  with  $m$  relatively prime to prime  $p$ . We will show that there are  $m$  distinct  $n$ th roots of unity over a field with characteristic  $p$ .

Let  $\zeta_n$  be an  $n$ th root of unity. Then,  $\zeta_n^n - 1 = 0$ , meaning

$$\begin{aligned}\zeta_n^{p^k m} - 1 &= 0 \\ (\zeta_n^m)^{p^k} - 1 &= 0 \\ (\zeta_n^m)^{p^k} - 1^{p^k} &= 0 \\ (\zeta_n^m - 1)^{p^k} &= 0.\end{aligned}$$

Since  $m \neq p^\ell \alpha$ , as  $m$  and  $p$  are relatively prime, it must be the case that, the  $m$  roots of unity are distinct, and each  $n$ th root of unity is an  $m$ th root of unity, meaning there are  $m$  distinct  $n$ th roots of unity.