Homework 9 (Due April 11, 2025)

Jack Hyatt
MATH 547 - Algebraic Structures II - Spring 2025

June 8, 2025

Justify all of your answers completely.

For the next problem, you may use the following lemma (which you proved in Homework 8 for $\theta = (2\pi)/7$, but the proof is the same for any θ):

Lemma 1. *Let $z = \cos\theta + i\sin\theta$ be a complex number with $\sin\theta \neq 0$. Then $\mathbb{Q}(\cos\theta) \subseteq \mathbb{Q}(z)$, and $[\mathbb{Q}(z) : \mathbb{Q}(\cos\theta)] = 2$*

1. (a) Prove that $\cos(2\pi/5)$ is constructible.

   Proof. One can easily see that $z = \cos(2\pi/5) + i\sin(2\pi/5)$ is a primitive 5th root of unity. This means that z is a root of the 5th cyclotomic polynomial, which is also irreducible. Meaning that $[\mathbb{Q}(z) : \mathbb{Q}]$ is the degree of $\Phi_5(x)$. Since $\Phi_n(x)$ is defined to be

   $$\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} (x - e^{2i\pi\frac{k}{n}})$$

   and n is prime, that means Φ_5 has degree $\varphi(5) = 4$.
   So then $4 = [\mathbb{Q}(z) : \mathbb{Q}] = [\mathbb{Q}(z) : \mathbb{Q}(\cos(2\pi/5))] \cdot [\mathbb{Q}(\cos(2\pi/5)) : \mathbb{Q}] = 2 \cdot [\mathbb{Q}(\cos(2\pi/5)) : \mathbb{Q}] \implies [\mathbb{Q}(\cos(2\pi/5)) : \mathbb{Q}] = 2$. So then $\cos(2\pi/5)$ is constructible since its extension has degree a power of 2. ■

   (b) Prove that $\cos(2\pi/7)$ is not constructible.

   Proof. Let $z = \cos(2\pi/7) + i\sin(2\pi/7)$.
   By the same argument in part a, we see that Φ_7 has degree 6, meaning that $6 = [\mathbb{Q}(z) : \mathbb{Q}] = [\mathbb{Q}(z) : \mathbb{Q}(\cos(2\pi/7))] \cdot [\mathbb{Q}(\cos(2\pi/7)) : \mathbb{Q}] = 2 \cdot [\mathbb{Q}(\cos(2\pi/7)) : \mathbb{Q}] \implies [\mathbb{Q}(\cos(2\pi/7)) : \mathbb{Q}] = 3$. So then $\cos(2\pi/7)$ is not constructible since its extension has degree not a power of 2. ■

2. Let F be a field and $f(x) \in F[x]$ a polynomial. Consider the tower of field extensions $F \subseteq F(f(x)) \subseteq F(x)$. For each of the two intermediary extensions, decide whether the extension is algebraic or not. Prove your answers.

Proof. For the field extension $F \subseteq F(f(x))$, one can easily see that a rational function contains indeterminates if it is a nonzero nonconstant polynomial (e.g. the literal 'x' in a polynomial). It is also clear that indeterminates are not algebraic since they cannot be zeros of a polynomial. So $f(x)$ is transcendental, making $F \subseteq F(f(x))$ not algebraic.

For the field extension $F(f(x)) \subseteq F(x)$, we can just consider the indeterminate x being algebraic, since adjoining x generates the whole field $F(x)$. This is because any rational function with coefficients in F is also a rational function with coefficients in $F(f(x))$.
Now to find a polynomial with coefficients in $F(f(x))$ s.t. x is a root. With T being a temporary (meta) indeterminate, let our polynomial be $f(T) - f(x) \in F(f(x))[T]$. We can see that x is a root of the polynomial, making x algebraic. So the field extension $F(f(x)) \subseteq F(x)$ is algebraic. ■

3. (a) Let $\mathbb{Z}_2 \subseteq E$ be a field extension of $\mathbb{Z}_2$, $f(x) \in \mathbb{Z}_2[x]$, and $u \in E$ a root of $f(x)$. Prove that u^2 is also a root of $f(x)$.

   Proof. It is important to note that squaring over $\mathbb{Z}_2$ does not change the element. Now denote $f(x) = \sum_{k=0}^{n} a_k x^k$. Then plugging in u and u^2, we see that

$$\begin{aligned} f(u)^2 &= \left(\sum_{k=0}^{n} a_k u^k\right)^2 \\ &= \left(\sum_{k=0}^{n} a_k^2 u^{2k}\right) + \left(2 \sum_{0 \le i < j \le n} a_i a_j u^{i+j}\right) \\ &= \sum_{k=0}^{n} a_k^2 u^{2k} = \sum_{k=0}^{n} a_k (u^2)^k \\ &= f(u^2) \end{aligned}$$

   So $0 = 0^2 = f(u)^2 = f(u^2)$. ■

   (b) Let $E = \mathbb{Z}_2[x]/(x^2 + x + 1)$. Prove that E is a splitting field of $f(x) = x^2 + x + 1$ over $\mathbb{Z}_2$.

   Proof. First, let us note that it is clear that there are no roots of $f(x)$ in $\mathbb{Z}_2$. And since $f(x)$ has degree 2, then the function is irreducible.
   As E is the quotient ring from the ideal $(x^2 + x + 1)$, then $\bar{x}$, denoted by α for convenience, is a "root" of the function $x^2 + x + 1$.
   By part (a), we then have α^2 also a root.
   Since the polynomial was degree 2, we only needed these two roots: α, α^2.
   Now to check that $\alpha \neq \alpha^2$. BWOC, assume $\alpha + \alpha^2 = 0 \implies \alpha(\alpha + 1) = 0$. But $\alpha \neq 0$ nor $\alpha \neq 1$. So $\alpha \neq \alpha^2$.
   We now have that f is irreducible over $\mathbb{Z}_2[x]$, and all two of its roots are in E. These facts together make E the splitting field. ■

(c) Let $L = \mathbb{Z}_2[x]/(x^3 + x^2 + 1)$. Prove that L is a splitting field of $g(x) = x^3 + x^2 + 1$ over $\mathbb{Z}_2$.

Proof. First, let us note that it is clear that there are no roots of $g(x)$ in $\mathbb{Z}_2$. And since $g(x)$ has degree 3, then the function is irreducible.
As L is the quotient ring from the ideal $(x^3 + x^2 + 1)$, then $\bar{x}$, denoted by α for convenience, is a "root" of the function $x^3 + x^2 + 1$.
By part (a), we then have α^2 also a root, with then α^4 subsequently being a root too.
Since the polynomial was degree 3, we only needed these three roots: $\alpha, \alpha^2, \alpha^4$.
To check that they are distinct roots, we would show two roots adding to 0 makes a contradiction. This would be tedious and long, so it is skipped. We now have that g is irreducible over $\mathbb{Z}_2[x]$, and all three of its roots are in L. These facts together make L the splitting field. ∎

4. For each of the following choices of u, decide whether $\mathbb{Q}(u) = \mathbb{Q}(u^2)$ or not. Prove your answers.

(a) $u = \sqrt[3]{2}$

Proof. We have $\mathbb{Q}(u) = \{a + b\sqrt[3]{2} + c\sqrt[3]{2^2} : a, b, c \in \mathbb{Q}\}$ and $\mathbb{Q}(u^2) = \{a + b\sqrt[3]{4} + c\sqrt[3]{2^4} : a, b, c \in \mathbb{Q}\}$. Note that these sets are the same as $\sqrt[3]{2^4} = 2\sqrt[3]{2}$, making $c\sqrt[3]{2^4}$ match up with $b\sqrt[3]{2}$ between the two sets. So then the extensions are the same. ∎

(b) $u = 1 + \sqrt{2}$

Proof. One can see that $u^2 = 3 + 2\sqrt{2} = 2u + 1$. So since we can rewrite u^2 in terms of u with field operations, $\mathbb{Q}(u^2) \subseteq \mathbb{Q}(u)$. The other direction is shown through $u = \frac{u^2 - 1}{2}$, making $\mathbb{Q}(u) \subseteq \mathbb{Q}(u^2)$. So $\mathbb{Q}(u^2) = \mathbb{Q}(u)$. ∎

(c) $u = \sqrt{2} + \sqrt{3}$

Proof. One can see check that u is a root of $f(x) = x^4 - 10x^2 + 1$, and that $f(x)$ is irreducible over $\mathbb{Q}$ since the roots are the four values $\pm\sqrt{2} \pm \sqrt{3} \notin \mathbb{Q}$. Therefore $[\mathbb{Q}(u) : \mathbb{Q}] = 4$.
Then, we can see also check that $u^2 = 5 + 2\sqrt{6}$ is a root of $f(x) = x^2 - 10x + 1$, and that $f(x)$ is irreducible over $\mathbb{Q}$ since the roots are the two values $5 \pm 2\sqrt{6} \notin \mathbb{Q}$. Therefore $[\mathbb{Q}(u^2) : \mathbb{Q}] = 2$.
Since the two extensions have different degrees, they are not the same extension. ∎