Homework 5

Most problems below are from Judson.

1. Show that each of the following numbers is algebraic over $\mathbb{Q}$ by finding the minimal polynomial of the number over $\mathbb{Q}$.

   (a) $\sqrt{1/3+\sqrt{7}}$

   (b) $\sqrt{3}+\sqrt[3]{5}$

   (c) $\sqrt{3}+\sqrt{2}\,i$

   Solution 1.

   (a) Let $x=\sqrt{1/3+\sqrt{7}}$, then $x^2-1/3=\sqrt{7}$, so $(x^2-1/3)^2=7$. Therefore,
   The minimal polynomial is $x^4-\frac{2}{3}x^2-\frac{62}{9}$.

   (b) The degree of the polynomial should be 6. The basis for the field should be $\{1, \sqrt{3}, \sqrt[3]{5}, \sqrt{3}\sqrt[3]{5}, \sqrt[3]{25}, \sqrt{3}\sqrt[3]{5}\}$.
   Let $\alpha=\sqrt{3}+\sqrt[3]{5}$. The strategy is to write $1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6$ in terms of the basis.

$$
\begin{aligned}
\alpha^0 &= 1+0\sqrt{3}+0\sqrt[3]{5}+0\sqrt{3}\sqrt[3]{5}+0\sqrt[3]{25}+0\sqrt{3}\sqrt[3]{5}\\
\alpha^1 &= 0+\sqrt{3}+\sqrt[3]{5}+0\sqrt{3}\sqrt[3]{5}+0\sqrt[3]{25}+0\sqrt{3}\sqrt[3]{5}\\
\alpha^2 &= 3+0\sqrt{3}+0\sqrt[3]{5}+2\sqrt{3}\sqrt[3]{5}+\sqrt[3]{25}+0\sqrt{3}\sqrt[3]{25}\\
\alpha^3 &= 5+3\sqrt{3}+9\sqrt[3]{5}+0\sqrt{3}\sqrt[3]{5}+0\sqrt[3]{25}+3\sqrt{3}\sqrt[3]{25}\\
\alpha^4 &= 9+20\sqrt{3}+5\sqrt[3]{5}+12\sqrt{3}\sqrt[3]{5}+18\sqrt[3]{25}+0\sqrt{3}\sqrt[3]{25}\\
\alpha^5 &= 150+9\sqrt{3}+45\sqrt[3]{5}+25\sqrt{3}\sqrt[3]{5}+5\sqrt[3]{25}+30\sqrt{3}\sqrt[3]{25}\\
\alpha^6 &= 52+300\sqrt{3}+225\sqrt[3]{5}+54\sqrt{3}\sqrt[3]{5}+135\sqrt[3]{25}+30\sqrt{3}\sqrt[3]{25}
\end{aligned}
$$

   These seven vectors must be linearly dependent. To figure out the linear dependence we can analyze the matrix

$$
\begin{pmatrix}
1 & 0 & 3 & 5 & 9 & 150 & 52\\
0 & 1 & 0 & 3 & 20 & 9 & 300\\
0 & 1 & 0 & 9 & 5 & 45 & 225\\
0 & 0 & 2 & 0 & 12 & 25 & 54\\
0 & 0 & 1 & 0 & 18 & 5 & 135\\
0 & 0 & 0 & 3 & 0 & 30 & 30
\end{pmatrix}
$$

   After reducing it using Gaussian row reduction we get

$$
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 2\\
0 & 1 & 0 & 0 & 0 & 0 & 90\\
0 & 0 & 1 & 0 & 0 & 0 & -27\\
0 & 0 & 0 & 1 & 0 & 0 & 10\\
0 & 0 & 0 & 0 & 1 & 0 & 9\\
0 & 0 & 0 & 0 & 0 & 1 & 0
\end{pmatrix}
$$

Therefore
$$\alpha^6 = 2 + 90\alpha - 27\alpha^2 + 10\alpha + 9\alpha^4.$$
Therefore, the minimal polynomial is
$$x^6 - 9x^4 - 10x^3 + 27x^2 - 90x - 2.$$

(c) The basis is $\{1, \sqrt{3}, \sqrt{2}i, \sqrt{6}i\}$. Let $\alpha = \sqrt{3} + \sqrt{2}i$. We have
$$\begin{aligned}
\alpha^0 &= 1 + 0\sqrt{3} + 0\sqrt{2}i + 0\sqrt{6}i \\
\alpha^1 &= 0 + 1\sqrt{3} + 1\sqrt{2}i + 0\sqrt{6}i \\
\alpha^2 &= 1 + 0\sqrt{3} + 0\sqrt{2}i + 2\sqrt{6}i \\
\alpha^3 &= 0 + -3\sqrt{3} + 7\sqrt{2}i + 0\sqrt{6}i \\
\alpha^4 &= -23 + 0\sqrt{3} + 0\sqrt{2}i + 4\sqrt{6}i
\end{aligned}$$

We now get the matrix
$$\begin{pmatrix} 1 & 0 & 1 & 0 & -23 \\ 0 & 1 & 0 & -3 & 0 \\ 0 & 1 & 0 & 7 & 0 \\ 0 & 0 & 2 & 0 & 4 \end{pmatrix}$$
After Gaussian row reduction we get
$$\begin{pmatrix} 1 & 0 & 0 & 0 & -25 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$
Therefore the minimal polynomial is $x^4 - 2x^2 + 25$.

2. Show that each of the following numbers is algebraic over $\mathbb{Q}$ by finding the minimal polynomial of the number over $\mathbb{Q}$.

   (a) $\cos\theta + i\sin\theta$ for $\theta = 2\pi/n$ with $n \in \mathbb{N}$

   (b) $\sqrt{\sqrt[3]{2} - i}$

Solution 2.

(a) $\cos(\theta) + i\sin(\theta)$ is a root of $x^n - 1$. We want the minimal polynomial though. The minimal polynomial is $\Phi_n(x)$ which satisfies the following recursive equation
$$\prod_{d|n} \Phi_d(x) = x^n - 1.$$
So $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$, $\Phi_3(x) = x^2 + x + 1$, $\Phi_4(x) = \frac{x^4-1}{(x-1)(x+1)} = x^2 + 1$, $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$, $\Phi_6(x) = \frac{x^6-1}{(x-1)(x+1)(x^2+x+1)} = x^2 - x + 1$, and so on.

(b) The degree of $\sqrt[3]{2}$ is 3, the degree of $\sqrt[3]{2} - i$ is 6, therefore the degree of $\sqrt{\sqrt[3]{2} - i}$ is 12. Let $\alpha = \sqrt{\sqrt[3]{2} - i}$. A reasonable basis for the field $\mathbb{Q}(\sqrt[3]{2} - i)$ is
$$\{1, i, \sqrt[3]{2}, \sqrt[3]{2}i, \sqrt[3]{4}, \sqrt[3]{4}i\}.$$

$$\begin{aligned}
\alpha^0 &= 1 \\
\alpha^2 &= -i + \sqrt[3]{2} \\
\alpha^4 &= -1 - 2i\sqrt[3]{2} + \sqrt[3]{4} \\
\alpha^6 &= 2 + i - 3\sqrt[3]{2} - 3i\sqrt[3]{4} \\
\alpha^8 &= 1 - 8i + 2\sqrt[3]{2} + 4i\sqrt[3]{2} - 6\sqrt[3]{4} \\
\alpha^{10} &= -20 - i + 5\sqrt[3]{2} - 10i\sqrt[3]{2} + 2\sqrt[3]{4} + 10i\sqrt[3]{4} \\
\alpha^{12} &= 3 + 40i - 30\sqrt[3]{2} + 6i\sqrt[3]{2} + 15\sqrt[3]{4} - 12i\sqrt[3]{4}
\end{aligned}$$

We row reduce the matrix

$$\begin{pmatrix}
1 & 0 & -1 & 2 & 1 & -20 & 3 \\
0 & -1 & 0 & 1 & -8 & -1 & 40 \\
0 & 1 & 0 & -3 & 2 & 5 & -30 \\
0 & 0 & -2 & 0 & 4 & -10 & -6 \\
0 & 0 & 1 & 0 & -6 & 2 & 15 \\
0 & 0 & 0 & -3 & 0 & 10 & -12
\end{pmatrix}$$

to get

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & -5 \\
0 & 1 & 0 & 0 & 0 & 0 & -12 \\
0 & 0 & 1 & 0 & 0 & 0 & -3 \\
0 & 0 & 0 & 1 & 0 & 0 & 4 \\
0 & 0 & 0 & 0 & 1 & 0 & -3 \\
0 & 0 & 0 & 0 & 0 & 1 & 0
\end{pmatrix}$$

Therefore, the minimal polynomial is

$$x^{12} + 3x^8 - 4x^6 + 3x^4 + 12x^2 + 5.$$

3. Find a basis for each of the following field extensions. What is the degree of each extension?
   (a) $\mathbb{Q}(\sqrt{3}, \sqrt{6}\,)$ over $\mathbb{Q}$
   (b) $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}\,)$ over $\mathbb{Q}$
   (c) $\mathbb{Q}(\sqrt{2}, i)$ over $\mathbb{Q}$

   Solution 3.

   (a) The basis is $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$. The degree is 4.
   (b) The basis is $\{1, \sqrt[3]{2}, \sqrt[3]{4}, \sqrt[3]{3}, \sqrt[3]{6}, \sqrt[3]{12}, \sqrt[3]{9}, \sqrt[3]{18}, \sqrt[3]{36}\}$. The degree is 9.
   (c) The basis is $\{1, \sqrt{2}, i, \sqrt{2}\,i\}$. The degree is 4.

4. Find a basis for each of the following field extensions. What is the degree of each extension?
   (a) $\mathbb{Q}(\sqrt{3}, \sqrt{5}, \sqrt{7}\,)$ over $\mathbb{Q}$
   (b) $\mathbb{Q}(\sqrt{8}\,)$ over $\mathbb{Q}(\sqrt{2}\,)$
   (c) $\mathbb{Q}(\sqrt{2}, \sqrt{6} + \sqrt{10}\,)$ over $\mathbb{Q}(\sqrt{3} + \sqrt{5}\,)$

   Solution 4.

   (a) The basis is $\{1, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{15}, \sqrt{21}, \sqrt{35}, \sqrt{105}\}$. The degree is 8.
   (b) The basis is $\{1\}$. The degree is 1. That is because $\sqrt{8} = 2\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

(c) The basis is $\{1, \sqrt{2}\}$. The degree is 2. (We are using that $\sqrt{2}(\sqrt{3}+\sqrt{5}) = \sqrt{6}+\sqrt{10}$, therefore $\mathbb{Q}(\sqrt{2}, \sqrt{6}+\sqrt{10}) = \mathbb{Q}(\sqrt{3}+\sqrt{5})(\sqrt{2})$.)

5. Determine all of the subfields of $\mathbb{Q}(\sqrt[4]{3}, i)$.

   Solution 5. $\mathbb{Q}, \mathbb{Q}(\sqrt{3}), \mathbb{Q}(i), \mathbb{Q}(\sqrt{3}\,i), \mathbb{Q}(\sqrt[4]{3}), \mathbb{Q}(\sqrt{3}, i), \mathbb{Q}(\sqrt[4]{3}\,i), \mathbb{Q}(\sqrt[4]{3} - \sqrt[4]{3}\,i), \mathbb{Q}(\sqrt[4]{3} + \sqrt[4]{3}\,i), \mathbb{Q}(\sqrt[4]{3}, i)$.

6. Show that $\mathbb{Z}_2[x]/\langle x^3+x+1\rangle$ is a field with eight elements. Construct a multiplication table for the multiplicative group of the field.

   Solution 6. Let α be a root of x^3+x+1, then the multiplication table is:

	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	0	0	0	0	0	0	0
1	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α	0	α	α^2	$\alpha^2+\alpha$	$\alpha+1$	1	$\alpha^2+\alpha+1$	α^2+1
$\alpha+1$	0	$\alpha+1$	$\alpha^2+\alpha$	α^2+1	$\alpha^2+\alpha+1$	α^2	1	α
α^2	0	α^2	$\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α	α^2+1	1
α^2+1	0	α^2+1	1	α^2	α	$\alpha^2+\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$
$\alpha^2+\alpha$	0	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	α^2+1	$\alpha+1$	α	α^2
$\alpha^2+\alpha+1$	0	$\alpha^2+\alpha+1$	α^2+1	α	1	$\alpha^2+\alpha$	α^2	$\alpha+1$

   To illustrate how to calculate. Consider $(\alpha^2+1)(\alpha+1)$. This would be $\alpha^3+\alpha^2+\alpha+1$. Since we know $\alpha^3+\alpha+1=0$, then $\alpha^3+\alpha^2+\alpha+1=\alpha^2$.

7. Prove or disprove: π is algebraic over $\mathbb{Q}(\pi^3)$.

   Solution 7. It is algebraic since it is a root of $x^3-\pi^3 \in \mathbb{Q}(\pi^3)[x]$.

8. Let $p(x)$ be a nonconstant polynomial of degree n in $F[x]$. Prove that there exists a splitting field E for $p(x)$ such that $[E:F] \le n!$.

   Solution 8. Suppose $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the roots of p. Then we want to show that $[F(\alpha_1, \alpha_2, \ldots, \alpha_n) : F] \le n$. Let's start by considering $F(\alpha_1)$. This one has degree $\le n$ (if $p(x)$ is irreducible, the degree is exactly n, otherwise it is smaller). We knnow $[F(\alpha_1) : F] \le n$. Now we want to consider $(F(\alpha_1))(\alpha_2)$. Since $p(x) = (x-\alpha_1)p_1(x)$ in $F(\alpha_1)[x]$, then $[F(\alpha_1,\alpha_2) : F(\alpha_1)] \le n-1$. Similarly, since $p(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_i)p_i(x)$ in $F(\alpha_1, \alpha_2, \ldots, \alpha_i)[x]$,

$$[F(\alpha_1, \alpha_2, \ldots, \alpha_{i+1}) : F(\alpha_1, \alpha_2, \ldots, \alpha_i)] \le n-i.$$

   Therefore

$$\begin{aligned}
&[F(\alpha_1, \alpha_2, \ldots, \alpha_n) : F] \\
&= [F(\alpha_1, \ldots, \alpha_n) : F(\alpha_1, \ldots, \alpha_{n-1})][F(\alpha_1, \ldots, \alpha_{n-1}) : F(\alpha_1, \ldots, \alpha_{n-2})] \cdots [F(\alpha_1) : F] \\
&\le n(n-1)\cdots 1 = n!.
\end{aligned}$$

9. Prove or disprove: $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}(\sqrt{3})$.

   Solution 9. They are not isomorphic. Let's prove it. Suppose $\psi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$ was an isomorphism. Then it must be a ring homomorphism and a bijection. We have $\psi(0) = \psi(0+0) = \psi(0)+\psi(0)$, so $\psi(0)=0$. Similarly $\psi(1) = \psi(1\cdot 1) = \psi(1)\psi(1)$, which implies $\psi(1)=0$ or $\psi(1)=1$. Since ψ is a bijection, $\psi(1) \neq 0$, so $\psi(1)=1$. Now $\psi(2) = \psi(\sqrt{2}\sqrt{2}) = \psi(\sqrt{2})\psi(\sqrt{2})$. But $\psi(2) = \psi(1)+\psi(1) = 2$. Therefore $\psi(\sqrt{2})^2 = 2$. This means $\psi(\sqrt{2})$ is $\sqrt{2}$ or $-\sqrt{2}$. Neither of these is in $\mathbb{Q}(\sqrt{3})$. Therefore they are not isomorphic.

10. Show that $\mathbb{Q}(\sqrt{3}, \sqrt{7}) = \mathbb{Q}(\sqrt{3}+\sqrt{7})$. Extend your proof to show that $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a}+\sqrt{b})$, where $\gcd(a,b)=1$.

Solution 10. $\sqrt{3}+\sqrt{7} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ because fields are closed under addition. But then $\mathbb{Q}(\sqrt{3}+\sqrt{7}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Since $\sqrt{3}+\sqrt{7} \in \mathbb{Q}(\sqrt{3}+\sqrt{7}) = B$, then $(\sqrt{3}+\sqrt{7})^2 = 10 + 2\sqrt{21} \in B$ But that means $\sqrt{21} \in B$. Therefore $\sqrt{21}(\sqrt{3}+\sqrt{7}) \in B$, but that means $3\sqrt{7}+7\sqrt{3} \in B$. But then $(3\sqrt{7}+7\sqrt{3}) - 7(\sqrt{3}+\sqrt{7}) = -4\sqrt{7} \in B$. Therefore $\sqrt{7} \in B$. Also $(3\sqrt{7}+7\sqrt{3}) - 3(\sqrt{3}+\sqrt{7}) = 4\sqrt{3} \in B$, so $\sqrt{3} \in B$. Therefore $\mathbb{Q}(\sqrt{3}, \sqrt{7}) \subseteq B = \mathbb{Q}(\sqrt{3}+\sqrt{7})$. We now have equality.

The proof for arbitrary a, b is similar. Let $A = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ and $B = \mathbb{Q}(\sqrt{a}+\sqrt{b})$. $B \subseteq A$ since $\sqrt{a}+\sqrt{b} \in A$.

We have $(\sqrt{a}+\sqrt{b})^2 \in B$, so $(a+b) + 2\sqrt{ab} \in B$. But then $\sqrt{ab} \in B$. Then $(\sqrt{a}+\sqrt{b})(\sqrt{ab}) \in B$, but

$$(\sqrt{a}+\sqrt{b})\sqrt{ab} = b\sqrt{a} + a\sqrt{b}.$$

Therefore

$$\begin{aligned}(b\sqrt{a}+a\sqrt{b}) - a(\sqrt{a}+\sqrt{b}) &= (b-a)\sqrt{a} \\ (b\sqrt{a}+a\sqrt{b}) - b(\sqrt{a}+\sqrt{b}) &= (a-b)\sqrt{b}\end{aligned}$$

Since $a \neq b$, then $(a-b), (b-a) \in \mathbb{Q}$, so $\sqrt{a}, \sqrt{b} \in B$. Therefore $B \subseteq A$, which implies $A = B$.