Math 392: Assignment 7

- Let $K_1 \subset K_2 \subset \cdots \subset K_n$ be a chain of field extensions such that $K_i \subset K_{i+1}$ is algebraic. Prove that $K_0 \subset K_n$ is algebraic, and compute the degree of the extension, $[K_n : K_0]$.

  Proof: First, we'll prove a true statement: replace the word "algebraic" with the word "finite" above, and that's what we'll prove. (The problem is that while all finite extensions are algebraic, there are algebraic extensions which are not finite.)

  We proceed by induction. Let $n \in \mathbb{N}$, let K_i be as above, and let $\mathrm{P}(n)$ be the statement: $[K_n : K_0] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \cdots [K_1 : K_0]$ Then $\mathrm{P}(1)$ is trivially true, and $\mathrm{P}(2)$ is true by theorem 9.22. To prove the inductive step, assume $\mathrm{P}(n)$ holds, and we'll prove $\mathrm{P}(n+1)$. Notice:

  $$[K_{n+1} : K_0] = [K_{n+1} : K_n][K_n : K_0]$$

  by theorem 9.22. Now by our inductive hypothesis, we have that

  $$\begin{aligned} [K_{n+1} : K_0] &= [K_{n+1} : K_n][K_n : K_0] \\ &= [K_{n+1} : K_n][K_n : K_{n-1}] \cdots [K_1 : K_0] \end{aligned}$$

  This completes our proof

38. Let c be a root $p(x) = 4 + 3x + x^2$ in an extension of $\mathbb{Z}_5$. Show that $p(x)$ is irreducible over $\mathbb{Z}_5$ and calculate the following sums and products in $\mathbb{Z}_5(c)$.

Notice $p(0) = 4, p(1) = 3, p(2) = 4, p(3) = 2, p(4) = 2$. Thus since $deg(p(x)) = 2$ we know $p(x)$ is irreducible over $\mathbb{Z}_5$. Also by $p(c) = 0$ we know $c^2 = 1 + 2c$.

$(3 + 2c) + (3 + 4c) = 1 + c$

$(2 + 3c)(4 + 2c) = 4 + 3c$

$(2 + 4c)^{-1} = 0 + 4c$ since $(2 + 4c)(0 + 4c) = 0 + 3c + c^2 = 0 + 3c + (1 + 2c) = 1$

50. Find the complete addition and multiplication tables for the field $\mathbb{Z}_2(c)$ where c is a root of the irreducible polynomial $p(x) = 1 + x + 0x^2 + x^3$ which is irreducible over $\mathbb{Z}_2$.

The elements of $\mathbb{Z}_2(c)$ are $0, 1, c, 1+c, c^2, 1+c^2, c+c^2, 1+c+c^2$. The Cayley tables are shown below.

$+$	0	1	c	$1+c$	c^2	$1+c^2$	$c+c^2$	$1+c+c^2$
0	0	1	c	$1+c$	c^2	$1+c^2$	$c+c^2$	$1+c+c^2$
1	1	0	$1+c$	c	$1+c^2$	c^2	$1+c+c^2$	$c+c^2$
c	c	$1+c$	0	1	$c+c^2$	$1+c+c^2$	c^2	$1+c^2$
$1+c$	$1+c$	c	1	0	$1+c+c^2$	$c+c^2$	$1+c^2$	c^2
c^2	c^2	$1+c^2$	$c+c^2$	$1+c+c^2$	0	1	c	$1+c$
$1+c^2$	$1+c^2$	c^2	$1+c+c^2$	$c+c^2$	1	0	$1+c$	c
$c+c^2$	$c+c^2$	$1+c+c^2$	c^2	$1+c^2$	c	$1+c$	0	1
$1+c+c^2$	$1+c+c^2$	$c+c^2$	$1+c^2$	c^2	$1+c$	c	1	0

$\cdot$	0	1	c	$1+c$	c^2	$1+c^2$	$c+c^2$	$1+c+c^2$
0	0	0	0	0	0	0	0	0
1	0	1	c	$1+c$	$0+c^2$	$1+c^2$	$c+c^2$	$1+c+c^2$
c	0	c	c^2	$c+c^2$	$1+c$	1	$1+c+c^2$	$1+c^2$
$1+c$	0	$1+c$	$c+c^2$	$1+c^2$	$1+c+c^2$	c^2	1	c
c^2	0	c^2	$1+c$	$1+c+c^2$	$c+c^2$	c	$1+c^2$	1
$1+c^2$	0	$1+c^2$	1	c^2	c	$1+c+c^2$	$1+c$	$c+c^2$
$c+c^2$	0	$c+c^2$	$1+c+c^2$	1	$1+c^2$	$1+c$	c	c^2
$1+c+c^2$	0	$1+c+c^2$	$1+c^2$	c	1	$c+c^2$	c^2	$1+c$

51. Using the result for the previous exercise, determine if there are other roots of $p(x)$ in $\mathbb{Z}_2(c)$.

$p(x) = 1 + x + 0x^2 + x^3$ over $\mathbb{Z}_2$ also has roots c^2 and $c + c^2$ in $\mathbb{Z}_2(c)$.

$p(c^2) = 1 + (c^2) + (c^2)^3 = 1 + c^2 + (c^2)(c + c^2) = 1 + c^2 + 1 + c^2 = 0$

$p(c + c^2) = 1 + (c + c^2) + (c + c^2)^3 = 1 + c + c^2 + (c + c^2)(c) = 1 + c + c^2 + 1 + c + c^2 = 0$

57. Suppose K is a field, E is an extension field of K, and n is a positive integer. Prove: If $[E : K] = n$ and $c \in E$ then the degree of the minimum polynomial for c over K must divide n.

Suppose K is a field, E is an extension field of K, n is a positive integer with $[E : K] = n$, and $c \in E$. We know E is an algebraic extension of K by Theorem 9.21, so c is algebraic over K. Thus $K(c)$ is a finite extension of K. Also by $K \subseteq E$ and $c \in E$ we know that $K(c) \subseteq E$. E is a finite extension $K(c)$ by Exercise 54, so by Theorem 9.22 we know $[E : K(c)][K(c) : K] = [E : K] = n$. Thus we see that $[K(c) : K]$ evenly divides n. Since the minimum polynomial for c over K, $d(x)$, has $deg(d(x)) = [K(c) : K]$ then $deg(d(x))$ must divide n.

63. Prove that $\sqrt{2+i} \notin \mathbb{Q}(\sqrt[3]{2})$ using Theorem 9.22.

Suppose $\sqrt{2+i} \in \mathbb{Q}(\sqrt[3]{2})$. Since $p(x) = -2 + x^3$ is an irreducible (Eisenstein's Criterion) monic polynomial with $\sqrt[3]{2}$ as a root we know $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Now as $\sqrt{2+i} \in \mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ we know $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2+i}) \subseteq \mathbb{Q}(\sqrt[3]{2})$. By Theorem 9.22 $3 = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}(\sqrt{2+i})][\mathbb{Q}(\sqrt{2+i}) : \mathbb{Q}]$.

Consider $t(x) = 5-4x^2+x^4$ in $\mathbb{Q}[x]$. The only possible rational roots are 1, -1, 5, 5 but $t(1) = 2, t(-1) = 2, t(5) = 530, t(-5) = 530$ so either $t(x)$ is irreducible or it factors into two irreducible polynomials of degree 2. Also $t(\sqrt{2+i}) = 5-4(2+i)+(2+i)^2 = 5-8-4i+4+4i-1 = 0$ so $\sqrt{2+i}$ is a root of $t(x)$. Thus the minimum polynomial for $\sqrt{2+i}$ is either $t(x)$ or an irreducible quadratic factor of $t(x)$. Thus $[\mathbb{Q}(\sqrt{2+i}) : \mathbb{Q}]$ is either 2 or 4, both of which are impossible. Thus $\sqrt{2+i} \notin \mathbb{Q}(\sqrt[3]{2})$.

64. Suppose that K is a field and c is algebraic over K with $[K(c) : K] = 2$. Prove: $K(c)$ is the root field for the minimum polynomial of c over K.

Suppose that K is a field and c is algebraic over K with $[K(c) : K] = 2$. Let $p(x) \in K[x]$ be the minimum polynomial for c over K. Suppose E is the root field for $p(x)$. Since c is a root and in $K(c)$ we can factor $p(x) = (-c + x)q(x)$ where $q(x) \in K(c)[x]$. Now $deg(q(x)) = 1$, so $q(x) = u + bx$ for some $u, b \in K(c)$ with $b \neq 0_{K(c)}$. Let $r = -ub^{-1}$ then $r \in K(c)$ and $q(r) = u + b(-ub^{-1}) = u - u = 0_K$. Thus r is the only other root of $q(x)$ since it can have

at most two roots and we can factor $p(x)$ into polynomials of degree 1 over $K(c)$. Hence by Definition 9.23 we have $E \subseteq K(c)$. But also $c \in E$ and $K \subseteq E$ so by Theorem 9.5 we have $K(c) \subseteq E$. Thus $K(c) = E$ and $K(c)$ is the root field for the minimum polynomial of c over K.

65. Suppose K is a field and E is a finite extension of K. Prove: there exist $u_1, u_2, \ldots, u_m \in E$ with $E = K(u_1, u_2, \ldots, u_m)$.

Let K be a field and E a finite extension of K. As E spans E, by Theorem 9.19 there is a basis $B \subseteq E$ for E over K. As the cardinality of the basis is the same as $[E : K]$, B is a finite set, or $B = \{u_1, u_2, \ldots, u_m\}$. We know that $K \subseteq E$, and $u_1, u_2, \ldots, u_m \in E$ so we have $K(u_1, u_2, \ldots, u_m) \subseteq E$. But also for any $t \in E$ we can write $t = a_1u_1 + a_2u_2 + \cdots + a_mu_m$ with all $a_j \in K$. Thus $t \in K(u_1, u_2, \ldots, u_m)$ and so $E \subseteq K(u_1, u_2, \ldots, u_m)$. Therefore $E = K(u_1, u_2, \ldots, u_m)$.

66. Find the root field E for $a(x) = \frac{5}{4} + 6x + \frac{11}{2}x^2 + 2x^3 + \frac{1}{4}x^4$ over $\mathbb{Q}$.

Consider first the associate $b(x) = 5 + 24x + 22x^2 + 8x^3 + x^4$. Notice that $b(x) = (5 + 4x + x^2)(1 + 4x + x^2)$ so we need to find the roots of both $d(x) = 5 + 4x + x^2$ and $t(x) = 1 + 4x + x^2$.

Using the quadratic formula we find the roots of $d(x) = 5 + 4x + x^2$ as seen below:

$$c_1 = \frac{-4+\sqrt{16-4(1)(5)}}{2} = \frac{-4+\sqrt{-4}}{2} = \frac{-4+2i}{2} = -2 + i$$
$$c_2 = \frac{-4-\sqrt{16-4(1)(5)}}{2} = \frac{-4-\sqrt{-4}}{2} = \frac{-4-2i}{2} = -2 - i$$

Similarly using the quadratic formula we find the roots of $t(x) = 1 + 4x + x^2$ as seen below:

$$c_3 = \frac{-4+\sqrt{16-4(1)(1)}}{2} = \frac{-4+\sqrt{12}}{2} = \frac{-4+2\sqrt{3}}{2} = -2 + \sqrt{3}$$
$$c_4 = \frac{-4-\sqrt{16-4(1)(1)}}{2} = \frac{-4-\sqrt{12}}{2} = \frac{-4-2\sqrt{3}}{2} = -2 - \sqrt{3}$$

Thus by Theorem 9.26 the root field of $b(x)$ is $E = \mathbb{Q}(-2 + i, -2 - i, -2 + \sqrt{3}, -2 - \sqrt{3})$. Notice however that $2 \in \mathbb{Q}$ and $-2 - i = -4 - (-2 + i)$. Also $-2 - \sqrt{3} = -4 - (-2 + \sqrt{3})$ so $E = \mathbb{Q}(-2 + i, -2 + \sqrt{3})$.

67. Prove that $\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ and use it to show $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$.

Consider $u = \sqrt{2} + \sqrt{3}$, then $\frac{1}{2}(u^3 - 9u) \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

$$\begin{aligned}
\tfrac{1}{2}(u^3 - 9u) &= \tfrac{1}{2}\left((\sqrt{2}+\sqrt{3})^3 - 9(\sqrt{2}+\sqrt{3})\right) \\
&= \tfrac{1}{2}\left((\sqrt{2}+\sqrt{3})(5+2\sqrt{6}) - 9(\sqrt{2}+\sqrt{3})\right) \\
&= \tfrac{1}{2}\left(11\sqrt{2}+9\sqrt{3} - 9(\sqrt{2}+\sqrt{3})\right) \\
&= \tfrac{1}{2}\left(2\sqrt{2}\right) \\
&= \sqrt{2}
\end{aligned}$$

Thus $\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ as needed. We know that $-2+x^2$ is the minimum polynomial for $\sqrt{2}$ over $\mathbb{Q}$ and $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Thus we only need to find $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}(\sqrt{2})]$. Let $t(x) = -1 - 2\sqrt{2}x + x^2$. Then $t(x) \in \mathbb{Q}(\sqrt{2})[x]$, has $\sqrt{2}+\sqrt{3}$ as a root as seen below:

$$\begin{aligned}
t(\sqrt{2}+\sqrt{3}) &= -1 - 2\sqrt{2}(\sqrt{2}+\sqrt{3}) + (\sqrt{2}+\sqrt{3})^2 \\
&= -1 - 4 - 2\sqrt{6} + 5 + 2\sqrt{6} \\
&= 0
\end{aligned}$$

If $t(x)$ is reducible over $\mathbb{Q}(\sqrt{2})$ it must factor into polynomials of degree 1 and thus each of its roots is in $\mathbb{Q}(\sqrt{2})$. Thus by showing $\sqrt{2}+\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ we can conclude $t(x)$ is irreducible over $\mathbb{Q}(\sqrt{2})$. Clearly if $\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2})$ then also $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$, so suppose we have $\sqrt{3} = a + b\sqrt{2}$ where $a, b \in \mathbb{Q}$. Thus $3 = a^2 + 2ab\sqrt{2} + 2b^2$ which means that $\sqrt{2}$ is a root of a polynomial of degree 1 over $\mathbb{Q}$ and $\sqrt{2} \in \mathbb{Q}$. However $-2+x^2$ is the minimum polynomial for $\sqrt{2}$ over $\mathbb{Q}$ which is impossible. Thus $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, and $t(x)$ is irreducible over $\mathbb{Q}(\sqrt{2})$. Thus $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ and so $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = 4$.