Math 581 Problem Set 5 Solutions

1. Show that the set $\{\sqrt{2}, \sqrt{2}+i, \sqrt{3}-i\}$ is linearly independent over $\mathbb{Q}$.

Proof: Suppose there exists a_0, a_1, and a_2 in $\mathbb{Q}$ so that

$$a_0\sqrt{2} + a_1(\sqrt{2}+i) + a_2(\sqrt{3}-i) = 0.$$

Then we see immediately that we must have $a_1 - a_2 = 0$ as these are the coefficients of the complex part of this equation. Thus, $a_1 = a_2$. Using this and looking at the real part of the equation we have

$$(a_0 + a_1)\sqrt{2} + a_1\sqrt{3} = 0.$$

This is impossible. (For example, square both sides and you'd get $\sqrt{6} \in \mathbb{Q}$.) Thus it must be that this set is linearly independent over $\mathbb{Q}$. ■

2. Let $F \subseteq K$ be fields with $[K : F] = p$ for some prime number p.
(a) Show that there is no field E so that $F \subsetneq E \subsetneq K$.

Proof: Suppose there is such a field E. Using Proposition 1.5 we have $p = [K : F] = [K : E][E : F]$. This implies that either $[K : E] = 1$ or $[E : F] = 1$, i.e., that either $K = E$ or $E = F$, a contradiction. Thus, no such field can exist. ■

(b) Use part (a) to conclude there is no field F so that $\mathbb{R} \subsetneq F \subsetneq \mathbb{C}$.

Proof: Since $[\mathbb{C} : \mathbb{R}] = 2$ and 2 is prime, we immediately see from part (a) that there can be no field between $\mathbb{R}$ and $\mathbb{C}$. ■

(c) Let $\alpha \in K$ with $\alpha \notin F$. Prove that $K = F[\alpha]$.

Proof: Using part (a) we see that $F[\alpha] = F$ or $F[\alpha] = K$. Since $\alpha \notin F$, $F[\alpha] \neq F$. Thus we have the result. ■

(d) Use part (c) to conclude that $\mathbb{C} = \mathbb{R}[i]$.

Proof: Since $i \notin \mathbb{R}$, we must have $\mathbb{C} = \mathbb{R}[i]$ by part (c). ■

3. Let V be a vector space over $\mathbb{Q}$. Prove that if $v, w \in V$ are linearly independent, then so are $v + w$, $2v - w$.

Proof: Suppose there exists $a, b \in \mathbb{Q}$ so that

$$a(v + w) + b(2v - w) = 0.$$

In particular, we have that $(a+2b)v+(a-b)w = 0$. Using that v and w are linearly independent over $\mathbb{Q}$ we have that $a + 2b = 0$ and $a - b = 0$. Thus, $a = b$ and $b + 2b = 0$, i.e., $b = 0$ and $a = 0$. Thus, the set $v + w$ and $2v - w$ is a linearly independent set over $\mathbb{Q}$. $\blacksquare$

4. Prove that $\{v_1, \ldots, v_k\}$ is a basis for V if and only if every vector in V can be written uniquely as a linear combination of $v_1, \ldots, v_k$.

5. Give a basis and the degree of the field extension in each of the following cases:
(a) $V = \mathbb{Q}[\omega_7]$ over $\mathbb{Q}$ where ω_7 is a seventh root of unity

A basis is given by $\{1, \omega_7, \omega_7^2, \omega_7^3, \omega_7^4, \omega_7^5\}$ and the degree of the extension is 6.

(b) $V = \mathbb{Q}[\omega_6]$ over $\mathbb{Q}[i]$ where ω_6 is a sixth root of unity

This problem is actually a mistake as written. The field $\mathbb{Q}[\omega_6]$ is the field $\mathbb{Q}[i\sqrt{3}]$ and is not an extension of $\mathbb{Q}[i]$! The problem was changed to read (for extra credit points) find a basis of $\mathbb{Q}[i, \sqrt{3}]$ over $\mathbb{Q}[\omega_6]$ and of course to prove it is a basis.
We begin by looking at $\mathbb{Q}[\sqrt{3}, i]$ over $\mathbb{Q}$ as this is a bit different then the field extensions we have encountered thus far. Observe that we have the following diagram of fields:

$$\begin{tikzcd}
 & \mathbb{Q}[\sqrt{3}, i] \arrow[dl, dash, "m"'] \arrow[dr, dash, "n"] & \\
\mathbb{Q}[\sqrt{3}] \arrow[dr, dash, "2"'] & & \mathbb{Q}[i] \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

We would like to show that $m = n = 2$ to show that $[\mathbb{Q}[\sqrt{3}, i] : \mathbb{Q}] = 4$. To see this, observe that $x^2 + 1$ is still an irreducible polynomial over $\mathbb{Q}[\sqrt{3}]$ as $\pm i \notin \mathbb{Q}[\sqrt{3}]$. Thus, $m = 2$. Incidentally, this also proves $n = 2$ and so $x^2 - 3$

is irreducible over $\mathbb{Q}[i]$ as well. So we now know that a basis of $\mathbb{Q}[\sqrt{3}, i]$ over $\mathbb{Q}$ must contain 4 elements. We claim that $\{1, i, \sqrt{3}, i\sqrt{3}\}$ is a basis. Since we know the dimension is 4, we only need to show these vectors are linearly independent or span the space to conclude they are a basis. We choose to show linear independence. Suppose there exists $a, b, c, d \in \mathbb{Q}$ so that

$$a + bi + c\sqrt{3} + di\sqrt{3} = 0.$$

Rearranging this we get $(a + c\sqrt{3}) + i(b + d\sqrt{3}) = 0$. Now we use that $\mathbb{C}$ is a 2-dimensional vector space over $\mathbb{R}$ with basis $\{1, i\}$ to conclude that we must have $a + c\sqrt{3} = 0 = b + d\sqrt{3}$. Finally, use that $\mathbb{Q}[\sqrt{3}]$ is a 2-dimensional vector space over $\mathbb{Q}$ with basis $\{1, \sqrt{3}\}$ to conclude that $a = c = 0$ and $b = d = 0$. Thus, we obtain linear independence of the set $\{1, i, \sqrt{3}, i\sqrt{3}\}$ as desired.
Recall that $\mathbb{Q}[i\sqrt{3}] = \{a + bi\sqrt{3} : a, b \in \mathbb{Q}\}$. When we consider $\mathbb{Q}[\sqrt{3}, i]$ as a vector space over $\mathbb{Q}[i\sqrt{3}]$, our constants will be of the form $a + bi\sqrt{3}$ for $a, b \in \mathbb{Q}$. We claim $\{1, i\}$ is a basis of $\mathbb{Q}[\sqrt{3}, i]$ over $\mathbb{Q}[i\sqrt{3}]$. Let $a + bi + c\sqrt{3} + di\sqrt{3} \in \mathbb{Q}[\sqrt{3}, i]$ with $a, b, c, d \in \mathbb{Q}$. (We use here that $\{1, i, \sqrt{3}, i\sqrt{3}\}$ is a basis of $\mathbb{Q}[\sqrt{3}, i]$ over $\mathbb{Q}$!) To see that $\{1, i\}$ spans, observe that $(a + di\sqrt{3}) + (b - ci\sqrt{3})i = a + bi + c\sqrt{3} + di\sqrt{3}$ and $a + di\sqrt{3}$, $b - ci\sqrt{3}$ are in $\mathbb{Q}[i\sqrt{3}]$. To prove linear independence, suppose there exists $\alpha = a + bi\sqrt{3}$ and $\beta = c + di\sqrt{3}$ in $\mathbb{Q}[i\sqrt{3}]$ so that $\alpha + \beta i = 0$. (Note here that you are using constants in the field the vector space is defined over, in this case $\mathbb{Q}[i\sqrt{3}]$!) So we have $a + bi\sqrt{3} + ci - d\sqrt{3} = 0$. Now just use the linear independence of $\{1, i, \sqrt{3}, i\sqrt{3}\}$ over $\mathbb{Q}$ to conclude that $a = b = c = d = 0$ and we are done. Thus $\{1, i\}$ is a basis of $\mathbb{Q}[\sqrt{3}, i]$ over $\mathbb{Q}[i\sqrt{3}]$ and so the dimension is 2. Note that a choice of basis is NOT unique, so it is quite possible to choose a different basis and still be correct. ■

(c) $V = \mathbb{C}$ over $\mathbb{R}$

This is a degree 2 extension with basis $\{1, i\}$.

(d) $V = (\mathbb{Z}/7\mathbb{Z})[x]/\langle x^3 - 3\rangle$ over $\mathbb{Z}/7\mathbb{Z}$.

The first thing one needs to observe is that $x^3 - 3$ is irreducible over $(\mathbb{Z}/7\mathbb{Z})[x]$ as one sees by showing $j^3 \neq 3$ for all $j \in \mathbb{Z}/7\mathbb{Z}$. So this is actually a field. A basis is then given by $\{1, \overline{x}, \overline{x}^2\}$ and the degree of the extension is 3. Note this gives a field with 7^3 elements.

6. Let $f(x) = 2x^{15} - 49x^{12} + 21x^7 + 70x^2 + 35$. Let K be an extension field of $\mathbb{Q}$ with $[K : \mathbb{Q}] = 32$. Show K does not contain any roots of $f(x)$.

Proof: First we observe that $f(x)$ is irreducible. This follows from Eisenstein's criterion with $p = 7$. Suppose K contains a root α of $f(x)$. We have that $\mathbb{Q} \subsetneq \mathbb{Q}[\alpha] \subset K$. However, we know from Lemma 1.6 that $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 15$. This would imply using Proposition 1.5 that $15|32$, clearly a contradiction. Thus K can contain no roots of $f(x)$. ■

7. Let p be a prime number. Show that $\mathbb{Q}[\sqrt[21]{p}] = \mathbb{Q}[\sqrt[3]{p}, \sqrt[7]{p}]$.

Proof: First observe that $\mathbb{Q}[\sqrt[3]{p}, \sqrt[7]{p}] \subseteq \mathbb{Q}[\sqrt[21]{p}]$ since $(\sqrt[21]{p})^7 = \sqrt[3]{p}$ and $(\sqrt[21]{p})^3 = \sqrt[7]{p}$. Since $f(x) = x^{21} - p$ is irreducible (see problem 8(a)), we know that $[\mathbb{Q}[\sqrt[21]{p}] : \mathbb{Q}] = 21$. If we can show that $[\mathbb{Q}[\sqrt[3]{p}, \sqrt[7]{p}] : \mathbb{Q}] = 21$, then we will have that $\mathbb{Q}[\sqrt[21]{p}] = \mathbb{Q}[\sqrt[3]{p}, \sqrt[7]{p}]$ by using Proposition 1.5. We have the following diagram of fields:

$$\begin{tikzcd}
& \mathbb{Q}[\sqrt[3]{p}, \sqrt[7]{p}] \arrow[dl, dash, "m"'] \arrow[dr, dash, "n"] & \\
\mathbb{Q}[\sqrt[7]{p}] \arrow[dr, dash, "7"'] & & \mathbb{Q}[\sqrt[3]{p}] \arrow[dl, dash, "3"] \\
& \mathbb{Q} &
\end{tikzcd}$$

We now need to determine what m and n are. Note that we have that $3|[\mathbb{Q}[\sqrt[3]{p}, \sqrt[7]{p}] : \mathbb{Q}]$ and $7|[\mathbb{Q}[\sqrt[3]{p}, \sqrt[7]{p}] : \mathbb{Q}]$ and so the least common multiple of 3 and 7 divides $[\mathbb{Q}[\sqrt[3]{p}, \sqrt[7]{p}] : \mathbb{Q}]$, i.e., $21|[\mathbb{Q}[\sqrt[3]{p}, \sqrt[7]{p}] : \mathbb{Q}]$. Note that $x^3 - p$ is the irreducible polynomial over $\mathbb{Q}$ that generates the extension $\mathbb{Q}[\sqrt[3]{p}]$. It is possible that $x^3 - p$ is reducible over $\mathbb{Q}[\sqrt[7]{p}]$ (in fact it cannot be, as you should be able to prove!). Regardless, since $\sqrt[3]{p}$ must be a root of a factor of $x^3 - p$ over $\mathbb{Q}[\sqrt[7]{p}]$, we have that $[\mathbb{Q}[\sqrt[7]{p}, \sqrt[3]{p}] : \mathbb{Q}[\sqrt[7]{p}]] \leq 3$, i.e., $m \leq 3$. Using Proposition 1.5 we obtain that $[\mathbb{Q}[\sqrt[3]{p}, \sqrt[7]{p}] : \mathbb{Q}] \leq 3 \cdot 7 = 21$. However, we already had $21|[\mathbb{Q}[\sqrt[3]{p}, \sqrt[7]{p}] : \mathbb{Q}]$, so it must be that $[\mathbb{Q}[\sqrt[3]{p}, \sqrt[7]{p}] : \mathbb{Q}] = 21$ as desired and the result follows. ■

8. Let p be a prime number.
(a) Let $n \in \mathbb{N}$. Show that $f(x) = x^n - p$ is irreducible.

Proof: This polynomial is irreducible by Eisenstein's criterion with the prime p.■

(b) What is the degree of the field $\mathbb{Q}[\sqrt[n]{p}]$ over $\mathbb{Q}$?

The degree of this extension is n.

(c) Use part (b) to show that $\mathbb{R}$ is not a finite extension of $\mathbb{Q}$.

Proof: Suppose $\mathbb{R}$ is a finite extension of $\mathbb{Q}$, say $[\mathbb{R} : \mathbb{Q}] = N$ for some $N \in \mathbb{N}$. Choose $n > N$. Then we have $\mathbb{Q} \subset \mathbb{Q}[\sqrt[n]{p}] \subset \mathbb{R}$ with $[\mathbb{Q}[\sqrt[n]{p}] : \mathbb{Q}] = n > N$. However, this is a contradiction as Proposition 1.5 implies that $n|N$. Thus, it must be that $\mathbb{R}$ is not a finite degree extension of $\mathbb{Q}$. ■

9. Let $f(x) \in \mathbb{Q}[x]$ be a polynomial of degree n and let K be the splitting field of $f(x)$. Prove that $[K : \mathbb{Q}] \leq n!$.

Proof: The easiest way to prove this result is to actually prove a more general result: Let $f(x) \in F[x]$ be a polynomial of degree n and let K be the splitting field of $f(x)$. Prove that $[K : F] \leq n!$.
We prove this result by induction on the degree of $f(x)$. The case of $n = 1$ is clear as there is no extension so the degree is clearly 1. Assume inductively that for a polynomial $g(x) \in E[x]$ where E is some field that the splitting field E_g of $g(x)$ has degree less then or equal to $(\deg g(x))!$ whenever $\deg(g(x)) \leq k - 1$. Note here that it is important to assume the result for all fields and all degrees of $g(x)$ less then or equal to $k - 1$. We will see why this is important in a moment.
Let $f(x) \in F[x]$ be a polynomial of degree k. Let α be a root of $f(x)$ and consider $F[\alpha]$ over F. The degree of this extension is at most k and is equal to k precisely when $f(x)$ is irreducible. We can factor $f(x) = (x - \alpha)^m g(x)$ in $F[\alpha][x]$. The degree of $g(x)$ is $k - m$ and so we can apply our induction hypothesis to $g(x)$ and the field $E = F[\alpha]$. So the splitting field E_g of $g(x)$ is a finite extension of $F[\alpha]$ of degree at most $(k - m)!$. Since E_g contains α and all the roots of $g(x)$, it must contain all the roots of $f(x)$. In particular, the splitting field of $f(x)$ must be contained in E_g. However, we see that we have $F \subseteq F[\alpha] \subseteq E_g$ and we have $[E_g : F] = [E_g : F[\alpha]][F[\alpha] : F] \leq k(k - m)! \leq k(k - 1)! = k!$. Now using that the splitting field of $f(x)$ is a subfield of E_g, it must be its degree over F is less then or equal to the degree of E_g over F, i.e., the degree of the splitting field of $f(x)$ over F is at most $k!$. Thus we are done by induction. ■