# Modern Algebra II: Problem Set 7

Nilay Kumar

Last updated: March 11, 2013

## Problem 1

Let $E = \mathbb{Q}(\sqrt{5}, \sqrt{7})$ and let $\alpha = 2\sqrt{5} - \sqrt{7} \in E$. We know that $\mathbb{Q}(\sqrt{5}, \sqrt{7}) = \mathbb{Q}(\sqrt{5})(\sqrt{7})$. Since $\sqrt{5}$ and $\sqrt{7}$ are obviously algebraic over $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{5})$ respectively, $E$ is a finite extension over $\mathbb{Q}$ by the theorem proved in class. Furthermore, since $\deg \operatorname{irr}(\sqrt{5}, \mathbb{Q}, x) = \deg x^2 - 5 = 2$ and $\deg \operatorname{irr}(\sqrt{7}, \mathbb{Q}(\sqrt{5}), x) = \deg x^2 - 7 = 2$, we have, $[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt{5})][\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2 \cdot 2 = 4$. We can write a basis for $E$, then, to be $\left\{1, \sqrt{5}, \sqrt{7}, \sqrt{35}\right\}$.

Let us now show that $E = \mathbb{Q}(\alpha)$. It is obvious that $\mathbb{Q}(\alpha) \subset E$ – let us show that $E \subset \mathbb{Q}(\alpha)$. First note that $\sqrt{35} \in \mathbb{Q}(\alpha)$, as

$$\alpha^2 = (2\sqrt{5} - \sqrt{7})^2 = 27 - 4\sqrt{35}.$$

Then we have $\alpha\sqrt{35} = 10\sqrt{7} - 7\sqrt{5}$. We can use this to show that

$$\begin{aligned} 13\sqrt{5} &= \alpha\sqrt{35} + 10\alpha \\ 27/2 \cdot \sqrt{2} &= \alpha\sqrt{35} - 7/2 \cdot \alpha, \end{aligned}$$

i.e. $\sqrt{5}$ and $\sqrt{7}$ are in $\mathbb{Q}(\alpha)$. Thus, $E = \mathbb{Q}(\alpha)$. We then know that $\deg \operatorname{irr}(\alpha, \mathbb{Q}, x) = 4$. Then, with some computation, we find

$$\begin{aligned} \alpha^2 &= 27 - 4\sqrt{35} \\ \alpha^4 &= 1289 - 216\sqrt{35} \\ 0 &= \alpha^4 - 54\alpha^2 + 169, \end{aligned}$$

i.e. $\operatorname{irr}(\alpha, \mathbb{Q}, x) = x^4 - 54x^2 + 169$. Finally, since we know that $[\mathbb{Q}(\alpha) = E : \mathbb{Q}] = 4$, $\left\{1, \alpha, \alpha^2, \alpha^3\right\}$ must be another basis for $E$.

## Problem 2

First note that $\mathbb{Q}(i)$ is a 2-dimensional finite extension of $\mathbb{Q}$, as $i$ is algebraic over $\mathbb{Q}$ and $\deg \operatorname{irr}(i, \mathbb{Q}, x) = \deg x^2 + 1 = 2$. Furthermore, $\mathbb{Q}(i, \sqrt[4]{2})$ is a 4-dimensional finite extension of $\mathbb{Q}(i)$, as $\sqrt[4]{2}$ is algebraic over $\mathbb{Q}(i)$ and $\deg \operatorname{irr}(\sqrt[4]{2}, \mathbb{Q}(i), x) = \deg x^2 - 4 = 4$. Then, $[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = 4 \cdot 2 = 8$. Note that $\{1, i\}$ forms a $\mathbb{Q}$-basis for $\mathbb{Q}(i)$ and that $\left\{1, \sqrt[4]{2}, \sqrt[4]{2}^2, \sqrt[4]{2}^3\right\}$ forms a $\mathbb{Q}(i)$ basis for $\mathbb{Q}(i, \sqrt[4]{2})$. It follows, then, that $\left\{1, i, \sqrt[4]{2}, \sqrt[4]{2}^2, \sqrt[4]{2}^3, i\sqrt[4]{2}, i\sqrt[4]{2}^2, i\sqrt[4]{2}^3\right\}$ forms a $\mathbb{Q}$-basis for $\mathbb{Q}(i, \sqrt[4]{2})$.

If $\alpha = i + \sqrt[4]{2}$, we can compute

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

Squaring this yields the eighth order irreducible polynomial for $\alpha$.

## Problem 3

Let $F$ be a field of characteristic not equal to 2. Suppose that $E$ is a finite extension field of $F$ and that $[E : F] = 2$. Thus, $E$ is a 2-dimensional $F$-vector space. This implies the existence of an $\alpha$ not in $F$, because otherwise, $E$ would be 1-dimensional, as $E$ would equal $F$. Since $\alpha^2 \in E$, we can write $\alpha^2 - d\alpha - c = 0$ for some $c, d \in F$. Completing the square, we find $(\alpha - d/2)^2 - d^2/4 - c = 0$, which yields

$$(\alpha - d/2)^2 = d^2/4 - c.$$

If we define $\beta = \alpha - d/2$ and $a = d^2/4 - c$, then, we have found a $\beta \notin F$ that satisfies $\beta^2 = a$.

Finally, let us show that $E = F(\beta)$; i.e. that every $c + d\alpha$ can be written as $e + f\beta$ for some $e, f \in F$ (and vice versa):

$$c + d\alpha = c + d(\beta + d/2) = cd/2 + d\beta$$

$$e + f\beta = e + f(\alpha - d/2) = -ed/2 + f\alpha$$

and we are done.

## Problem 4

Let $F$ be a field and suppose that $F$ is a subring of an integral domain $R$. Thus $R$ is a vector space over $F$. Suppose further that $R$ is a finite,

$d$-dimensional vector space over $F$. Then, if we consider the set of vectors $\{1, r, r^2, \cdots\}$, there must be some non-trivial linear combination that yields zero, as they cannot all be linearly independent. Take $\sum_{i=0}^{n} a_i r^i = 0$, with $a_i \in F$ not identically zero and $n \geq d$. Let $m$ be the smallest $i$ such that $a_i \neq 0$. Then the sum becomes $\sum_{i=m}^{n} a_i r^i = r^m \sum_{i=m}^{n} a_i r^{i-m} = 0$. Since $R$ is an integral domain, we can cancel the factor out front, and we get $\sum_{i=m}^{n} a_i r^{i-m} = 0$. Note that $m$ cannot equal $n$ (otherwise we'd only have one term, and that too, trivial, with $a_n = 0$), so

$$a_m + a_{m+1} r + \cdots + a_n r^{n-m} = 0,$$

and dividing through by $-a_m$ and factoring out an $r$ shows that $r$ times some element of $R$ is equal to 1, i.e. that $r$ has an inverse. This implies that $R$ is a field, as $r$ was arbitrary, and we are done.

## Problem 5

Let $E$ be a finite extension of a field $F$, and suppose that the degree $[E : F] = t$ is a prime number. Take some $\alpha \in E$ that is not in $F$. It should be clear that $F \leq F(\alpha) \leq E$, as $F(\alpha)$ is the smallest field containing $F$ and $\alpha$. Then we have

$$\begin{aligned} [E : F] &= [E : F(\alpha)][F(\alpha) : F] \\ t &= [E : F(\alpha)][F(\alpha) : F]. \end{aligned}$$

Since $t$ is prime, and $F(\alpha) \neq F$ (by construction) and so $[F(\alpha) : F] \neq 1$, we must have that $[F(\alpha) : F] = t$ and $[E : F(\alpha)] = 1$. Consequently, $E = F(\alpha)$ for all such $\alpha$, and $E$ must be a simple extension of $F$.

## Problem 6

Let $F$ be a field and let $E = F(\alpha)$ be a finite extension field of $F$ with $\alpha \notin F$ such that $[E : F] = \deg_F \alpha = 2n+1$, $n \in \mathbb{N}$. It should be clear that $\alpha^2 \notin F$, as otherwise $[E : F]$ would be 2, which is a contradiction. Furthermore, $F(\alpha^2) \leq F(\alpha)$, as $\alpha^2 \in F(\alpha)$. Then we can write

$$[F(\alpha) : F] = 2n + 1 = [F(\alpha) : F(\alpha^2)][F(\alpha^2) : F]$$

Consider $[F(\alpha) : F(\alpha^2)] = \deg_{F(\alpha^2)} \alpha = \deg \operatorname{irr}(\alpha, F(\alpha^2), x)$. Since this irreducible polynomial must divide $x^2 - \alpha^2$, either $[F(\alpha) : F(\alpha^2)]$ is one or two. It cannot be two, however, as this would contradict the above product (since an odd is always the product of two odds). Consequently, $[F(\alpha) : F(\alpha^2)] = 1$, i.e $F(\alpha) = F(\alpha^2)$.

## Problem 7

Let $F$ be a field and $E$ an extension field of $F$. Suppose that $\alpha, \beta \in E$ are both algebraic over $F$, and that $\deg_F \alpha = n, \deg_F \beta = m$. If we construct $F(\alpha)$, it should be clear that $\beta$ is algebraic over $F(\alpha)$, as the polynomial in $F[x]$ whose solution is $\beta$ is also in $F(\alpha)[x]$. For precisely this reason, $\deg_{F(\alpha)} \beta$ cannot be greater than $m$, i.e. $\deg_{F(\alpha)} = [F(\alpha, \beta) : F(\alpha)] \leq m$. Then, using

$$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)]n,$$

we have that $[F(\alpha, \beta) : F] \leq mn$. Hence, since $\alpha + \beta$ and $\alpha\beta$ are in $F(\alpha, \beta)$, we must have $\deg_F(\alpha + \beta) \leq mn$ and $\deg_F(\alpha\beta) \leq mn$.

## Problem 8

Let $F$ be a field and $E$ an extension field of $F$. Suppose that $\alpha \in E$ and $\beta \in E$ are both algebraic over $F$, and that $\deg_F \alpha = n, \deg_F \beta = m$, with $n$ and $m$ relatively prime. We can compute

$$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)]n$$

and

$$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\beta)]m.$$

Both $n, m$ divide $[F(\alpha, \beta) : F]$, and since $n, m$ are relatively prime, this degree must be a multiple of $mn$. By the last problem, however, we know that the degree must be less than or equal to $mn$, and thus the degree of $F(\alpha, \beta)$ over $F$ is $nm$.

We can use this result to compute

$$[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] = 2 \times 3 = 6$$

because $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ are relatively prime.