MATH453M Homework Solutions Week 7

Nick Inglis
ninglis@math.purdue.edu

3.2.1 We have $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = (x - c_1)(x - c_2)\ldots(x - c_n)$ so that $a_0 = f(0) = (-c_1)(-c_2)\ldots(-c_n) = (-1)^n c_1c_2\ldots c_n$. Using the distributive law the product is a sum of terms, each of which is a product, selecting one entry from each bracket ($x - c_i$). To get a constant multiple of x^{n-1} we must pick x from all but one bracket and $-c_i$ from the other bracket. therefore a_{n-1}, the coefficient of x^{n-1} is $-c_1 - c_2 - \cdots - c_n$.

3.2.2 a Let $\alpha = \sqrt{2}+i$, so $\mathbb{Q}[\alpha] \subseteq \mathbb{Q}[\sqrt{2}, i]$. Then $\alpha^3 = -\sqrt{2}+5i$ so that $i = (\alpha^3+\alpha)/5 \in \mathbb{Q}[\alpha]$. Hence $\sqrt{2} = \alpha - i \in \mathbb{Q}[\alpha]$ so $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{2}, i]$.

If $i \in \mathbb{Q}[\sqrt{2}i]$ then $i = a + b\sqrt{2}i$ for some $a, b \in \mathbb{Q}$. Then $a = 0$ since i has no real part, so $1 = b\sqrt{2}$, which is impossible since $\sqrt{2} \notin \mathbb{Q}$.

3.2.2 b Let $\alpha = \sqrt{2}+\sqrt{3}$, so $\mathbb{Q}[\alpha] \subseteq \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Then $\alpha^3 = 11\sqrt{2}+9\sqrt{3}$ so that $\sqrt{2} = (\alpha^3-9\alpha)/2 \in \mathbb{Q}[\alpha]$ and $\sqrt{3} = (11\alpha - \alpha^3)/2 \in \mathbb{Q}[\alpha]$. Hence $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

If $\sqrt{2} \in \mathbb{Q}[\sqrt{6}]$ then $\sqrt{2} = a + b\sqrt{6}$ for some $a, b \in \mathbb{Q}$. Then $2 = a^2 + 2ab\sqrt{6} + 6b^2$, so $ab = 0$ since $2ab\sqrt{6}$ is the only irrational term. Now if $b = 0$ then $2 = a^2$ which is impossible with $a \in \mathbb{Q}$ and if $b = 0$ then $2 = 6b^2$ so $1 = 3b^2$ which is impossible with $b \in \mathbb{Q}$.

3.2.3 a Let $\mathbb{F}$ be the splitting field over $\mathbb{Q}$. $x^6 + 1 = (x^12 - 1)/(x^6 - 1) = (x^2 + 1)(x^4 + x^2 = 1)$ has roots $\pm i$ and $\pm\exp(\pm i\pi/6) = (\pm\sqrt{3} \pm i)/2$ since these are the 12th roots of 1 which are not 6th roots of 1. Now $i \in \mathbb{F}$ and $\alpha = (\sqrt{3}+i)/2 \in \mathbb{F}$ so $\sqrt{3} = 2\alpha - i \in \mathbb{F}$ and hence $\mathbb{F} = \mathbb{Q}[\sqrt{3}, i]$.

3.2.3 c Let $\mathbb{F}$ be the splitting field over $\mathbb{Q}$. $x^4 - 9 = (x^2 - 3)(x^2 + 3)$ has roots $\pm\sqrt{3}$ and $\pm\sqrt{3}i$. Now $\sqrt{3} \in \mathbb{F}$ and $i = \sqrt{3}i/\sqrt{3} \in \mathbb{F}$ so $\mathbb{F} = \mathbb{Q}[\sqrt{3}, i]$.

3.2.3 e Let $\mathbb{F}$ be the splitting field over $\mathbb{Q}$. $x^6 - 2x^4 + x^2 - 2 = (x^2 - 2)(x^4 + 1)$ has roots $\pm\sqrt{2}$ and $\pm\exp(\pm i\pi/4) = (\pm 1 \pm i)/\sqrt{2}$. Now $\sqrt{2} \in \mathbb{F}$ and $\alpha = (1+i)/\sqrt{2} \in \mathbb{F}$ so $i = \sqrt{2}\alpha - 1 \in \mathbb{F}$ and hence $\mathbb{F} = \mathbb{Q}[\sqrt{2}, i]$.

3.2.5 a We have $\alpha^2 = 1$ so

$.$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	1	$\alpha+1$
$\alpha+1$	0	$\alpha+1$	$\alpha+1$	0

This is not a field since $\alpha + 1$ has no multiplicative inverse.

3.2.5 b We have $\alpha^3 = \alpha + 1$ and $\alpha^4 = \alpha^2 + \alpha$ so

$.$	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	$\alpha+1$

This is a field since every non-zero element has a multiplicative inverse.

3.2.5 d

$.$	0	1	α	$\alpha+1$					
0	0	0	0	0	0	0	0	0	0
1	0	1	-1	α	$\alpha+1$	$\alpha-1$	$-\alpha$	$-\alpha+1$	$-\alpha-1$
-1	0	-1	1	$-\alpha$	$-\alpha-1$	$-\alpha+1$	α	$\alpha-1$	$\alpha+1$
α	0	α	$-\alpha$	-1	$\alpha-1$	$-\alpha-1$	1	$\alpha+1$	$-\alpha+1$
$\alpha+1$	0	$\alpha+1$	$-\alpha-1$	$\alpha-1$	$-\alpha$	1	$-\alpha+1$	-1	α
$\alpha-1$	0	$\alpha-1$	$-\alpha+1$	$-\alpha-1$	1	α	$\alpha+1$	$-\alpha$	-1
$-\alpha$	0	$-\alpha$	α	1	$-\alpha+1$	$\alpha+1$	-1	$-\alpha-1$	$\alpha-1$
$-\alpha+1$	0	$-\alpha+1$	$\alpha-1$	$\alpha+1$	-1	$-\alpha$	$-\alpha-1$	α	1
$-\alpha-1$	0	$-\alpha-1$	$\alpha+1$	$-\alpha+1$	α	-1	$\alpha-1$	1	$-\alpha$

This is not a field since $\alpha + 1$ has no multiplicative inverse.

3.2.6 c Let $g(x) = x^2 - 1$ so that $\beta = g(\alpha)$. Now $f(x) = (x+1)g(x) + x$ and $g(x) = x.x + 1$ so that

$$1 = g(x) - x.x = g(x) - x[f(x) - (x+1)g(x)] = (x^2 + x + 1)g(x) - xf(x).$$

Substituting $x = \alpha$ we see that $\beta^{-1} = \alpha^2 + \alpha + 1$.

3.2.6 d Let $g(x) = x + 1$ so that $\beta = g(\alpha)$. Now $f(x) = (x^2 - x + 1)g(x) - 3$ so that

$$1 = \frac{1}{3}(x^2 - x + 1)g(x) - \frac{1}{3}f(x).$$

Substituting $x = \alpha$ we see that $\beta^{-1} = (\alpha^2 - \alpha + 1)/3$.

3.2.11 Let $S = \{h(x) \in F[x] : h(\alpha) = 0\}$. Now $f(x) \in S$ so if we let $m(x)$ be a monic element of S of least degree then $\deg m > 0$. If $h(x) \in S$ then there exist $q(x), r(x) \in F[x]$ with $r(x) = 0$ or $\deg(r) < \deg(m)$, such that $h(x) = q(x)m(x) + r(x)$. We have $r(\alpha) = h(\alpha) - q(\alpha)m(\alpha) = 0$ so $r(x) \in S$ and hence, by minimality of $\deg(m)$, we have $r(x) = 0$. Thus $m(x)$ divides $h(x)$ for all $h(x) \in S$.