Modern Algebra II: Problem Set 6

Nilay Kumar

Last updated: March 4, 2013

Problem 1

Let $r \in \mathbb{Q}$ and $r = \delta^2$ for some $\delta \in \mathbb{Q}(\sqrt{2})$. We can write $\delta = a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$, and thus, $\delta^2 = a^2 + 2b^2 + 2ab\sqrt{2}$. Since we know $r \in \mathbb{Q}$, it must be that $ab = 0$, i.e. $a = 0$ or $b = 0$. Then, $r = a^2$ or $r = 2b^2$, as desired. Applying this to the case of $r = 3$, we see that $3 = a^2$ or $3 = 2b^2$. Noting that a is rational, i.e. can be written as p/q for p, q relatively prime integers, one can carry out the standard high school argument that there are no such p, q that the two above equations can hold. Let me detail the argument for $3 = a^2$: this means that $3 = p^2/q^2$, which means that p is divisble by 3, which implies that q must also be divisible by 3, which contradicts that p, q are relatively prime. Consequently, no such a exists in $\mathbb{Q}$, and it follows very similarly that no such b exists in $\mathbb{Q}$ either. Such a δ cannot exist, then, and $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Thus, $x^2 - 3$ is irreducible in $\mathbb{Q}(\sqrt{2})[x]$, as it has no roots in $\mathbb{Q}(\sqrt{2})[x]$. In other words, $x^2 - 3 = \mathrm{irr}(\sqrt{3}, \mathbb{Q}(\sqrt{2}), x)$.

Problem 2

Let $\alpha = \sqrt{2} + \sqrt{3}$; α is a root of $x^4 - 10x^2 + 1$:

$$\begin{aligned}
(\sqrt{2} + \sqrt{3})^4 &- 10(\sqrt{2} - \sqrt{3})^2 + 1 \\
&= (5 + 2\sqrt{6})^2 - 10(5 + 2\sqrt{6}) + 1 \\
&= 25 + 24 + 20\sqrt{6} - 50 - 20\sqrt{6} + 1 \\
&= 0
\end{aligned}$$

By the remark that we proved in class, then, $\mathrm{irr}(\alpha, \mathbb{Q}, x)$ divides $x^4 - 10x^2 + 1$. Note also that any subfield S of $\mathbb{R}$ contains a subfield isomorphic to $\mathbb{Q}$. Thus, if S contains $\sqrt{2}$ and $\sqrt{3}$, it contains every number of the form $a + b(\sqrt{2} + \sqrt{3})$, where $a, b \in \mathbb{Q}$, i.e. S contains $\mathbb{Q}(\alpha)$. Additionally,

$$\alpha^2 = (\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6},$$

so $\sqrt{6} \in \mathbb{Q}(\alpha)$. Then, if we multiply,

$$\alpha\sqrt{6} = \sqrt{12} + \sqrt{18} = 2\sqrt{3} + 3\sqrt{2},$$

which is in $\mathbb{Q}(\alpha)$. But note that we can now isolate $\sqrt{2}$ and $\sqrt{3}$ as:

$$\begin{aligned}
\sqrt{2} &= (2\sqrt{3} + 3\sqrt{2}) - 2(\sqrt{2} + \sqrt{3}) \\
\sqrt{3} &= 3(\sqrt{2} + \sqrt{3}) - (2\sqrt{3} + 3\sqrt{2}),
\end{aligned}$$

and thus $\sqrt{2}$ and $\sqrt{3}$ are in $\mathbb{Q}(\alpha)$, and $\mathbb{Q}(\alpha)$ is the smallest field that contains both.

Problem 3

Let $\alpha = \sqrt{3 + 2\sqrt{2}}$; α is a root of $x^4 - 6x^2 + 1$:

$$\begin{aligned}
(3 + 2\sqrt{2})^2 &- 6(3 + 2\sqrt{2}) + 1 \\
&= 17 + 12\sqrt{2} - 18 - 12\sqrt{2} + 1 \\
&= 0.
\end{aligned}$$

This polynomial is, in fact, reducible. Take the product

$$(x^2 + ax + b)(x^2 - ax + b) = x^4 + (2b - a^2)x^2 + b^2.$$

If we choose $b = -1$ and $a = 2$ we obtain our polynomial:

$$x^4 - 6x^2 + 1 = (x^2 + 2x - 1)(x^2 - 2x - 1).$$

Let us try to write the nested radical as $r + s\sqrt{2}$:

$$\begin{aligned}
\sqrt{3 + 2\sqrt{2}} &= r + s\sqrt{2} \\
3 + 2\sqrt{2} &= r^2 + 2s^2 + 2rs\sqrt{2},
\end{aligned}$$

which implies that $3 = r^2 + 2s^2$ and $rs = 1 \iff r = 1/s$. Inserting the second equation into the first yields solutions for $s = \pm 1, \pm 1/\sqrt{2}$. Of course, the second pair are not rational, so we neglect them. The first pair yields $\sqrt{3 + 2\sqrt{2}} = 1 + \sqrt{2}$. Thus, we see that our quartic polynomial has no root in $\mathbb{Q}$, though it is reducible. Instead, there is a solution in $\mathbb{Q}(\sqrt{2})$.

Problem 4

Working in the ring $\mathbb{F}_2[x]$, it is clear that the only linear polynomials are x and $x+1$. Since these are linear, they are irreducible. Recall from class that any linear or cubic polynomials over a field are irreducible if and only if they have no roots. Note that any polynomial without a constant term is reducible, as an x can always be factored out. In addition, any polynomial with a constant term and an even number of terms will have 1 as a root, and will thus be reducible. This leaves us with only x^2+x+1 as an irreducible quadratic and x^3+x+1 and x^3+x^2+1 as irreducible cubics. Now, let us check if $x^4+x^3+x^2+x+1$ is irreducible in $\mathbb{F}_2[x]$. First note that it has no roots, as $x = 0, 1$ both yield 1. Thus, this polynomial cannot have a linear factor, and thus we only check whether our quadratic irreducible squares to it:

$$(x^2+x+1)^2 = x^4 + (x+1)^2 = x^4 + x^2 + 1,$$

and our polynomial must be irreducible.

Problem 5

Let F be a field and let $f(x) \in F[x]$ and $g(x) \in F[x]$ be relatively prime. We define a homormorphism $\rho : F[x] \to (F[x]/(f(x))) \times (F[x]/(g(x)))$ by

$$\rho(h(x)) = (h(x) + (f(x)), h(x) + (g(x))).$$

(i) $\rho(h(x)) = 0$ if and only if $h(x) + (f(x)) = 0$ and $h(x) + (g(x)) = 0$, i.e. $h(x) \equiv 0 \mod f(x)$ and $h(x) \equiv 0 \mod g(x)$. Of course, this is true if and only if $f(x)$ and $g(x)$ and both divide $h(x)$. But since f, g are relatively prime, by what we showed in class, this is true if and only if $f(x)g(x)$ divides $h(x)$. Consequently, $h(x) \in (f(x)g(x))$.

(ii) By definition of relatively prime, there must exist $rs \in F[x]$ such $1 = rf + sg$. We can use this to show that ρ is surjective. If we take any $a(x), b(x) \in F[x]$ and set $h(x) = r(x)b(x)f(x) + s(x)a(x)g(x)$, we have

$$\begin{aligned} r(x)f(x) &= 1 - s(x)g(x) \\ s(x)g(x) &= 1 - r(x)f(x), \end{aligned}$$

which allows us to simplify

$$\begin{aligned}\rho(h(x)) =& (r(x)b(x)f(x) + s(x)a(x)g(x) + (f(x)),\\ & r(x)b(x)f(x) + s(x)a(x)g(x) + (g(x)))\\ =& (a(x) - r(x)a(x)f(x) + r(x)b(x)f(x) + (f(x)),\\ & b(x) - s(x)b(x)g(x) + s(x)a(x)g(x) + (g(x)))\\ =& (a(x) + (f(x)), b(x) + (g(x))),\end{aligned}$$

and hence ρ is surjective.

In particular, if $a, b \in F$ and $a \neq b$, then $x-a$ and $x-b$ are relatively prime, we have

$$\frac{F[x]}{((x-a)(x-b))} \cong \frac{F[x]}{(x-a)} \times \frac{F[x]}{(x-b)} \cong F \times F.$$

where we have used the fact that elements of $F[x]/(x-a)$ and $F[x]/(x-b)$ can uniquely be written as constants (as we know from long division), and are thus each isomorphic to F.

Problem 6

Let $E = \mathbb{F}_2(\alpha)$ where α is the root of $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$. Thus $f(x)$ must factor into a product of linear polynomials $f(x) = (x+\alpha)(x+\beta)$, i.e.

$$x^2 + x + 1 = x^2 + (\alpha + \beta)x + \alpha\beta.$$

The only β that satisfies $\alpha + \beta = 1$ and $\alpha\beta = 1$ in E is $\alpha + 1$, as $\alpha(\alpha+1) = \alpha + \alpha^2 = -1 = 1$:

$$x^2 + x + 1 = (x + \alpha)(x + \alpha + 1)$$

α cannot be a repeated root, because $(x+\alpha)^2 = x^2 + \alpha^2$, which is not, in general, equal to $x^2 + x + 1$.

Problem 7

Let $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$. Note that f has no roots, as $f(0) = 1, f(1) = f(2) = 2$. Consequently, since f is degree 2, it is irreducible in $\mathbb{F}_3[x]$. Then, $E = \mathbb{F}_3(\alpha) = \mathbb{F}_3[x]/(f(x))$ is a field (where $\alpha = x + (f(x))$). Since $f(\alpha) = 0$, we can find a linear factor (other than $x - \alpha$) of $x^2 + 1$ by long division, to be $x + \alpha$ with remainder $1 + \alpha^2 = 0$:

$$(x+\alpha)(x-\alpha) = x^2 - \alpha^2 = x^2 + 1,$$

using the fact that $\alpha^2+1=0$. Note that every element of E can be written uniquely as $a_0+a_1\alpha$ where $a_0, a_1 \in \mathbb{F}_3$, so E has $3\times 3 = 9$ elements. Indeed, as a group, $(E,+)$ is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, as one can add elements of E "componentwise", and that addition is simply the addition of $\mathbb{Z}/3\mathbb{Z}$ (more rigorously, $f(a_0+a_1\alpha) = (a_0, a_1)$ is an isomorphism). Since E is a field, every element but zero is a unit, i.e. $(E^*, \cdot)$ has 8 elements. Note that $\varphi(8) = 4$, and so we expect E^* to have 4 generators. It should be clear that 1 and 2 cannot be generators ($2^2 = 1$), as well as $\alpha, 2\alpha$ ($\alpha^4 = 1$). This leaves $1+\alpha, 2+\alpha, 1+2\alpha, 2+2\alpha$. Let us check these:

$$\begin{array}{cc}
(1+\alpha)^2 = 2\alpha & (1+2\alpha)^2 = \alpha \\
(1+\alpha)^3 = 1+2\alpha & (1+2\alpha)^3 = \alpha-2 \\
(1+\alpha)^4 = 2 & (1+2\alpha)^4 = 2 \\
(1+\alpha)^5 = 2+2\alpha & (1+2\alpha)^5 = \alpha+2 \\
(1+\alpha)^6 = \alpha & (1+2\alpha)^6 = 2\alpha \\
(1+\alpha)^7 = \alpha+2 & (1+2\alpha)^7 = 2+2\alpha \\
(1+\alpha)^8 = 1 & (1+2\alpha)^8 = 1,
\end{array}$$

and the others follow just as powers of negatives of these elements. Consequently, there are four generators.