Kris Harper
MATH 25900
Homework 2 April 16, 2010

Problem 1 (13.1.3). *Show that $x^3 + x + 1$ is irreducible over $\mathbb{F}_2$ and let θ be a root. Compute the powers of θ in $\mathbb{F}_2(\theta)$.*

Proof. Note that $0 + 0 + 1 = 1 = 1 + 1 + 1$ so neither 0 or 1 is a root of $x^3 + x + 1$. Thus this polynomial is irreducible. We know that $\mathbb{F}_2(\theta) \cong \mathbb{F}_2[x]/(x^3 + x + 1)$. Thus we have

$$\theta^3 = -\theta - 1 = \theta + 1.$$

Then

$$\begin{aligned}\theta^4 &= \theta^2 + \theta,\\ \theta^5 &= \theta^3 + \theta^2 = \theta^2 + \theta + 1,\\ \theta^6 &= \theta^3 + \theta^2 + \theta = \theta^2 + 1\\ \theta^7 &= \theta^3 + \theta = 1.\end{aligned}$$

Taken together with 0, 1, θ and θ^2 we see that these powers of θ form all 8 elements of $\mathbb{F}_2(\theta)$. Moreover, $(\mathbb{F}_2(\theta))^\times = \langle\theta\rangle$. □

Problem 2 (13.1.5). *Suppose α is a rational root of a monic polynomial in $\mathbb{Z}[x]$. Prove that α is an integer.*

Proof. Let $\alpha = a/b$ and take $(a, b) = 1$ with $b > 0$. There exists a polynomial $p(x) \in \mathbb{Z}[x]$ such that $p(a/b) = (a/b)^m + c_1(a/b)^{m-1} + \cdots + c_m = 0$. Multiply this equation by b^m so we have $a^m + c_1 ba^{m-1} + \cdots + b^m c = 0$. Since b divides each term following a^m and it divides the right hand side we see that $b \mid a^m$. Since $(a, b) = 1$ we must have $b = 1$ so that $a/b \in \mathbb{Z}$. □

Problem 3 (13.1.8). *Prove that $x^5 - ax - 1 \in \mathbb{Z}[x]$ is irreducible unless $a = 0$, 2 or -1. The first two correspond to linear factors, the third corresponds to the factorization $(x^2 - x + 1)(x^3 + x^2 - 1)$.*

Proof. From the rational root theorem we know that roots of this polynomial which lie in $\mathbb{Q}$ can only be ± 1. Putting these in gives $-a = 0$ and $-2 + a = 0$ so if $a = 0$ or $a = 2$ then we have a linear factorization. If $a = -1$ then we have the above factorization so these three cases do indeed imply $x^5 - ax - 1$ is reducible. By the rational root theorem we've exhausted all the possibilities of $x^5 - ax - 1$ having a linear factor. Thus it can only factor into two polynomials of degree 2 and 3.

Suppose $x^5 - ax - 1 = (x^2 + bx + c)(x^3 + dx^2 + ex + f)$. Multiplying this out gives us the equations $b + d = 0$, $c + bd + e = 0$, $cd + be + f = 0$, $ce + bf = -a$ and $cf = -1$. Thus $b = -d$ and $c = \pm 1$. If $c = 1$ then $f = -1$ and we have $1 - b^2 + e = 0$, $-b + be - 1 = 0$ and $e - b = -a$. The second of these equations gives us $b(e - 1) = 1$ so $e = 0$ or $e = 2$. If $e = 2$ then $b = 1$ and the first equation gives $0 = 1 - 1 + 2 = 2$. If $e = 0$ then $b = -1$ and by the third equation $a = -1$ as we had earlier.

Now we consider $c = -1$. Then $f = 1$ and we now have $-1 - b^2 + e = 0$, $b + be + 1 = 0$ and $b - e = -a$. Thus $b(e + 1) = -1$ so $b = \pm 1$. By the first equation $0 = -1 - 1 + e$ so $e = 2$. But then by the second equation again we have $b = -1/3$ which is not an integer. So $c \neq -1$ and we see that $x^5 - ax - 1$ can only be factored into a quadratic and a cubic if $a = -1$. □

Problem 4 (13.2.3). *Determine the minimal polynomial over $\mathbb{Q}$ for $1 + i$.*

Proof. Note that $(1 + i)^2 - 2(1 + i) + 2 = 2i - 2 - 2i + 2 = 0$ so $1 + i$ is a root of $x^2 - 2x + 2$. But this polynomial is irreducible over $\mathbb{Q}$ using Eisenstein. Thus it must be the minimal polynomial for $1 + i$. □

Problem 5 (13.2.4). *Determine the degree over $\mathbb{Q}$ of $2 + \sqrt{3}$ and of $1 + \sqrt[3]{2} + \sqrt[3]{4}$.*

Proof. Note that $(2+\sqrt{3})^2 - 4(2+\sqrt{3}) + 1 = 0$ so $2+\sqrt{3}$ is a root for $x^2 - 4x + 1$. Moreover this polynomial is irreducible over $\mathbb{Q}$ by the rational root theorem so this must be the minimal polynomial for $2+\sqrt{3}$. Therefore $\deg(2 + \sqrt{3}) = 2$.

Note that $(1 + \sqrt[3]{2} + \sqrt[3]{4})^3 - 3(1 + \sqrt[3]{2} + \sqrt[3]{4})^2 - 3(1 + \sqrt[3]{2} + \sqrt[3]{4}) - 1 = 0$ so $1 + \sqrt[3]{2} + \sqrt[3]{4}$ is a root of $x^3 - 3x^2 - 3x - 1$. Furthermore by the rational root theorem this is irreducible in $\mathbb{Q}$ so this must be the minimal polynomial. Thus $\deg(1 + \sqrt[3]{2} + \sqrt[3]{4}) = 3$. □

Kris Harper
MATH 25900
Homework 2 April 16, 2010

Problem 6 (13.2.5)**.** *Let $F = \mathbb{Q}(i)$. Prove that $x^3 - 2$ and $x^3 - 3$ are irreducible over F.*

Proof. There are no rational roots to either of these polynomials by the rational root theorem. Suppose we have a root of the form $a + ib$ where $a, b \in \mathbb{Q}$. Then $(a+ib)^3 - 2 = (a^3 - 3ab^2 - 2) + i(3a^2b - b^3) = 0$. This gives the two equations $a^3 - 3ab^2 - 2 = 0$ and $3a^2b - b^3 = 0$. Clearly $a \neq 0$ otherwise we get $-2 = 0$. If $b = 0$ then $a^3 - 2 = 0$ which we know has no solutions in $\mathbb{Q}$. The rational root theorem tells us that solutions to $a^3 - 3ab^2 - 2 = 0$ are either $a = \pm 2$ or $a = \pm 1/2$. If $a = 2$ then $b^2 = 1$ so $b = \pm 1$. In either case the second equation tells us that $a^2 = 1/3$ which has no solutions in $\mathbb{Q}$. Thus $a \neq 2$. If $a = -2$ then $b^2 = 5/3$ which has no solutions in $\mathbb{Q}$. If $a = 1/2$ then $b^2 = -5/4$ which has no solutions in $\mathbb{Q}$. If $a = -1/2$ then $b^2 = 17/12$ which has no solutions in $\mathbb{Q}$. All possibilities have been exhausted so there are no possible roots to $x^3 - 2$ of the form $a + ib$.

For the second polynomial we have similar equations $a^3 - 3ab^2 - 3 = 0$ and $3a^2b - b^3 = 0$. Now $a = \pm 3$ or $\pm 1/3$. If $a = 3$ then $b^2 = 8/3$. If $a = -3$ then $b^2 = 10/3$. If $a = 1/3$ then $b^2 = -80/27$ and if $a = -1/3$ then $b^2 = 82/27$. None of these have solutions in $\mathbb{Q}$ so there are no roots to $x^3 - 3$ of the form $a + ib$. Since each of these is cubic we see that they must be irreducible over F. $\square$

Problem 7 (13.2.7)**.** *Prove that $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Conclude that $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$. Find an irreducible polynomial satisfied by $\sqrt{2} + \sqrt{3}$.*

Proof. The field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ clearly contains $\mathbb{Q}$ and the element $\sqrt{2} + \sqrt{3}$ so we must have containment $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Now note that

$$\frac{\left(\sqrt{2} + \sqrt{3}\right)^3 - 9\left(\sqrt{2} + \sqrt{3}\right)}{2} = \sqrt{2}$$

and

$$\frac{\left(\sqrt{2} + \sqrt{3}\right)^3 - 11\left(\sqrt{2} + \sqrt{3}\right)}{-2} = \sqrt{3}.$$

Thus $\sqrt{2}$ and $\sqrt{3}$ are both contained in $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ so we must have the second inclusion as well. Since $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ we must also have $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$. Note that $(\sqrt{2} + \sqrt{3})^4 - 10(\sqrt{2} + \sqrt{3})^2 + 1 = 0$ so $\sqrt{2} + \sqrt{3}$ satisfies $x^4 - 10x + 1$. The rational root theorem tells us that this is irreducible. $\square$

Problem 8 (13.2.10)**.** *Determine the degree of the extension $\mathbb{Q}(\sqrt{3 + 2\sqrt{2}})$ over $\mathbb{Q}$.*

Proof. If we write $3 + 2\sqrt{2} = 1 + 2\sqrt{2} + 2 = (1 + \sqrt{2})^2$ we see that $\sqrt{3 + 2\sqrt{2}} = 1 + \sqrt{2}$. Using this it's easy to see that $(1 + \sqrt{2})^2 - 2(1 + \sqrt{2}) - 1 = 0$ so $\sqrt{3 + 2\sqrt{2}}$ is a root for $x^2 - 2x - 1$. By the rational root theorem we know this is irreducible and thus $[\mathbb{Q}(\sqrt{3 - 2\sqrt{2}}) : \mathbb{Q}] = 2$. $\square$

Problem 9 (13.2.11)**.** *(a) Let $\sqrt{3 + 4i}$ denote the square root of the complex number $3 + 4i$ that lies in the first quadrant and let $\sqrt{3 - 4i}$ denote the square root of $3 - 4i$ that lies in the fourth quadrant. Prove that $[\mathbb{Q}(\sqrt{3 + 4i} + \sqrt{3 - 4i}) : \mathbb{Q}] = 1$.*
(b) Determine the degree of the extension $\mathbb{Q}(\sqrt{1 + \sqrt{-3}} + \sqrt{1 - \sqrt{-3}})$ over $\mathbb{Q}$.

Proof. (a) Write $3 + 4i = 4 + 4i - 1 = (2 + i)^2$ so that $\sqrt{3 + 4i} = 2 + i$. Likewise $\sqrt{3 - 4i} = 2 - i$. Summing these we get 4 so $\sqrt{3 + 4i} + \sqrt{3 - 4i} - 4 = 0$ and this is a root of $x - 4$. Thus $[\mathbb{Q}(\sqrt{3 + 4i} + \sqrt{3 - 4i}) : \mathbb{Q}] = 1$.

(b) We see that

$$\left(\sqrt{1 + \sqrt{-3}} + \sqrt{1 - \sqrt{-3}}\right)^4 - 4\left(\sqrt{1 + \sqrt{-3}} + \sqrt{1 - \sqrt{-3}}\right)^2 - 36 = 0$$

so that $\sqrt{1 + \sqrt{-3}} + \sqrt{1 - \sqrt{-3}}$ is a root of $x^4 - 4x^2 - 36$. Eisenstein will tell us that this is irreducible over $\mathbb{Q}$ so $[\mathbb{Q}(\sqrt{1 + \sqrt{-3}} + \sqrt{1 - \sqrt{-3}}) : \mathbb{Q}] = 4$. $\square$

Kris Harper
MATH 25900
Homework 2 April 16, 2010

Problem 10 (13.2.13). *Suppose $F = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where $\alpha_i^2 \in \mathbb{Q}$ for $i = 1, 2, \ldots, n$. Prove that $\sqrt[3]{2} \notin F$.*

Proof. Since $\alpha_i^2 \in \mathbb{Q}$ for $i = 1, 2, \ldots, n$ we see that $\deg \alpha_i \leq 2$. Furthermore, since degree extensions are multiplicative we have that $[F : \mathbb{Q}] = 2^k$ for some $k \leq n$. But $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ and $3 \nmid 2^k$ so $\sqrt[3]{2} \notin F$. $\square$

Problem 11 (13.2.21). *Let $K = \mathbb{Q}(\sqrt{D})$ for some squarefree integer D. Let $\alpha = a + b\sqrt{D}$ be an element of K use the basis $1, \sqrt{D}$ for K as a vector space over $\mathbb{Q}$ and show that the matrix of the linear transformation "multiplication by α" on K considered in the previous exercises has the matrix $\begin{pmatrix} a & bD \\ b & a \end{pmatrix}$. Prove directly that the map $a + b\sqrt{D} \mapsto \begin{pmatrix} a & bD \\ b & a \end{pmatrix}$ is an isomorphism of the field K with a subfield of the ring of 2×2 matrices with coefficients in $\mathbb{Q}$.*

Proof. Let $\beta = c + d\sqrt{D} \in K$. Then $\alpha\beta = (ac + bdD) + (ad + bc)\sqrt{D}$. But also

$$\begin{pmatrix} a & bD \\ b & a \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac + bdD \\ bc + ad \end{pmatrix}$$

so this matrix is precisely the transformation "multiplication by α". Now note that

$$\alpha\beta = (ac + bdD) + (ad + bc)\sqrt{D} \mapsto \begin{pmatrix} ac + bdD & (ad + bc)D \\ ad + bc & ac + bdD \end{pmatrix} = \begin{pmatrix} a & bD \\ b & a \end{pmatrix} \begin{pmatrix} c & dD \\ d & c \end{pmatrix}$$

so this is a homomorphism. It's clearly injective because K is a field and this is not the 0 map (1 is sent to the identity matrix). Thus K is isomorphic to its image under this map and so it's image is a subfield of 2×2 matrices with coefficients in $\mathbb{Q}$. $\square$