MATH 7211 Homework 1

Andrea Bourque

May 9, 2023

1 Problem 13.1.2

Show that $x^3 - 2x - 2$ is irreducible over $\mathbb{Q}$ and let θ be a root. Compute $(1+\theta)(1+\theta+\theta^2)$ and $\dfrac{1+\theta}{1+\theta+\theta^2}$ in $\mathbb{Q}(\theta)$.

Proof. The irreducibility of $x^3 - 2x - 2$ can be checked by either Eisenstein's criterion or the rational root theorem. For Eisenstein's criterion, we apply it for the prime 2. We see that 2 divides the non-leading coefficients $0, -2, -2$, and $2^2 = 4$ does not divide the constant coefficient -2. To apply rational root theorem for irreducibility, we note that a cubic can only be non-trivially factored into a product of a linear term and a quadratic term. The presence of a linear term means that the polynomial, if reducible, must have a root in $\mathbb{Q}$. The rational root theorem says that the only possible rational roots of $p(x) = x^3 - 2x - 2$ are $1, 2, -1, -2$, and we can check in each of these cases that these are not roots: $p(1) = -3, p(2) = 2, p(-1) = -1, p(-2) = -6$.

Note that $\theta^3 = 2\theta + 2$. Now

$$(1+\theta)(1+\theta+\theta^2) = 1 + 2\theta + 2\theta^2 + \theta^3 = 3 + 4\theta + 2\theta^2.$$

To compute the next expression, we find the inverse of $1+\theta+\theta^2$, say $a+b\theta+c\theta^2 \in \mathbb{Q}(\theta)$. We have

$$\begin{aligned} (1+\theta+\theta^2)(a+b\theta+c\theta^2) &= 1; \\ a + 2b + 2c + (a+3b+4c)\theta + (a+b+3c)\theta^2 &= 1. \end{aligned}$$

Therefore

$$\begin{aligned} \begin{pmatrix} 1 & 2 & 2 \\ 1 & 3 & 4 \\ 1 & 1 & 3 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} &= \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}; \\ \begin{pmatrix} a \\ b \\ c \end{pmatrix} &= \begin{pmatrix} 5/3 \\ 1/3 \\ -2/3 \end{pmatrix}. \end{aligned}$$

Thus

$$\frac{1+\theta}{1+\theta+\theta^2} = (1+\theta)\left(\frac{5}{3}+\frac{1}{3}\theta-\frac{2}{3}\theta^2\right) = \frac{1}{3}+\frac{2}{3}\theta-\frac{1}{3}\theta^2.$$

□

2 Problem 13.1.4

Prove directly that the map $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ is an isomorphism of $\mathbb{Q}(\sqrt{2})$ with itself.

Proof. First we show the map is a homomorphism.

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \mapsto (a + c) - (b + d)\sqrt{2},$$
$$(a + c) - (b + d)\sqrt{2} = (a - b\sqrt{2}) + (c - d\sqrt{2}).$$
$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \mapsto (ac + 2bd) - (ad + bc)\sqrt{2},$$
$$(ac + 2bd) - (ad + bc)\sqrt{2} = (a - b\sqrt{2})(c - d\sqrt{2}).$$

The map is surjective since for any element $a+b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, we have $a-b\sqrt{2} \mapsto a + b\sqrt{2}$. Finally, the map is injective, since if $a + b\sqrt{2} \mapsto a - b\sqrt{2} = 0$, then $a = 0$ and $b = 0$, so $a + b\sqrt{2} = 0$. □

3 Problem 13.1.5

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

Proof. By the rational root theorem, any rational root of a polynomial in $\mathbb{Z}[x]$ has a denominator which divides the leading coefficient. For a monic polynomial, the leading coefficient is 1, and the only divisors of 1 are 1 and -1. Thus a rational root of a monic polynomial in $\mathbb{Z}[x]$ has a denominator of ± 1, meaning it is an integer. $\square$

4 Problem 13.1.6

Show that if α is a root of $a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$, then $a_n\alpha$ is a root of the monic polynomial $x^n + a_{n-1}x^{n-1} + a_n a_{n-2}x^{n-2} + ... + a_n^{n-2}a_1 x + a_n^{n-1}a_0$.

Proof.

$$\begin{aligned}(a_n\alpha)^n &+ a_{n-1}(a_n\alpha)^{n-1} + a_n a_{n-2}(a_n\alpha)^{n-2} + ... + a_n^{n-2}a_1(a_n\alpha) + a_n^{n-1}a_0 \\ &= a_n^{n-1}\left(a_n\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0\right) = a_n^{n-1}\cdot 0 = 0.\end{aligned}$$

□

5 Problem 13.1.8

Prove that $x^5 - ax - 1 \in \mathbb{Z}[x]$ is irreducible unless $a = 0, 2, -1$.

Proof. First suppose that $x^5 - ax - 1$ has a linear factor over $\mathbb{Z}[x]$, i.e. there is an integer root. The rational root theorem says that the only possible integer roots of $x^5 - ax - 1$ are 1 and -1. If 1 is a root, then $1 - a - 1 = -a = 0$, so $a = 0$. If -1 is a root, then $-1 + a - 1 = a - 2 = 0$, so $a = 2$.

Now suppose there are no linear factors. The only possible decomposition is into a product of quadratic and cubic factors. Thus suppose

$$x^5 - ax - 1 = (x^2 + bx \pm 1)(x^3 + cx^2 + dx \mp 1)$$

for $b, c, d \in \mathbb{Z}$. Note the constant terms are $\pm 1, \mp 1$, since the only possible factorization of -1 over $\mathbb{Z}$ is $-1 \cdot 1$. After expanding the right hand side, the coefficient of x^4 is $b + c$. Since this coefficient must vanish, we have $c = -b$. Expanding the rest of the right hand side in terms of b, d gives

$$x^5 + (d - b^2 \pm 1)x^3 + (\mp 1 + bd \mp b)x^2 + (\mp b \pm d)x - 1.$$

The coefficient of x^3 must vanish, so $d = b^2 \mp 1$. The coefficient of x^2 also vanishes, so $\mp 1 + bd \mp b = b^3 \mp 2b \mp 1 = 0$. Since $b \in \mathbb{Z}$, the rational root theorem implies b is either 1 or -1. Checking these cases shows that the only possibility is that $b^3 - 2b - 1 = 0$ and $b = -1$. Thus $d = 0$ and $a = b - d = -1$.

Since the reducibility of $x^5 - ax - 1$ implies $a = 0, 2, -1$, we have that $x^5 - ax - 1$ is irreducible for $a \neq 0, 2, -1$. $\square$