# Homework 1

Kevin Guillen

MATH 202 — Algebra III — Spring 2022

**Problem 13.1.1** Show that $p(x) = x^3 + 9x + 6$ is irreducible in $\mathbb{Q}[x]$. Let $\theta$ be a root of $p(x)$. Find the inverse of $1 + \theta$ in $\mathbb{Q}(\theta)$

*Proof.* First to show that $p(x)$ is indeed irreducible we will use Eisenstein's Irreducibility Criterion, which we learned in Math 200, to show it is irreducible over $\mathbb{Z}[x]$ and by the Gauss Lemma irreducible over $\mathbb{Q}[x]$. We can see that with $p = 3$ we have that 3 divides 6 and 9, 3 doesn't divide 1, and finally that $3^2$ doesn't divide 6. Meaning then that $p(x)$ is irreducible.

Now if $\theta$ is a root of $p(x)$ to find the inverse of $1 + \theta$ we will first perform division with remainder on $p(x)$ by $(1 + x)$.

$$
\begin{array}{rrrrr}
 & & x^2 & -x & +10 \\ \cline{2-5}
x+1\big) & x^3 & & +9x & +6 \\
 & -x^3 & -x^2 & & \\ \cline{2-3}
 & & -x^2 & +9x & \\
 & & x^2 & +x & \\ \cline{3-4}
 & & & 10x & +6 \\
 & & & -10x & -10 \\ \cline{4-5}
 & & & & -4
\end{array}
$$

To get that $p(x) = (x + 1)(x^2 - x + 10) - 4$. We were given that $\theta$ is a root of $p(x)$, so it must be that case then that,

$$(1 + \theta)(\theta^2 - \theta + 10) = 4$$

implying,

$$(1 + \theta)^{-1} = \frac{(\theta^2 - \theta + 10)}{4}$$

as desired.

$\square$

**Problem 13.1.2** Show that $x^3 - 2x - 2$ is irreducible over $\mathbb{Q}$ and let $\theta$ be a root. Compute $(1+\theta)(1+\theta+\theta^2)$ and $\dfrac{1+\theta}{1+\theta+\theta^2}$ in $\mathbb{Q}(\theta)$.

*Proof.* Like the previous problem we will use Eisenstein's Irreducibility Criterion again and apply the Gauss Lemma, but in this case $p = 2$. We see that 2 divides $-2$, 2 doesn't divide 1, and that $2^2$ doesn't divide $-2$. Therefore $x^3 - 2x - 2$ is irreducible.

Computing $(1+\theta)(1+\theta+\theta^2)$ we get,

$$\theta^3 + 2\theta^2 + 2\theta + 1 \tag{1}$$

Recall though $\theta$ being a root of $x^3 - 2x - 2$ means $\theta^3 - 2\theta - 2 = 0$ and therefore,

$$\theta^3 = 2\theta + 2$$

so plugging back into (1) we get,

$$2\theta^2 + 4\theta + 3$$

Now we compute $\dfrac{1+\theta}{1+\theta+\theta^2}$, so first we need to obtain $(1+\theta+\theta^2)^{-1}$ which we do by performing division with remainder on $(x^3 - 2x - 2)$ by $(x^2 + x + 1)$,

$$\begin{array}{r|r}
 & x - 1 \\ \hline
x^2 + x + 1 & x^3 \qquad - 2x - 2 \\
 & -x^3 - x^2 \;\; - x \qquad \\ \cline{2-2}
 & -x^2 - 3x - 2 \\
 & x^2 \;\; + x + 1 \\ \cline{2-2}
 & -2x - 1
\end{array}$$

continuing we get,

$$\begin{array}{r|r}
 & -\frac{1}{2}x - \frac{1}{4} \\ \hline
-2x - 1 & x^2 \;\; + x + 1 \\
 & -x^2 - \frac{1}{2}x \qquad \\ \cline{2-2}
 & \frac{1}{2}x + 1 \\
 & -\frac{1}{2}x - \frac{1}{4} \\ \cline{2-2}
 & \frac{3}{4}
\end{array}$$

Giving us,

$$\begin{aligned}
x^3 - 2x - 2 &= (x^2 + x + 1)(x - 1) + (-2x - 1) \\
x^2 + x + 1 &= (-2x - 1)(\frac{1}{2}x - \frac{1}{4}) + \frac{3}{4}
\end{aligned}$$

Solving for the remainder in both these equations we get,

$$(-2x - 1) = (x^3 - 2x - 2) - (x^2 + x + 1)(x - 1) \tag{2}$$

$$\frac{3}{4} = (x^2 + x + 1) - (-2x - 1)(\frac{1}{2}x - \frac{1}{4}) \tag{3}$$

Now we multiply equation (3) by $\frac{4}{3}$ and plug in equation (2) into it to get,

$$1 = \frac{4}{3}(x^2+x+1) - \frac{4}{3}((x^3-2x-2)-(x^2+x+1)(x-1))(\frac{1}{2}x-\frac{1}{4})$$

which works out to be,

$$1 = (-\frac{2}{3}x^2+\frac{1}{3}x+\frac{5}{3})(x^2+x+1)+(\frac{2}{3}x+\frac{1}{3})(x^3-2x-2)$$

Meaning if we evaluate the equation at $\theta$ we get that,

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

therefore $(\theta^2+\theta+1)^{-1} = (-\frac{2}{3}\theta^2+\frac{1}{3}\theta+\frac{5}{3})$. Now we can compute,

$$\begin{aligned}
\frac{1+\theta}{1+\theta+\theta^2} &= (1+\theta)(-\frac{2}{3}\theta^2+\frac{1}{3}\theta+\frac{5}{3}) \\
&= -\frac{2}{3}\theta^2+\frac{1}{3}\theta+\frac{5}{3}-\frac{2}{3}\theta^3+\frac{1}{3}\theta^2+\frac{5}{3}\theta \\
&= -\frac{2}{3}\theta^3-\frac{1}{3}\theta^2+\frac{6}{3}\theta+\frac{5}{3} \\
&= -\frac{4}{3}\theta-\frac{4}{3}-\frac{1}{3}\theta^2+\frac{6}{3}\theta+\frac{5}{3} \\
&= -\frac{1}{3}\theta^2+\frac{2}{3}\theta+\frac{1}{3}
\end{aligned}$$

as desired.

□

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

*Proof.* We see the given polynomial is of degree 3, therefore it will have to have a linear factor in order to be reducible. So it is enough to show that it has no roots, and because we are in $\mathbb{F}_2$ the only roots it could possibly have are 0 and 1. We see though,

$$\begin{aligned}
1^3+1+1 &= 1 \\
0+0+1 &= 1
\end{aligned}$$

therefore $x^3+x+1$ is irreducible over $\mathbb{F}_2$. Now obtaining the powers of $\theta$ we get,

$$\begin{aligned}
\theta^0 &= 1 \\
\theta^1 &= \theta \\
\theta^2 &= \theta^2
\end{aligned}$$

we pause here to note that since $\theta$ is a root of the given polynomial we have,

$$\theta^3 + \theta + 1 = 0 \Rightarrow \theta^3 = \theta + 1$$

continuing,

$$\begin{aligned}
&\theta^4 = \theta^3\theta = (\theta+1)\theta = \theta^2 + \theta \\
&\theta^5 = (\theta^2+\theta)\theta = \theta^3 + \theta^2 = \theta^2 + \theta + 1 \\
&\theta^6 = (\theta^2+\theta+1)\theta = \theta^3 + \theta^2 + \theta = \theta + 1 + \theta^2 + \theta = \theta^2 + 1 \\
&\theta^7 = (\theta^2+1)\theta = \theta^3 + \theta = \theta + 1 + \theta = 1 && \text{cycles back}
\end{aligned}$$

Therefore $\theta^i$ is unique for $0 \leqslant i \leqslant 6$, giving us all the powers of $\theta$, as desired. □

**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.* Let us denote the given map as $\pi$. The first thing we must do is show that $\pi$ is a homomorphism. First we see the additive property,

$$\begin{aligned}
\pi(a + b\sqrt{2} + c + d\sqrt{2}) &= \pi((a+c) + (b+d)\sqrt{2}) \\
&= a + c - b\sqrt{2} - d\sqrt{2} \\
&= a - b\sqrt{2} + c - d\sqrt{2} \\
&= \pi(a + b\sqrt{2}) + \pi(c + d\sqrt{2})
\end{aligned}$$

now the multiplicative property,

$$\begin{aligned}
\pi((a + b\sqrt{2}) \cdot (c + d\sqrt{2})) &= \pi(ac + 2bd + (ad + bc)\sqrt{2}) \\
&= ac + 2bd - ad\sqrt{2} - bc\sqrt{2} \\
&= (a - b\sqrt{2})(c - d\sqrt{2}) \\
&= \pi(a + b\sqrt{2}) \cdot \pi(c + d\sqrt{2})
\end{aligned}$$

meaning $\pi$ is a homomorphism.

Now we must show that $\pi$ is injective,

$$\pi(a + b\sqrt{2}) = \pi(c + d\sqrt{2}) \Rightarrow a - b\sqrt{2} = c - d\sqrt{2}$$

and because $\sqrt{2}$ is irrational so therefore not in the field of rational numbers, we have that

$$a = b \text{ and } c = d$$

therefore $\pi$ is injective. Now we show that it is surjective, consider any $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, we have then that,

$$\pi(a + (-b)\sqrt{2}) = a + b\sqrt{2}$$

therefore $\pi$ is surjective. All this together means that $\pi$ is an isomorphism of $\mathbb{Q}(\sqrt{2})$ with itself. □

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

*Proof.* We will do a proof by contradiction and let's assume $\alpha = \frac{c}{d}$ where $c$ and $d$ are relatively prime, and $d \neq \pm 1$. We are given that $\alpha$ is a root of some monic polynomial $p(x) \in \mathbb{Z}[x]$ so,

$$\begin{aligned}
0 &= \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 \\
0 &= \left(\frac{c}{d}\right)^n + a_{n-1}\left(\frac{c}{d}\right)^{n-1} + \cdots + a_1\left(\frac{c}{d}\right) + \alpha_0 \\
-\frac{c^n}{d^n} &= a_{n-1}\frac{c^{n-1}}{d^{n-1}} + \cdots + a_1\frac{c}{d} + a_0 \\
-c^n &= d^n(a_{n-1}\frac{c^{n-1}}{d^{n-1}} + \cdots + a_1\frac{c}{d} + a_0) \\
-c^n &= d(a_{n-1}c^{n-1} + \cdots + a_1 c d^{n-2} + a_0 d^{n-1})
\end{aligned}$$

Meaning that any prime that divides $d$ must also divide $c^n$ and therefore divide $c$, but recall $c$ and $d$ were relatively prime, so there can't be a prime dividing $d$, but that means $d = \pm 1$ which is a contradiction. Therefore $\alpha$ must be an integer. $\square$

**Problem 13.2.3** Determine the minimal polynomial over $\mathbb{Q}$ for the element $1 + i$

*Proof.* It is clear that the minimal polynomial of the given element has to be at least degree 2 since $1 + i$ is not in the field of rational numbers. We see through conjugation that,

$$\begin{aligned}
(x - (1+i))(x - (1-i)) &= (x - 1 - i)(x - 1 + i) \\
&= x^2 - x - xi - x + 1 + i + xi - i + 1 \\
&= x^2 - 2x + 2
\end{aligned}$$

Then like in previous problems we apply Eisenstein's Irreducibility Criterion with $p = 2$, we see that 2 divides 2 and -2, doesn't divide 1, and 4 doesn't divide 2, so it is irreducible. Meaning the minimal polynomial over $\mathbb{Q}$ for the given element is,

$$x^2 - 2x + 2.$$

$\square$

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

*Proof.* Since $x^3 - 2$ is of degree 3, if we it assume it to be reducible we would have that it can be factored by a linear factor, and therefore have at least one root in $F$. In other words,

$$x^3 - 2 = (x - \alpha)p(x)$$

where $p(x)$ is a monic quadratic polynomial and $\alpha \in F$. Now let $\zeta = \frac{1}{2} + \frac{\sqrt{3}}{2}i$, we have that the roots of $x^3 - 2$ to be $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta$, and $\sqrt[3]{2}(\bar{\zeta})$. Note though that elements of $F$ are of the form $a + bi$ where $a, b \in \mathbb{Q}$, we see that none of these roots are of this form, therefore $x^3 - 2$ is irreducible over $F$.

We proceed similarly to show the same for $x^3 - 3$. If it were to be reducible over $F$ we would have the same story as above and the roots to be $\sqrt[3]{3}$, $\sqrt[3]{3}\zeta$, and $\sqrt[3]{3}(\bar{\zeta})$, but none of them are in $F$, meaning $x^3 - 3$ is irreducible over $F$. $\square$

**Problem 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.* This will be a proof by contradiction. We see that ,

$$[\mathbb{Q}(\alpha_1, \ldots, \alpha_i) : \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})] \in \{1, 2\}$$

for $i = 1, \ldots, n$. So $[F : \mathbb{Q}] = 2^k$ for $k \in \mathbb{N}$. Now assume that $\sqrt[3]{2} \in F$, we would have then that,

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset F$$

and therefore $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$ must divide $[F : \mathbb{Q}]$, but that means 3 divides $2^k$ which is a contradiction as desired. Meaning then that $\sqrt[3]{2} \in F$ $\square$

**Problem 13.2.15** A field $F$ is said to be formally real if $-1$ is not expressible as a sum of squares in $F$. Let $F$ be a formally real field, let $f(x) \in F[x]$ be an irreducible polynomial of odd degree and let $\alpha$ be a root of $f(x)$. Prove that $F(\alpha)$ is also formally real. [Pick $\alpha$ a counterexample of minimal degree. Show that $-1 + f(x)g(x) = (p_1(x))^2 + \cdots + (p_m(x))^2$ for some $p_i(x), g(x) \in F[x]$ where $g(x)$ has odd degree $<$ deg $(f)$. Show that some root $\beta$ of $g$ has odd degree over $F$ and $F(\beta)$ is not formally real, violating the minimality of $\alpha$.]

*Proof.* Let $\alpha$ be of minimal degree so that $F(\alpha)$ is NOT formally real and $\alpha$ having minimal polynomial $f$ which is of odd degree. Meaning we can express the degree of said $f$ as,

$$\deg(f) = 2k + 1, \ k \in \mathbb{N}$$

As given in the problem statement $-1$ can be expressed as a sum of squares in $F(\alpha)$, and we have that $F(\alpha)$ is isomorphic to $F[x]/(f(x))$. Then we have that there exists polynomials $p_1(x), \ldots, p_m(x)$, and $g(x)$ so that,

$$(p_1(x))^2 + \cdots + (p_m(x))^2 = -1 + f(x)g(x) \tag{4}$$

We know that elements of $F[x]/(f(x))$ can be expressed as a polynomial in $\alpha$ with degree $< \deg(f)$. Meaning we have then that, $\deg p_i < 2k+1$ for all $i$. This means that the degree on the LHS of (4) is less than $4k+1$, so the degree of $g$ is also less than $2k+1$. We want to show then that the degree of $g$ is odd because then that would imply the degree of the LHS of (4) must be even.

So now we let $d$ be the maximal degree over $p_i$ for all $i$. We see that $x^{2d}$ is a sum of squares. Because $F$ is formally real, we have then that 0 cannot be expressed as a sum of squares in $F$, therefore $x^{2d} \neq 0$. Meaning the degree of the LHS of (4) must be $2d$, and thus the degree of $g$ is odd. Meaning $g$ contains an irreducible factor of odd degree which we will denote $r(x)$, and because the degree of $g$ is less than the degree of $f$ we have,

$$deg(r) < deg(g) < deg(f)$$

So let $\beta$ be a root of $r(x)$ (therefore a root of $g(x)$), then,

$$(p_1(x))^2 + \cdots + (p_m(x))^2 = -1r(x)\frac{f(x)g(x)}{r(x)}$$

meaning $-1$ is a square in $F[x]/(h(x))$ which is isomorphic to $F(\beta)$. Giving to us that $F(\beta)$ is not formally real. Implying that $\beta$ is a root of $r$ such that $F(\beta)$ is not formally real, but $deg(r) < deg(f)$ which violates the minimality of $\alpha$, as desired. $\square$

**Problem 13.2.16** Let $K/F$ be an algebraic extension and let $R$ be a ring contained in $K$ and containing $F$. Show that $R$ is a subfield of $K$ containing $F$.

*Proof.* All we have to show is that $R$ contains multiplicative inverses. So let $r \in R$ and $r \neq 0$. We have that $r$ is algebraic over $F$ meaning that there exists an irreducible polynomial $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ in $F[x]$ such that $r$ is a root. Because $p$ is irreducible we have that the constant term of $p(x)$ must be non-zero. We know that,

$$r^{-1} = -a_0^{-1}(r^{n-1} + \cdots + a_1) \tag{5}$$

because $a_i \in F$ and $F$ is contained in $R$, and $r$ was an element of $R$, we have that $r^{-1} \in R$. Meaning $R$ has multiplicative inverse, making it a subfield of $K$ which contains $F$, as desired. $\square$