Math 620: §4.3 Existence of Roots

Due on Monday, December 7, 2015

Boynton 10:00

Kailee Gray

Exercise 4.3.5: Let $\phi : F_1 \to F_2$ be an isomorphism of fields. Prove that $\phi(1) = 1$. That is, prove that ϕ must map the multiplicative identity of F_1 to the multiplicative identity of F_2.

Proof. Let $\phi : F_1 \to F_2$ be an isomorphism of fields. Since F_1, F_2 are fields they contain a multiplicative and additive idenity. Let 1_1, 1_2 denote the multiplicative identities in F_1, F_2, respectively; let 0_1 and 0_2 be the additive identities of F_1 and F_2, respectively. First, to show $\phi(1_1)$ has a multiplicative inverse in F_2 we will show that $\phi(1_1) \neq 0_2$:

Since F_1, F_2 are fields, there exists an additive inverse of every element in F_1, F_2. Note that ϕ is an isomorphism so it preserves addition; also, F_1, F_2 are fields so addition and multiplication are associative. Then:

$$\begin{aligned}
\phi(0_1) &= \phi(0_1) + 0_2 \\
&= \phi(0_1) + \phi(0_1) - \phi(0_1) \\
&= \phi(0_1 + 0_1) - \phi(0_1) \\
&= \phi(0_1) - \phi(0_1) \\
&= 0_2.
\end{aligned}$$

Since ϕ is a bijection, if $\phi(0_1) = 0_2$, $\phi(1_1) \neq 0_2$ so $\phi(1_1)$ has a multiplicative inverse in F_2, denote by $\phi(1_1)^{-1}$. Following a similar process and justifications as above, we have:

$$\begin{aligned}
\phi(1_1) &= \phi(1_1) \cdot 1_2 \\
&= \phi(1_1) \cdot (\phi(1_1) \cdot \phi(1_1)^{-1}) \\
&= (\phi(1_1) \cdot \phi(1_1)) \cdot \phi(1_1)^{-1} \\
&= \phi(1_1 \cdot 1_1) \cdot \phi(1_1)^{-1} \\
&= \phi(1_1) \cdot \phi(1_1)^{-1} \\
&= 1_2.
\end{aligned}$$

□

Exercise 4.3.6: Let F be a field, let $p(x)$ be an irreducible polynomial in $F[x]$, and let $E = \{[a] \in F[x]/\langle p(x)\rangle \,|a \in F\}$. Show that E is a subfield of $F[x]/\langle p(x)\rangle$.

(prove E is a subfield). First, since $p(x)$ is irreducible, note that $F[x]/\langle p(x)\rangle$ is a field by theorem 4.3.6. Given the definition of E, it is clear E is a subset of $F[x]/\langle p(x)\rangle$; also $F \neq \emptyset$ so $E \neq \emptyset$. Thus, by exercise 4.3.4, it suffices to show E is closed under addition, subtraction, multiplication, and division of E.

(addition, subtraction) Consider any $[a], [b] \in E$. Then, using the definition of $\boxplus$ given in theorem 5 of Boynton, $[a] \boxplus [b] = [a + b] \in E$ since F is closed under $+$. If $[a], [b] \in E$, then $a, b \in F$ so a, b have additive inverses in F, denote $-a, -b$. Thus

$[a] - [b] = [a] \boxplus [-b] = [a - b] = [a + (-b)] \in E$ since F is closed under $+$ and

$[b] - [a] = [b] \boxplus [-a] = [b - a] = [b + (-a)] \in E$ since F is closed under $+$.

(multiplication, division) Consider any $[a], [b] \in E$, $[a], [b] \neq 0$. Then, using the definition of $\boxdot$ given in theorem 5 of Boynton,

$[a] \boxdot [b] = [a \cdot b] \in E$ since F is closed under $\cdot$. If $[a], [b] \in E$, then $a, b \in F$ and $[a], [b] \neq 0$ so a, b have multiplicative inverses in F, denote a^{-1}, b^{-1}. Note

$[a] \div [b] = [a] \boxdot [b]^{-1} = [a] \boxdot [b^{-1}] = [a \cdot b^{-1}] \in E$ since F is closed under $\cdot$. Also,

$[b] \div [a] = [b] \boxdot [a]^{-1} = [b] \boxdot [a^{-1}] = [b \cdot a^{-1}] \in E$ since F is closed under $\cdot$.

Hence, E is a subfield of F. □

Prove $\phi : F \to E$ defined by $\phi(a) = [a]$ is an isomorphism of fields.

Proof. **(well-defined)** Consider $a_1, a_2 \in F$ with $a_1 = a_2$. Then, $a_1 - a_2 = 0$ so $p(x)|(a_1 - a_2)$. Hence $[a_1] = [a_2]$.

(one to one) Suppose $\phi(a_1) = \phi(a_2)$ for some $a_1, a_2 \in F$. Then, $[a_1] = [a_2]$ and $[a_1], [a_2] \in F[x]/\langle p(x)\rangle$ imply $p(x) \mid a_1 - a_2$. So there exists some $q(x) \in F[x]/\langle p(x)\rangle$ such that $a_1 - a_2 = p(x)q(x)$. Since $\deg(a_1 - a_2) = 0$, $\deg(p(x)q(x)) = 0$ and so $\deg(p(x)) + \deg(q(x)) = 0$. But $\deg(p(x)) \geq 1$ so $\deg(q(x)) < 0$ and $q(x) = 0$, $a_1 = a_2$.

(onto) Consider any $[a] \in E$. Then, $a \in F$ and so $\phi(a) = [a]$.

(preserves +) Let $a_1, a_2 \in F$. Then, Let $a_1, a_2 \in F$. Then, $\phi(a_1 + a_2) = [a_1 + a_2] = [a_1] + [a_2] = \phi(a_1) + \phi(a_2)$.

(preserves $\cdot$) Let $a_1, a_2 \in F$. Then, $\phi(a_1 \cdot a_2) = [a_1 \cdot a_2] = [a_1] \cdot [a_2] = \phi(a_1) \cdot \phi(a_2)$.

Thus, by definition 4.3.7, ϕ is an isomorphism of fields. □

Exercise 4.3.8: Prove that $\mathbb{R}[x]/\langle x^2 + 2\rangle$ is isomorphic to $\mathbb{C}$.

Proof. By proposition 4.3.3 in Beachy, all elements in $\mathbb{R}[x]/\langle x^2 + 2\rangle$ are of the form $[a + bx]$. Define $\phi : \mathbb{R}[x]/\langle x^2 + 2\rangle \to \mathbb{C}$ by $\phi([a + bx]) = a + bi\sqrt{2}$. We will show ϕ is an isomorphism.

(well-defined) Consider $[a_1 + b_1x], [a_2 + b_2x] \in \mathbb{R}[x]/\langle x^2 + 2\rangle$ with $[a_1 + b_1x] = [a_2 + b_2x]$. Then, by definition 4.3.2, $(x^2 + 2) \mid (a_1 + b_1x - (a_2 + b_2x))$ and so $(x^2 + 2) \mid (a_1 - a_2 + (b_1 - b_2)x)$. Thus, there exists $q(x)$ such that $a_1 - a_2 + (b_1 - b_2)x = (x^2 + 2)q(x)$. Since $\deg(a_1 - a_2 + (b_1 - b_2)x) = 1$ and $\deg(x^2 + 2) = 2$, $\deg(q(x)) < 0$. Thus, $q(x) = 0$ and so $a_1 - a_2 + (b_1 - b_2)x = 0$ which implies $a_1 - a_2 = 0$ and $b_1 - b_2 = 0$. Thus, $a_1 + b_1i\sqrt{2} = a_2 + b_2i\sqrt{2}$ which implies $\phi([a_1 + b_1x]) = \phi([a_2 + b_2x])$.

(one to one) Suppose $\phi([a_1 + b_1x]) = \phi([a_2 + b_2x])$ for some $[a_1 + b_1x], [a_2 + b_2x] \in \mathbb{R}[x]/\langle x^2 + 2\rangle$. Then, $a_1 + b_1i\sqrt{2} = a_2 + b_2i\sqrt{2}$; equivalently $a_1 = a_2$ and $b_1 = b_2$. Thus, $a_1 + b_1x = a_2 + b_2x$ and so $[a_1 + b_1x] = [a_2 + b_2x]$.

(onto) Consider any $a + bi \in \mathbb{C}$. Then, $a, b \in \mathbb{R}$ and so

$$\phi\left(\left[a + \frac{b}{\sqrt{2}}\,x\right]\right) = a + \frac{b}{\sqrt{2}}i\sqrt{2} = a + bi.$$

(preserves addition, multiplication) Let $[a_1 + b_1x], [a_2 + b_2x] \in \mathbb{R}[x]/\langle x^2 + 2\rangle$. Then, $\phi([a_1 + b_1x] + [a_2 + b_2x]) = \phi[a_1 + b_1x + a_2 + b_2x] = \phi[a_1 + a_2 + (b_1 + b_2)x] =$ $a_1 + a_2 + (b_1 + b_2)i\sqrt{2} = a_1 + b_1i\sqrt{2} + a_2 + b_2i\sqrt{2} = \phi([a_1 + b_1x]) + \phi([a_2 + b_2x])$. Next, notice $\phi([a_1 + b_1x] \cdot [a_2 + b_2x]) = \phi([(a_1 + b_1x) \cdot (a_2 + b_2x)]) = \phi(a_1a_2 + (a_2b_1 + a_1b_2)x + b_1b_2x^2)$. In $\mathbb{R}[x]/\langle x^2 + 2\rangle$, $[x^2 + 2] = 0$ so $[x]^2 = -[2]$. Thus, $b_1b_2x^2 = -2b_1b_2$ so we have

$$\begin{aligned}
\phi(a_1a_2 + (a_2b_1 + a_1b_2)x + -2b_1b_2) &= \phi((a_1a_2 - 2b_1b_2) + (a_2b_1 + a_1b_2)x) \\
&= (a_1a_2 - 2b_1b_2) + (a_2b_1 + a_1b_2)i\sqrt{2} \\
&= (a_1 + b_1i\sqrt{2})(a_2 + b_2i\sqrt{2}) \\
&= \phi([a_1 + b_1x]) \cdot \phi([a_2 + b_2x])
\end{aligned}$$

By definition 4.3.7, ϕ is an isomorphism; hence $\mathbb{R}[x]/\langle x^2 + 2\rangle$ is isomorphic to $\mathbb{C}$. $\square$

Exercise 4.3.9: Prove that $\mathbb{R}[x]/\langle x^2 + x + 1\rangle$ is isomorphic to $\mathbb{C}$.

Proof. By proposition 4.3.3 in Beachy, all elements in $\mathbb{R}[x]/\langle x^2 + x + 1\rangle$ are of the form $[a + bx]$. Define $\phi : \mathbb{R}[x]/\langle x^2 + x + 1\rangle \to \mathbb{C}$ by $\phi([a + bx]) = a - \frac{b}{2} + \frac{b\sqrt{3}}{2}i$. We will show ϕ is an isomorphism.

(well-defined) Consider $[a_1 + b_1x], [a_2 + b_2x] \in \mathbb{R}[x]/\langle x^2 + x + 1\rangle$ with $[a_1 + b_1x] = [a_2 + b_2x]$. Then, by definition 4.3.2, $(x^2 + x + 1) \mid (a_1 + b_1x - (a_2 + b_2x))$ and so $(x^2 + x + 1) \mid (a_1 - a_2 + (b_1 - b_2)x)$. Thus, there exists $q(x)$ such that $a_1 - a_2 + (b_1 - b_2)x = (x^2 + x + 1)q(x)$. Since $\deg(a_1 - a_2 + (b_1 - b_2)x) = 1$ and $\deg(x^2 + x + 1) = 2$, $\deg(q(x)) < 0$. Thus, $q(x) = 0$ and so $a_1 - a_2 + (b_1 - b_2)x = 0$ which implies $a_1 - a_2 = 0$ and $b_1 - b_2 = 0$. Thus, $a_1 + b_1\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = a_2 + b_2\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)$ which implies $\phi([a_1 + b_1x]) = \phi([a_2 + b_2x])$.

(one to one) Suppose $\phi([a_1 + b_1x]) = \phi([a_2 + b_2x])$ for some

$[a_1 + b_1x], [a_2 + b_2x] \in \mathbb{R}[x]/\langle x^2 + x + 1\rangle$. Then,

$$a_1 - \frac{b_1}{2} + \frac{b_1\sqrt{3}}{2}i = a_2 - \frac{b_2}{2} + \frac{b_2\sqrt{3}}{2}i \text{ and } a_1 - a_2 + \frac{b_2 - b_1}{2} + (b_1 - b_2)\frac{\sqrt{3}}{2}i = 0.$$

Therefore, $b_1 - b_2 = 0$ so $b_1 = b_2$ and $b_2 - b_1 = 0$. Also, $a_1 - a_2 + \frac{b_2 - b_1}{2} = 0$ so $a_1 - a_2 = 0$.

Thus, $a_1 = a_2$. Therefore, $a_1 + b_1x = a_2 + b_2x$ and so $[a_1 + b_1x] = [a_2 + b_2x]$.

(onto) Consider any $a + bi \in \mathbb{C}$. Then, $a, b \in \mathbb{R}$ so $a + \frac{b}{\sqrt{3}}, \frac{2b}{\sqrt{3}} \in \mathbb{R}$ and

$$\phi\left(\left[a + \frac{b}{\sqrt{3}} + \frac{2b}{\sqrt{3}}\ x\right]\right) = a + \frac{b}{\sqrt{3}} - \frac{1}{2}\frac{2b}{\sqrt{3}} + \frac{2b}{\sqrt{3}}\frac{\sqrt{3}}{2}i = a + bi.$$

(preserves addition, multiplication) Let $[a_1 + b_1x], [a_2 + b_2x] \in \mathbb{R}[x]/\langle x^2 + x + 1\rangle$.

$$\begin{aligned}
\text{Then, } \phi([a_1 + b_1x] + [a_2 + b_2x]) &= \phi([a_1 + a_2 + (b_1 + b_2)x]) \\
&= a_1 + a_2 + -\frac{b_1 + b_2}{2} + \frac{(b_1 + b_2)\sqrt{3}}{2} \\
&= a_1 - \frac{b_1}{2} + \frac{b_1\sqrt{3}}{2}i + a_2 - \frac{b_2}{2} + \frac{b_2\sqrt{3}}{2}i \\
&= \phi([a_1 + b_1x]) + \phi([a_2 + b_2x]). \text{ Next, notice}
\end{aligned}$$

$\phi([a_1 + b_1x] \cdot [a_2 + b_2x]) = \phi([(a_1 + b_1x) \cdot (a_2 + b_2x)]) = \phi(a_1a_2 + (a_2b_1 + a_1b_2)x + b_1b_2x^2)$.

In $\mathbb{R}[x]/\langle x^2 + x + 1\rangle$, $[x^2 + x + 1] = 0$ so $[x]^2 = -[x] - [1]$. Thus, $x^2b_1b_2 = -(x + 1)b_1b_2$ so

we have $\phi((a_1a_2 - b_1b_2) + (a_2b_1 + a_1b_2 - b_1b_2)x) =$

$$\begin{aligned}
&= (a_1a_2 - b_1b_2) + \frac{a_2b_1 + a_1b_2 - b_1b_2}{2} + \frac{\sqrt{3}}{2}(a_2b_1 + a_1b_2 - b_1b_2)i \\
&= \left(a_1 + \frac{b_1}{2} + b_1i\frac{\sqrt{3}}{2}\right)\left(a_2 + \frac{b_2}{2} + b_2i\frac{\sqrt{3}}{2}\right) = \phi([a_1 + b_1x]) \cdot \phi([a_2 + b_2x])
\end{aligned}$$

By definition 4.3.7, ϕ is an isomorphism; hence $\mathbb{R}[x]/\langle x^2 + x + 1\rangle$ is isomorphic to $\mathbb{C}$. $\square$

Exercise 4.3.10: Is $\mathbb{Q}[x]/\langle x^2+2\rangle$ isomorphic to $\mathbb{Q}[x]/\langle x^2+1\rangle$?

Proof. No. By proof similar to 4.3.8, 4.3.9, 4.3.13 and by Jason's approval to use, $\mathbb{Q}[x]/\langle x^2+2\rangle$ is isomorphic to $\mathbb{Q}(i\sqrt{2})$ and $\mathbb{Q}[x]/\langle x^2+1\rangle$ is isomorphic to $\mathbb{Q}(i)$. Thus $\mathbb{Q}[x]/\langle x^2+2\rangle$ isomorphic to $\mathbb{Q}[x]/\langle x^2+1\rangle$ if and only if $\mathbb{Q}(i\sqrt{2})$ is isomorphic to $\mathbb{Q}(i)$. So, suppose $\mathbb{Q}(i\sqrt{2})$ is isomorphic to $\mathbb{Q}(i)$. First, note that the polynomial x^2+2 has a root in $\mathbb{Q}(i\sqrt{2})$, $i\sqrt{2} \in \mathbb{Q}(i\sqrt{2})$: $(i\sqrt{2})^2+2 = -2+2 = 0$.
Suppose the polynomial x^2+2 has a root in $\mathbb{Q}(i)$. Then, there would be some $a, b \in \mathbb{Q}$ such that $(a+bi)^2+2 = 0$. Equivalently, $a^2-b^2+2 = -2abi$. But, $a^2-b^2+2 \in \mathbb{R}, \notin \mathbb{C}$ and $-2abi \in \mathbb{C}$ so this is a contradiction. Thus, x^2+2 does not have a root in $\mathbb{Q}(i)$.
Now, we assumed that $\mathbb{Q}(i\sqrt{2})$ is isomorphic to $\mathbb{Q}(i)$ so there is an isomorphism $\phi : \mathbb{Q}(i\sqrt{2}) \to \mathbb{Q}(i)$. Let $x \in \mathbb{Q}(i\sqrt{2})$ be a root of x^2+2. Then, $x^2+2 = 0$ and so $\phi(x^2+2) = \phi(0)$. $\phi(0) = 0$ and ϕ preserves multiplication and addition so $\phi(x)^2 + \phi(2) = 0$. Also, $\phi(2) = \phi(1+1) = \phi(1)+\phi(1) = 1+1 = 2$ which implies there is some $\phi(x) \in \mathbb{Q}(i)$ with $\phi(x)^2+2 = 0$ and so $\phi(x)$ is a root of x^2+2. This is a contradiction since we proved $\mathbb{Q}(i)$ does not contain a root of x^2+2. $\square$

Exercise 4.3.13: Prove that $\mathbb{Q}[x]/\langle x^2-3\rangle$ is isomorphic to $\mathbb{Q}(\sqrt{3})$.

Proof. Define By proposition 4.3.3 in Beachy, all elements in $\mathbb{Q}[x]/\langle x^2-3\rangle$ are of the form $[a+bx]$. Define $\phi : \mathbb{Q}[x]/\langle x^2-3\rangle \to \mathbb{Q}(\sqrt{3})$ by $\varphi([a+bx]) = a+b\sqrt{3}$. We will show ϕ is an isomorphism.

(well-defined) Consider $[a_1+b_1x], [a_2+b_2x] \in \mathbb{Q}[x]/\langle x^2-3\rangle$ with $[a_1+b_1x] = [a_2+b_2x]$. Then, by definition 4.3.2, $(x^2-3) \mid (a_1-a_2+(b_1-b_2)x)$. Thus, there exists $q(x)$ such that $a_1-a_2+(b_1-b_2)x = (x^2-3)q(x)$. Since $\deg(a_1-a_2+(b_1-b_2)x) = 1$ and $\deg(x^2-3) = 2$, $\deg(q(x)) < 0$. Thus, $q(x) = 0$ and so $a_1-a_2+(b_1-b_2)x = 0$ which implies $a_1-a_2 = 0$ and $b_1-b_2 = 0$. Thus, $a_1+b_1\sqrt{3} = a_2+b_2\sqrt{3}$ which implies $\phi([a_1+b_1x]) = \phi([a_2+b_2x])$.

(one to one) Suppose $\phi([a_1+b_1x]) = \phi([a_2+b_2x])$ for some $[a_1+b_1x], [a_2+b_2x] \in \mathbb{Q}[x]/\langle x^2-3\rangle$. Then, $a_1+b_1\sqrt{3} = a_2+b_2\sqrt{3}$; because $a_1, a_2, b_1, b_1 \in \mathbb{Q}$ this is equivalent to $a_1 = a_2$ and $b_1 = b_2$. Thus, $a_1+b_1x = a_2+b_2x$ and so $[a_1+b_1x] = [a_2+b_2x]$.

(onto) Consider any $a+b\sqrt{3} \in \mathbb{Q}(\sqrt{3})$. Then, $a, b \in \mathbb{Q}$ and so $\phi\left([a+bx]\right) = a+b\sqrt{3}$.

(preserves addition, multiplication) Let $[a_1+b_1x], [a_2+b_2x] \in \mathbb{Q}[x]/\langle x^2-3\rangle$. Then, $\phi([a_1+b_1x]+[a_2+b_2x]) = \phi[a_1+b_1x+a_2+b_2x] = \phi[a_1+a_2+(b_1+b_2)x] = a_1+a_2+(b_1+b_2)\sqrt{3} = a_1+b_1\sqrt{3}+a_2+b_2\sqrt{3} = \phi([a_1+b_1x])+\phi([a_2+b_2x])$. Next, notice $\phi([a_1+b_1x]\cdot[a_2+b_2x]) = \phi([(a_1+b_1x)\cdot(a_2+b_2x)]) = \phi(a_1a_2+(a_2b_1+a_1b_2)x+b_1b_2x^2)$. In $\mathbb{Q}[x]/\langle x^2-3\rangle$, $[x^2-3] = 0$ so $[x]^2 = [3]$. Thus, $b_1b_2x^2 = 3b_1b_2$ so we have

$$\begin{aligned}
\phi(a_1a_2+(a_2b_1+a_1b_2)x+3b_1b_2) &= \phi((a_1a_2+3b_1b_2)+(a_2b_1+a_1b_2)x) \\
&= (a_1a_2+3b_1b_2)+(a_2b_1+a_1b_2)\sqrt{3} \\
&= (a_1+b_1\sqrt{3})(a_2+b_2\sqrt{3}) \\
&= \phi([a_1+b_1x])\cdot\phi([a_2+b_2x])
\end{aligned}$$

By definition 4.3.7, ϕ is an isomorphism; hence $\mathbb{Q}[x]/\langle x^2-3\rangle$ is isomorphic to $\mathbb{Q}(\sqrt{3})$.

□

Exercise 4.3.14: Show that the polynomial $x^2 - 3$ has a root in $\mathbb{Q}(\sqrt{3})$ but not in $\mathbb{Q}(\sqrt{2})$. Explain why this implies $\mathbb{Q}(\sqrt{3})$ is not isomorphic to $\mathbb{Q}(\sqrt{2})$.

Proof. First, show $x^2 - 3$ has a root in $\mathbb{Q}(\sqrt{3})$ but not in $\mathbb{Q}(\sqrt{2})$. Notice $\sqrt{3} \in \mathbb{Q}(\sqrt{3})$ and $\sqrt{3}^2 - 3 = 0$ so $x^2 - 3$ has a root in $\mathbb{Q}(\sqrt{3})$. Suppose $x^2 - 3$ has a root in $\mathbb{Q}(\sqrt{2})$. Then, there exists some $a + b\sqrt{2}$, with $a, b \in \mathbb{Q}$, such that $(a + b\sqrt{2})^2 - 3 = 0$. Simplifying,

$$(a + b\sqrt{2})^2 - 3 = a^2 + 2b^2 + 2ab\sqrt{2} - 3 = (a^2 + 2b^2 - 3) + 2ab\sqrt{2}.$$

$$\text{If } (a^2 + 2b^2 - 3) + 2ab\sqrt{2} = 0, \ a^2 + 2b^2 - 3 = 0 \text{ and } 2ab = 0. \text{ Thus, } a = 0 \text{ or } b = 0.$$

Suppose $b = 0$. Then, $a^2 + 2 \cdot 0^2 - 3 = 0$ implies $a^2 = 3$ and so $a = \pm\sqrt{3} \notin \mathbb{Q}$. Thus, $b \neq 0$. Suppose $a = 0$, then $0^2 + 2 \cdot b^2 - 3 = 0$ implies $2b^2 = 3$ and so $b = \pm\sqrt{\frac{3}{2}} \notin \mathbb{Q}$. Thus, $a \neq 0$. Hence, $x^2 - 3$ does not have a root in $\mathbb{Q}(\sqrt{2})$.

Next, show $\mathbb{Q}(\sqrt{2})$ is not isomorphic to $\mathbb{Q}(\sqrt{3})$. Suppose $\mathbb{Q}(\sqrt{2})$ is isomorphic to $\mathbb{Q}(\sqrt{3})$. Then, there exists a bijective map $\phi : \mathbb{Q}(\sqrt{3}) \to \mathbb{Q}(\sqrt{2})$ that preserves multiplication and addition. From above we know there is $x \in \mathbb{Q}(\sqrt{3})$ with $x^2 - 3 = 0$, then $\phi(x^2 - 3) = \phi(0)$. ϕ is an isomorphism so $\phi(0) = 0$. Also,

$$\phi(x^2-3) = \phi(x^2)+\phi(-3) = \phi(x)\phi(x)-\phi(3) = \phi(x)^2-\phi(1+1+1) = \phi(x)^2-(\phi(1)+\phi(1)+\phi(1)).$$

Hence there must be an element in $\mathbb{Q}(\sqrt{2})$, $\phi(x)$ with $\phi(x)^2 - 3 = 0$. From above, no such element exists in $\mathbb{Q}(\sqrt{2})$. Thus, $\mathbb{Q}(\sqrt{2})$ is not isomorphic to $\mathbb{Q}(\sqrt{3})$. □

Exercise 4.3.17: Find an irreducible polynomial $p(x)$ of degree 3 over $\mathbb{Z}_2$, and list all elements of $\mathbb{Z}_2[x]/\langle p(x)\rangle$. Give the identities necessary to multiply elements.

Proof. From section 4.2 homework, number 12, the polynomial $x^3 + x + 1$ is irreducible over $\mathbb{Z}_2$. Then, by theorem 9 of Boynton, all elements in $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$ can be represented by some polynomial of the form $ax^2 + bx + c$ for some $a, b, c \in \mathbb{Z}_2$. By statement on page 209 of Beachy, $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$ has $2^3 = 8$ polynomials of degree less than 3. There are 8 polynomials of degree 2 or less in $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$, so we have the following elements:

$$[0], [1], [x], [x + 1], [x^2], [x^2 + 1], [x^2 + x], [x^2 + x + 1]$$

The identities necessary to multiply elements are $[x]^3 = [-x - 1]$ and $[x]^4 = [-x^2 - x]$. $\square$

Exercise 4.3.18: Give addition and multiplication tables for the field $\mathbb{Z}_3[x]/\langle x^2 + x + 2\rangle$.

Let $p(x) = x^2 + x + 2$ with $p(x) \in \mathbb{Z}_3$. Then, $p(0) = 2, p(1) = 1, p(2) = 2$ so by proposition 4.2.7, $p(x)$ is irreducible in $\mathbb{Z}_3$. By theorem 9 of Boynton, all elements in $\mathbb{Z}_3[x]/\langle x^2 + x + 2\rangle$ can be represented by a polynomial of the form $a + bx$ with $a, b \in \mathbb{Z}_3$. Then, by page 209 of Beachy, $\mathbb{Z}_3[x]/\langle x^2 + x + 2\rangle$ has $3^2 = 9$ elements. To simplify the table, brackets have been omitted in listing the congruence classes.
We will use the identity $[x]^2 = [2x + 1]$ to multiply these elements.

$+$	0	1	2	x	$2x$	$x+1$	$x+2$	$2x+1$	$2x+2$
0	0	1	2	x	$2x$	$x+1$	$x+2$	$2x+1$	$2x+2$
1	1	2	0	$x+1$	$2x+1$	$x+2$	x	$2x+2$	$2x$
2	2	0	1	$x+2$	$2x+2$	x	$x+1$	$2x$	$2x+1$
x	x	$x+1$	$x+2$	$2x$	0	$2x+1$	$2x+2$	1	2
$2x$	$2x$	$2x+1$	$2x+2$	0	x	1	2	$x+1$	$x+2$
$x+1$	$x+1$	$x+2$	x	$2x+1$	1	$2x+2$	$2x$	2	0
$x+2$	$x+2$	x	$x+1$	$2x+2$	2	$2x$	$2x+1$	0	1
$2x+1$	$2x+1$	$2x+2$	$2x$	1	$x+1$	2	0	$x+2$	x
$2x+2$	$2x+2$	$2x$	$2x+1$	2	$x+2$	0	1	x	$x+1$

$\cdot$	0	1	2	x	$2x$	$x+1$	$x+2$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$2x$	$x+1$	$x+2$	$2x+1$	$2x+2$
2	0	2	1	$2x$	x	$2x+2$	$2x+1$	$x+2$	$x+1$
x	0	x	$2x$	$2x+1$	$x+2$	1	$x+1$	$2x+2$	2
$2x$	0	$2x$	x	$x+2$	$2x+1$	2	$2x+2$	$x+1$	1
$x+1$	0	$x+1$	$2x+2$	1	2	$x+2$	$2x$	x	$2x+1$
$x+2$	0	$x+2$	$2x+1$	$x+1$	$2x+2$	$2x$	2	1	x
$2x+1$	0	$2x+1$	$x+2$	$2x+2$	$x+1$	x	1	2	$2x$
$2x+2$	0	$2x+2$	$x+1$	2	1	$2x+1$	x	$2x$	$x+2$

Exercise 4.3.19: Find a polynomial of degree 3 irreducible over $\mathbb{Z}_3$, and use it to construct a field with 27 elements. List the elements of the field; give the identities necessary to multiply elements.

From exercise 13 in section 4.2 homework, the polynomial $x^3 + 2x + 1$ is irreducible over $\mathbb{Z}_3$. By theorem 4.3.6 of Beachy, $\mathbb{Z}_3/\langle x^3 + 2x + 1\rangle$ is a field. Also, by page 209 of Beachy, $\mathbb{Z}_3/\langle x^3 + 2x + 1\rangle$ contains $3^3 = 27$ elements. Notice there are 27 possible polynomials of degree ≤ 2 over $\mathbb{Z}_3$, so we have the following elements in $\mathbb{Z}_3/\langle x^3 + 2x + 1\rangle$

$[0], [1], [2], [x], [2x], [x+1], [x+2], [2x+1], [2x+2], [x^2], [2x^2], [x^2+1], [x^2+2], [2x^2+1], [2x^2+2],$

$$[x^2 + x], [x^2 + x + 1], [x^2 + x + 2], [x^2 + 2x], [x^2 + 2x + 1], [x^2 + 2x + 2]$$

$$[2x^2 + x], [2x^2 + x + 1], [2x^2 + x + 2], [2x^2 + 2x], [2x^2 + 2x + 1], [2x^2 + 2x + 2]$$

We will need the identities $[x]^3 = [x + 2]$ and $[x]^4 = [x^2 + 2x]$ to multiply these elements.

Exercise 4.3.21: Find multiplicative inverses of the elements in the given fields.

(a) $[a + bx]$ in $\mathbb{R}[x]/\langle x^2 + 1\rangle$

If $a = 0, b = 0$, the element $[0]$ does not have a multiplicative inverse.

If $a \neq 0, b = 0$, then the inverse of $[a]$ is just $\frac{1}{a}$.

Now suppose $b \neq 0$. Use the division algorithm to divide $x^2 + 1$ by $a + bx$:

$$x^2 + 1 = (a + bx)\left(\frac{1}{b}x - \frac{a}{b^2}\right) + \frac{b^2 + a^2}{b^2}.$$

Equivalently, $\dfrac{b^2}{b^2 + a^2}(x^2+1) = \dfrac{b^2}{b^2 + a^2}(a+bx)\left(\dfrac{1}{b}x - \dfrac{a}{b^2}\right)+1$. Thus, in $\mathbb{R}[x]/\left\langle x^2 + 1\right\rangle$,

$1 = \dfrac{-b^2}{b^2 + a^2}\left(\dfrac{1}{b}x - \dfrac{a}{b^2}\right)(a+bx) = \dfrac{(-bx + a)}{b^2 + a^2}(a+bx)$. Hence, $[a+bx]^{-1} = \dfrac{(-bx + a)}{b^2 + a^2}$.

(b) $[a+bx]$ in $\mathbb{Q}[x]/\langle x^2-2\rangle$

If $a=0, b=0$, the element $[0]$ does not have a multiplicative inverse.

If $a\neq 0, b=0$, then the inverse of $[a]$ is $\frac{1}{a}$.

Now suppose $b\neq 0$. Use the division algorithm to divide x^2-2 by $a+bx$:

$$x^2-2=(a+bx)\left(\frac{1}{b}x-\frac{a}{b^2}\right)+\frac{a^2-2b^2}{b^2}.\text{ First, consider } a^2-2b^2\neq 0.$$

Then, $\dfrac{b^2}{a^2-2b^2}(x^2-2)=\dfrac{b^2}{a^2-2b^2}(a+bx)\left(\dfrac{1}{b}x-\dfrac{a}{b^2}\right)+1$. Thus, in $\mathbb{Q}[x]/\left\langle x^2-2\right\rangle$,

$1=\dfrac{b^2}{2b^2-a^2}\left(\dfrac{1}{b}x-\dfrac{a}{b^2}\right)(a+bx)=\dfrac{(bx-a)}{2b^2-a^2}(a+bx)$. Hence, $[a+bx]^{-1}=\dfrac{(bx-a)}{2b^2-a^2}$.

Now, if $a^2-2b^2=0$, we'll have $a^2=2b^2$ so

$$\left(\frac{a}{b}\right)^2=2 \text{ therefore } \frac{a}{b}=\pm\sqrt{2}.$$

However, $a,b\in\mathbb{Q}$, $b\neq 0$ implies $\frac{a}{b}\in\mathbb{Q}$ so $a^2-2b^2\neq 0$.

(c) $[x^2-2x+1]$ in $\mathbb{Q}[x]/\langle x^3-2\rangle$

The extended Euclidean algorithm yields

$$1=(-5x+6)(x^3-2)+(5x^2+4x+13)(x^2-2x+1).$$

However, after expanding $(5x^2+4x+13)(x^2-2x+1)$ and reducing mod x^3-2 using the identities $x^3\equiv 2$ and $x^4\equiv 2x$, we do not get 1. So, knowing that the multiplicative inverse is likely of the form ax^2+bx+c, solve for a,b,c:

$1=(ax^2+bx+c)(x^2-2x+1)=ax^4+(b-2a)x^3+(a-2b+c)x^2+(b-2c)x+c=$ $(a-2b+c)x^2+(2a+b-2c)x+(2b-4a+c)$. Thus, a,b,c must satisfy $a-2b+c=0$, $2a+b-2c=0$, and $2b-4a+c=1$. So, we will row reduce to solve this system of equations and obtain:

$$\left[\begin{array}{rrr|r} 1 & -2 & 1 & 0 \\ 2 & 1 & -2 & 0 \\ -4 & 2 & 1 & 1 \end{array}\right] \sim \left[\begin{array}{rrr|r} 1 & 0 & 0 & 3 \\ 0 & 1 & 0 & 4 \\ 0 & 0 & 1 & 5 \end{array}\right]$$

So, $[x^2 - 2x + 1]^{-1} = 3x^2 + 4x + 5$. Now, check this inverse works:

$$(3x^2 + 4x + 5)(x^2 - 2x + 1) = 3x^4 - 2x^3 - 6x + 5 \equiv 3 \cdot 2x - 2 \cdot 2 - 6x + 5 = 1.$$

Thus, $[x^2 - 2x + 1]^{-1} = 3x^2 + 4x + 5$.

(d) $[x^2 - 2x + 1]$ in $\mathbb{Z}_3[x]/\langle x^3 + x^2 + 2x + 1\rangle$

Use the Euclidean Algorithm to find $\gcd(x^2 - 2x + 1, x^3 + x^2 + 2x + 1)$:

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

Next, back substitute and simplify to find the multiplicative inverse:

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

Thus, $[x^2 - 2x + 1]^{-1} = 1 + x^2$.

(e) $[x]$ in $\mathbb{Z}_5[x]/\langle x^2 + x + 1\rangle$ Use the Division Algorithm to find $\gcd(x, x^2 + x + 1)$:

$$x^2 + x + 1 = (x)(x + 1) + 1. \text{ Thus, } x^2 + x + 1 - (x)(x + 1) = 1$$

In $\mathbb{Z}_5, -x-1 \equiv 4x+4$ so $[x]^{-1} = 4x+4$.

(f) $[x+4]$ in $\mathbb{Z}_5[x]/\langle x^3+x+1\rangle$

Use the division algorithm to find $\gcd(x+4, x^3+x+1)$:

$x^3+x+1 = (x+4)(x^2+x+2)+3$. Equivalently, $x^3+x+1-(x+4)(x^2+x+2) = 3$.

In $\mathbb{Z}_5$, $3^{-1} = 2$, so we can multiply the last equation by 2 to obtain:

$$2(x^3+x+1) - 2(x+4)(x^2+x+2) = 1. \text{ Also, } -2 \mod 5 = 3, \text{ so}$$

$$[x+4]^{-1} = 3(x^2+x+2) = 3x^2+3x+6 = 3x^2+3x+1.$$