Problem Set 8
Abstract Algebra II

Bennett Rennier
barennier@gmail.com

January 15, 2018

Section 9.4

Ex 1 Determine whether the following polynomials are irreducible in the rings indicated. For those that are reducible, determine their factorization into irreducibles. The notations $\mathbb{F}_p$ denotes the finite field $\mathbb{Z}/p\mathbb{Z}$, p a prime.

a) $x^2 + x + 1$ in $\mathbb{F}_2[x]$

b) $x^3 + x + 1$ in $\mathbb{F}_3[x]$

c) $x^4 + 1$ in $\mathbb{F}_5[x]$

d) $x^4 + 10x^2 + 1$ in $\mathbb{Z}[x]$

Proof. a) Since $\deg p(x) = 2$, we need only to check if $p(x)$ has a root. We see that $p(0) = 1$ and that $p(1) = 1 + 1 + 1 = 3 = 1$. Since there is no root in $\mathbb{F}_2$, we see that $p(x)$ is irreducible.

b) We see that $p(1) = 1^3 + 1 + 1 = 3 = 0$. Thus, $p(x) = q(x)(x+2) = (x^2 + ax + b)(x+2) = x^3 + 2x^2 + ax^2 + 2ax + bx + 2b = x^3 + (a+2)x^2 + (2a+b)x + 2b$. We see that $a = 1$ and $b = 2$ fulfills this, so we get that $p(x) = (x^2 + x + 2)(x + 2)$. Now $x + 2$ is irreducible, as it's linear. We also see that $q(x) = x^2 + x + 2$ is irreducible as well, since $q(0) = 2$, $q(1) = 4 = 1$, and $q(2) = 8 = 2$. Thus, we have completely factored $p(x)$.

c) Since we're in $\mathbb{F}_5$, we see that $p(x) = x^4 + 1 = x^4 - 4 = (x^2 + 2)(x^2 - 2) = (x^2 + 2)(x^2 + 3)$. Since in $\mathbb{F}_5$,

$$0^2 = 0 \quad 1^2 = 1 \quad 2^2 = 4 \quad 3^2 = 4 \quad 4^2 = 1$$

we see that $x^2 + 2$ and $x^2 + 3$ have no roots. This proves that we have fully factored $p(x)$.

d) We see that $p(x)$ is positive everywhere, which means that it has no roots. Thus, $p(x)$ has no linear factors. Suppose that $p(x) = (x^2 + ax + b)(x^2 + cx + d)$. This would mean that

$$p(x) = x^4 + (a + c)x^3 + (ac + b + d)x^2 + (ad + bc)x + bd$$

Comparing the coefficients, we see that $a + c = 0$, $ac + b + d = 10$, $ad + bc = 0$, and $bd = 1$. Since $bd = 1$, we have that $b = 1$ or $b = -1$.

Case 1) If $b = 1$, then $d = 1$, which means that $ac + 2 = 10$. From $a + c = 0$, this gives us that $-a^2 = 8$, which is a contradiction.

Case 2) If $b = -1$, then $d = -1$, which means that $ac + 2 = 10$. Similarly, we get that $-a^2 = 12$, which is again a contradiction.

This proves that $p(x)$ has no quadratic factors, proving that it's irreducible over $\mathbb{Z}$.

□

Ex 2 Prove that the following polynomials are irreducible in $\mathbb{Z}[x]$:

a) $x^4 - 4x^3 + 6$

b) $x^6 + 30x^5 - 15x^3 + 6x - 120$

c) $x^4 + 4x^3 + 6x^2 + 2x + 1$

d) $\frac{(x+2)^p - 2^p}{x}$, where p is an odd prime.

Proof. a) By Eisenstein's Criterion for $\mathbb{Z}[x]$, since 2 divides 4 and 6 and $2^2 = 4$ does not divide 6, we get that $x^4 - 4x^3 + 6$ is irreducible.

b) By Eisenstein's Criterion for $\mathbb{Z}[x]$, since 3 divides 30, 15, 6, and 120 and $3^2 = 9$ does not divide 120, we get that the polynomial is irreducible.

c) Subsituting $x - 1$ for x, we get that

$$\begin{aligned} p(x-1) &= (x-1)^4 + 4(x-1)^3 + 6(x-1)^2 + 2(x-1) + 1 \\ &= (x^4 - 4x^3 + 6x^2 - 4x + 1) + 4(x^3 - 3x^2 + 3x - 1) + 6(x^2 - 2x + 1) + (2x - 2) + 1 \\ &= x^4 - 2x + 2 \end{aligned}$$

By Eisenstein's Criterion for $\mathbb{Z}[x]$, since 2 divides -2 and 2 and $2^2 = 4$ does not divide 2, we get that $p(x-1)$ is irreducible. It follows then that $p(x)$ is irreducible as well, as any factorization of $p(x)$ would give a factorization of $p(x-1)$.

d) We see that

$$\frac{(x+2)^p - 2^p}{x} = \frac{\sum_{i=0}^{p} \binom{p}{i} x^i 2^{p-i} - 2^p}{x} = \sum_{i=1}^{p} \binom{p}{i} x^{i-1} 2^{p-i} = \sum_{i=0}^{p-1} \left[\binom{p}{i+1} 2^{p-i-1} \right] x^i$$

From this, we see that the coefficient on last term of the sum is 1, which proves that the polynomial is monic. We also see that the coefficient on all the other terms is $\binom{p}{i} 2^{p-i}$, where $1 \leq i \leq p-1$, which means that this are divisibly by p. Finally, since the first term is $\binom{p}{1} 2^{p-1} = p2^{p-1}$, we find that it's not divisble by p^2, as p was assumed to be odd. This proves that the polynomial is irreducible.

□

Ex 3 Show that the polynomial $(x-1)(x-2)\dots(x-n)-1$ is irreducible over $\mathbb{Z}$ for all $n \geq 1$. [If the polynomial factors, consider the values of the factors at $x = 1, 2, \dots, n$.]

Proof. Let n be fixed and let $p(x)$ denote this polynomial. Suppose that $p(x)$ is reducible. That means that $p(x) = a(x)b(x)$, where $a(x), b(x) \in \mathbb{Z}[x]$. We see also that for all $1 \leq k \leq n$, $p(k) = a(k)b(k) = -1$. This means that $\{a(k), b(k)\} = \{-1, 1\}$ for each k. Let $A = \{k \in [1,n] : a(k) = 1\}$ and let $B = \{k \in [1,n] : b(k) = 1\}$. Note that, in fact, $A \cup B = [1,n]$.

Using this, we see that A is a set of roots for $a(x)+1$, which proves that $a(x) = q(x)\prod_{k\in A}(x-k)-1$ for some polynomial $q(x)$. Similarly, $b(x) = r(x)\prod_{k\in B}(x-k)-1$ for some polynomial $r(x)$. However, since $a(x)$ and $b(x)$ are monic and $\deg p = \deg a + \deg b$, we see that it must be that $q(x) = r(x) = 1$.

Plugging in these new formulations of $a(x)$ and $b(x)$, we get that

$$\begin{aligned} p(x) = a(x)b(x) &= \left(\prod_{k\in B}(x-k)-1\right)\left(\prod_{k\in A}(x-k)-1\right) \\ &= \prod_{k=1}^{n}(x-k) - \prod_{k\in A}(x-k) - \prod_{k\in B}(x-k) + 1 = p(x) - \left(\prod_{k\in A}(x-k) + \prod_{k\in B}(x-k)\right) + 2. \end{aligned}$$

This proves that $\prod_{k\in A}(x-k) + \prod_{k\in B}(x-k) = 2$. However, this is a contradiction, as the degree of the left hand side is at least 1 (since $n \geq 1$ and $A \cap B = \varnothing$). This proves that $p(x)$ is irreducible. □

Section 13.1

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

Proof. We see that $p(x)$ is irreducible using the Eisenstein Criterion with $n = 3$. Let θ be a root of $p(x)$. To find the inverse, we use the Euclidean Algorithm to see that

$$\left[-\frac{1}{4}\right](x^3 + 9x + 6) + \left[\frac{1}{4}(x^2 - x + 10)\right](x+1) = 1$$

which proves that $(\frac{\theta^2}{4} - \frac{\theta}{4} + \frac{5}{2})(\theta + 1) = 1$ in $\mathbb{Q}(\theta)$. □

Ex 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 $\frac{1+\theta}{1+\theta+\theta^2}$ in $\mathbb{Q}(\theta)$.

Proof. We see that $p(x)$ is irreducible over $\mathbb{Q}$ using the Eisenstein Criterion with $n = 2$. We see that $\theta^3 = 2\theta + 2$ by construction. This means that

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

which is in $\mathbb{Q}(\theta)$, as it's an extension of degree 3 over $\mathbb{Q}$.

Using the Euclidean Algorithm, we see that

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

which proves that $(1+\theta+\theta^2)^{-1}=\frac{1}{3}(-2\theta^2+\theta+5)$. This gives us that

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

□

Ex 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. We see that $p(0)=0^3+0+1=1$ and that $p(1)=1^3+1+1=1$, which proves that $p(x)$ has no roots over $\mathbb{F}_2$. Since $p(x)$ is of degree 3, this proves that $p(x)$ is irreducible. We see that $\theta^3=\theta+1$ in $\mathbb{F}_2$ by construction. This means that

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

which are all the powers of θ. □

Ex 4 Prove directly that the map $a+b\sqrt{2}\mapsto a-b\sqrt{2}$ is an automorphism of $\mathbb{Q}(\sqrt{2})$.

Proof. Let $\varphi:\mathbb{Q}(\sqrt{2})\to\mathbb{Q}(\sqrt{2})$ be defined as $\varphi(a+b\sqrt{2})=a-b\sqrt{2}$. Firstly, we see that

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

and that

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

which proves that φ is a field homomorphism. Since φ is not the zero map, we get that φ is injective for free. To prove that it's surjective, let $a+b\sqrt{2}\in\mathbb{Q}(\sqrt{2})$. We see then that $\varphi(a-b\sqrt{2})=a+b\sqrt{2}$. This proves that φ is a bijective field homomorphism between $\mathbb{Q}(\sqrt{2})$ and itself. Thus φ is an automorphism of $\mathbb{Q}(\sqrt{2})$. □

Ex 5 Suppose α is a rational root of a monic polynomial in $\mathbb{Z}[x]$. Prove that α is an integer.

Proof. Let $m(x) = a_0 + a_1x + \cdots + x^n$ be an arbitrary monic polynomial in $\mathbb{Z}[x]$ and let $\alpha = p/q$ be a root of this polynomial in lowest terms. Let p/q is a root, we see that

$$m(\frac{p}{q}) = a_0 + a_1\frac{p}{q} + \cdots + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \left(\frac{p}{q}\right)^n = 0$$

Multiplying by q^n, we get that

$$a_0q^n + a_1pq^{n-1} + \cdots + a_{n-1}p^{n-1}q + p^n = 0$$

Collecting a q term and moving p^n to the other side, we get that

$$q(a_0q^{n-1} + a_1pq^{n-2} + \cdots + a_{n-1}p^{n-1}) = (-1)p^n$$

Since q doesn't divide p by assumption, this means that $q \mid -1$. Thus, $q = 1$ or $q = -1$, which proves that $\alpha = p/q$ was an integer all along. □

Section 13.2

Ex 1 Let $\mathbb{F}$ be a finite field of characteristic p. Prove that $|\mathbb{F}| = p^n$ for some positive integer n.

Proof. Since $\mathbb{F}$ has characteristic p, that means that it contains $\mathbb{F}_p$ as a subfield. Let n be the dimension of $\mathbb{F}$ as a vector space over $\mathbb{F}_p$. If n were infinite, then $\mathbb{F}$ would be infinite, which is a contradiction. Thus, $n < \infty$. Since n is finite, we get that $|\mathbb{F}| = |\mathbb{F}_p^n| = |\mathbb{F}_p|^n = p^n$. □

Ex 3 Determine the minimal polynomial over $\mathbb{Q}$ for the element $1 + i$.

Proof. Working backwards, we see that $x = 1 + i \implies x - 1 = i \implies (x - 1)^2 = 1 \implies (x - 1)^2 - 1 = 0$. This proves that $1 + i$ is a root of $p(x) = x^2 - 2x$. Since $1 + i \notin \mathbb{Q}$, the extension must be at least degree 2. Since $p(x)$ is of degree 2, has $1 + i$ as a root, and is monic, this proves that $x^2 - 2x$ is the minimal polynomial over $\mathbb{Q}$ for the element $1 + i$. □

Ex 4 Determine the degree over $\mathbb{Q}$ of $2 + \sqrt{3}$ and of $1 + \sqrt[3]{2} + \sqrt[3]{4}$.

Proof. Working backwards, we see that $x = 2 + \sqrt{3} \implies x - 2 = \sqrt{3} \implies (x - 2)^2 = 3 \implies (x - 2)^2 - 3 = 0$. This proves that $2 + \sqrt{3}$ is a root of $p(x) = x^2 - 4x + 1$. Since $2 + \sqrt{3} \notin \mathbb{Q}$, the extension must be at least degree 2. Since $p(x)$ is of degree 2, has $2 + \sqrt{3}$ as a root, and is monic, this proves that $x^2 - 4x + 1$ is the minimal polynomial over $\mathbb{Q}$ for the element $2 + \sqrt{3}$.

Let $\theta = 1 + \sqrt[3]{2} + \sqrt[3]{2}^2$. We see that $\theta \in \mathbb{Q}(\sqrt[3]{2})$. This proves that $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\sqrt[3]{2})$. Now, we also see that since $\theta - 1 = \sqrt[3]{2} + \sqrt[3]{4} \in \mathbb{Q}(\theta)$, we get that $(\sqrt[3]{2} + \sqrt[3]{4})^2 = \sqrt[3]{4} + 2\sqrt[3]{2}\sqrt[3]{4} + \sqrt[3]{4}^2 = \sqrt[3]{4} + 4 + 2\sqrt[3]{2}$. Subtracting this from the previous equation, we get that $4 + \sqrt[3]{2} \in \mathbb{Q}(\theta)$. Finally, this proves that $(4 + \sqrt[3]{2}) - 4 = \sqrt[3]{2} \in \mathbb{Q}(\theta)$, which proves that $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt[3]{2})$. Since $\mathbb{Q}(\sqrt[3]{2})$ is an extension of degree 3, so must $\mathbb{Q}(\theta)$. □

Ex 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. We see that $\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$, which proves that $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$. We also see that

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

which proves that $\sqrt{3}-\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Using this, we see that $(\sqrt{2}+\sqrt{3})+(\sqrt{3}-\sqrt{2}) = 2\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$, which means that $\frac{2\sqrt{2}}{2} = \sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Similarly, $\sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. This proves that $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$. We conclude that $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$.

Working backwards, we see that $x = \sqrt{2}+\sqrt{3} \implies x^2 = 2+2\sqrt{6}+3 \implies x^2-5 = 2\sqrt{6} \implies (x^2-5)^2 = 24 \implies x^4-10x^2+1 = 0$. This proves that $p(x) = x^4-10x^2+1$ is a polynomial satisfied by $\sqrt{2}+\sqrt{3}$. If $p(x)$ were reducible, then one of its factors would contain $\sqrt{2}+\sqrt{3}$ as a root, and thus the degree of the extension would be less than 4. This a contradiction, which proves that $p(x)$ is irreducible. □

Ex 10 Determine the degree of the extension $\mathbb{Q}(\sqrt{3+2\sqrt{3}})$ over $\mathbb{Q}$.

Proof. Working backwards, we see that $x = \sqrt{3+2\sqrt{3}} \implies x^2-3 = 2\sqrt{3} \implies (x^2-3)^2 = 12 \implies x^4-6x^2-3 = 0$, which means that $\sqrt{3+2\sqrt{3}}$ is the root of the polynomial x^4-6x^2-3. By the Eisenstein's Criterion for $n=3$ we see that $p(x)$ is irreducible. Since $p(x)$ is monic, this proves that it's the minimal polynomial for $\sqrt{3+2\sqrt{3}}$, which proves that the degree of the extension $\mathbb{Q}(\sqrt{3+2\sqrt{3}})$ over $\mathbb{Q}$ is 4. □

Ex 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) We can see pretty easily that $\sqrt{3+4i} = 2+i$ and that $\sqrt{3-4i} = 2-i$. Using this, we see that $\sqrt{3+4i}+\sqrt{3-4i} = 2+i+2-i = 4 \in \mathbb{Q}$. This proves that $[\mathbb{Q}(\sqrt{3+4i}+\sqrt{3-4i}) : \mathbb{Q}] = 1$.

b) We see that

$$\left(\sqrt{1+\sqrt{-3}}+\sqrt{1-\sqrt{-3}}\right)^2 = \left(1+\sqrt{-3}\right)+2\sqrt{(1+\sqrt{-3})(1-\sqrt{-3})}+(1-\sqrt{-3})$$
$$= 2+2\sqrt{1+3} = 2+2\cdot 2 = 6$$

which means that $\sqrt{1+\sqrt{-3}}+\sqrt{1-\sqrt{-3}}$ is just a fancy way of writing $\sqrt{6}$, and we know that $\mathbb{Q}(\sqrt{6})$ is an extension of degree 2 over $\mathbb{Q}$.

□

Ex 14 Prove that if $[F(\alpha) : F]$ is odd then $F(\alpha) = F(\alpha^2)$.

Proof. Since $\alpha^2 \in F(\alpha)$ and $F(\alpha^2)$ is the smallest field containing both F and α^2, we see that $F(\alpha^2) \subseteq F(\alpha)$, which gives the following hierarchy:

$$\begin{array}{c} F(\alpha) \\ | \\ F(\alpha^2) \\ | \\ F \end{array}$$

We know that $[F(\alpha) : F] = [F(\alpha) : F(\alpha^2)][F(\alpha^2) : F]$ is odd. We see that $p(x) = x^2 - \alpha^2$ is a polynomial in $F(\alpha^2)[x]$ that has α as a root. This means that $[F(\alpha) : F(\alpha^2)] \leq 2$. However, we see that $[F(\alpha) : F(\alpha^2)] \neq 2$, as we know that $[F(\alpha) : F]$ has to be odd. Thus, $[F(\alpha) : F(\alpha^2)] = 1$, which proves that $F(\alpha) = F(\alpha^2)$. □