Test II Exercise Solutions

1. Consider the field $\mathbb{Z}_{17} = \mathbb{Z}/(17)$.

   (a) Find the reciprocals $1^{-1}, 2^{-1}, \ldots, 16^{-1} \in \mathbb{Z}_{17}$.
   We find the reciprocal of any $[a] \neq [0]$ by writing $as + pt = 1$, then taking $[a]^{-1} = [s]$. For example, for 6^{-1}, we do the Euclidean Algorithm for $6, 17$:

   $$\begin{array}{r|l} 17 = 6(2) + 5 & 5 = 17 - 6(2) \\ 6 = 5(1) + 1 & 1 = 6 - 5(1) \\ & \quad = 6 - (17 - 6(2))(1) \\ & \quad = 6(3) + 17(-1) \end{array}$$

   Thus $6(3) + 17(-1) = 1 = \gcd(6, 17)$; we knew that 1 would be the gcd since $[6] \neq [0]$ so $17 \not| 6$ and the only common divisor is ± 1. Finally we have $[6][3] = [1] \in \mathbb{Z}_{17}$, and $[6]^{-1} = [3]$.

   Once we are comfortable remembering that all numbers are mod 17, we can drop the [ ] notation and just write $6^{-1} = 3 \in \mathbb{Z}_{17}$.

   (b) The squares of the elements of $\mathbb{Z}_{17}$ are:

   $$1, 4, 9, 16, 8, 2, 15, 13, 13, 15, 2, 8, 16, 9, 4, 1.$$

   The symmetry comes from the fact that $[17-a]^2 = [-a]^2 = [a]^2$.

   (c) The quadratic formula is valid in any field (or even commutative ring), so long as its features make sense: we must have field elements corresponding to $\frac{1}{2a} = (2a)^{-1}$ and $\sqrt{b^2 - 4ac}$. Here we get:

   $$\begin{aligned} x &= \tfrac{1}{2(2)} \left(-4 \pm \sqrt{4^2 - 4(2)(1)} \right) \\ &= 4^{-1} \left(-4 \pm \sqrt{8} \right) = 13(-4 \pm 5) = 13 \text{ or } 2 \end{aligned}$$

   Here we use that $4^{-1} = 13$ and $5^2 = 8$ so $\sqrt{8} = \pm 5$.

2. We construct a field K with 8 elements

   (a) There $2^3 = 8$ degree 3 polynomials in $\mathbb{Z}_2[x]$. For degree ≤ 3, any non-trivial factorization must include a linear factor, and a linear factor is equivalent to a root, so the irreducible $p(x)$ are those with no root in $\mathbb{Z}_2$: $p(x) = x^3 + x + 1$ and $x^3 + x^2 + 1$. Let us take the first of these: $p(x) = x^3 + x + 1$.
   We construct $K = \mathbb{Z}_2[x]/(x^3 + x + 1)$. The division algorithm will cut down any polynomial $f(x)$ to a remainder $r(x)$ of degree $< \deg p(x) = 3$, i.e. $r(x) = ax^2 + bx + c$, and these are the standard forms of elements. In compact notation we write $r(\alpha)$ for $[r(x)]$:

   $$K = \{0,\ 1,\ \alpha,\ \alpha{+}1,\ \alpha^2,\ \alpha^2{+}1,\ \alpha^2{+}\alpha,\ \alpha^2{+}\alpha{+}1\}$$

   Here $\alpha = [x]$, satisfying $p(\alpha) = \alpha^3 + \alpha + 1 = 0 \in K$.

(b) In pefect analogy to #1(a), we find the reciprocal of any $f(\alpha) = [f(x)] \neq [0]$ by writing $f(x)g(x) + p(x)q(x) = 1$, then taking $\frac{1}{f(\alpha)} = [f(x)]^{-1} = [g(x)] = g(\alpha)$.

For example, for $\frac{1}{\alpha^2+\alpha+1} = [x^2+x+1]^{-1}$, we do the Euclidean Algorithm for $f(x) = x^2+x+1$ and $p(x) = x^3+x+1$:

$$\begin{array}{l|l} x^3+x+1 = (x^2+x+1)(x+1) + x & x = (x^3+x+1) - (x^2+x+1)(x+1) \\ x^2+x+1 = x(x+1) + 1 & 1 = (x^2+x+1) - x(x+1) \\ & \quad = (x^2+x+1) - \big((x^3+x+1) - (x^2+x+1)(x+1) \big)(x+1) \\ & \quad = (x^2+x+1)(x^2) + (x^3+x+1)(x+1) \end{array}$$

Thus $f(x)g(x) + p(x)q(x) = 1 = \gcd(f(x), p(x))$; we knew that 1 would be the gcd since $[f(x)] \neq [0]$ so $p(x) \not| f(x)$ and the only common divisors are constants $c \neq 0$. (If the Euclidean Algorithm gives $f(x)g(x) + p(x)q(x) = c$, we just divide out to get: $f(x)(\frac{1}{c}g(x)) + p(x)(\frac{1}{c}q(x)) = 1$.)

Finally we have $[f(x)][g(x)] = [x^2+x+1][x^2] = [1] \in K$, and $\frac{1}{a^2+\alpha+1} = \alpha^2$.

To get the complete list of reciprocals, use relations like $\frac{1}{\alpha^2} = \left(\frac{1}{\alpha}\right)^2$ and the fact that, for any $\beta, \gamma \in K$, we have $(\beta+\gamma)^2 = \beta^2+2\beta\gamma+\gamma^2 = \beta^2 + \gamma^2$. It is also a fact that $\beta^7 = 1$ for any $\beta \in K$, so that $\beta^{-1} = \beta^6$.

(c) We know that $y = \alpha, \alpha^2$ are roots of $p(y)$, since $p(\alpha) = 0$ by the construction of K, and

$$\begin{aligned} p(\alpha^2) &= \alpha^6 + \alpha^2 + 1 = (\alpha^3)^2 + \alpha^2 + 1 \\ &= (\alpha+1)^2 + \alpha^2 + 1 = (\alpha^2+1) + \alpha^2 + 1 = 0. \end{aligned}$$

Dividing $(y-\alpha)$ into $p(y)$, we get $p(y) = (y-\alpha)(y^2+\alpha y+(\alpha^2+1)$. Then dividing $(y - \alpha^2)$ into the second factor, we get the full factorization:

$$p(y) = y^3 + y + 1 = (y - \alpha)(y - \alpha^2)(y - (\alpha^2+\alpha).$$

Now we have $(y-\alpha)(y-\alpha^2) = y^2+(\alpha^2+\alpha)y+(\alpha+1)$, and dividing into $p(y)$, we get:

$$p(y) = y^3 + y + 1 = (y^2 + (\alpha^2+\alpha)y + (\alpha+1))($$

(It is a general fact that if K is an extension field of $\mathbb{Z}_p$, and $f(y) \in \mathbb{Z}_p[y]$ has a root $\beta \in K$, then $\beta^2 \in K$ is also a root of $f(y)$. Thus, for the above case, the initial root α of $p(y)$ leads to the other two roots α^2 and $(\alpha^2)^2 = \alpha^2+\alpha$.)

3. We have a real number α such that $\alpha^3 + \alpha + 1 = 0$, and the ring $K = \mathbb{Q}[\alpha] = \{f(\alpha)$ for all $f(x) \in \mathbb{Q}[x]\}$.

(a) The mapping $\phi : \mathbb{Q}[x] \to K$ given by $\phi(f(x)) = f(\alpha)$ is a homomorphism since it respects addition, $\phi(f(x) + g(x)) = f(\alpha) +$

$g(\alpha) = \phi(f(x)) + \phi(g(x))$, and similarly for multiplication. The mapping is surjective since clearly all elements $f(\alpha) \in K$ are hit.

The kernel is the set of inputs with output zero:

$$\text{Ker}(\phi) = \{f(x) \in \mathbb{Q}[x] \text{ s.t. } \phi(f(x)) = f(\alpha) = 0\}.$$

Like the kernel of any homomorphism, $\text{Ker}(\phi) \subset \mathbb{Q}[x]$ is an ideal.

Now, by definition of α, it is a root of $p(x) = x^3 + x + 1$, so $\phi(p(x)) = p(\alpha) = 0$ and $p(x) \in \text{Ker}(\phi)$. Further, $\text{Ker}(\phi)$ is an ideal of $\mathbb{Q}[x]$, so by absorption we have $p(x)q(x) \in \text{Ker}(\phi)$ for any $q(x)$; indeed, $\phi(p(x)q(x)) = p(\alpha)q(\alpha) = 0$.

Therefore we have the principal ideal:

$$(p(x)) = \{p(x)q(x) \text{ for } q(x) \in \mathbb{Q}[x]\} \subset \text{Ker}(\phi).$$

Now, $p(x)$ is irreducible in $\mathbb{Q}[x]$. Any non-trivial factorization would have a linear factor, and hence a root in $\mathbb{Q}$. The Rational Root Test gives all possible candidates for such roots as $r = \pm 1$, but neither of these works, so there is no factorization.

Since $p(x)$ is irreducible, the ideal $(p(x)) \in \mathbb{Q}[x]$ is maximal: the only larger ideal is all of $\mathbb{Q}[x]$. Thus, if $\text{Ker}(\phi) \supset (p(x))$ had any elements other than $p(x)q(x)$, it would be bigger than $(p(x))$ and we would get $\text{Ker}(\phi) = \mathbb{Q}[x]$, which is clealy false: for example $\phi(1) = 1 \neq 0$. Therefore $\text{Ker}(\phi) = (p(x))$.

(b) The Isomorphism Theorem states that if $\phi : R \to S$ is a surjective homomorphism, then we have an isomorphism $S \cong R/\text{Ker}(\phi)$.

In our case, $\phi : \mathbb{Q}[x] \to K$ is surjective, since every possible output $f(\alpha) \in K$ is hit by some input, namely the polynomial $f(x) \in \mathbb{Q}[x]$. Therefore the Theorem guarantees:

$$K \cong \frac{\mathbb{Q}[x]}{\text{Ker}(\phi)} = \frac{\mathbb{Q}[x]}{(p(x))} = \frac{\mathbb{Q}[x]}{(x^3 + x + 1)}.$$

(c) Now that we know that K is a polynomial quotient ring, we can compute in it by the same techniques as in #2 above.