Name: Huize Shi - A92122910
Discussion: A04
Homework: 8

1. Prove that the following polynomials are irreducible.

   (a) $x^n - 12 \in \mathbb{Q}[x]$ if $n \geq 2$.
   Observe $x^n - 12 \in \mathbb{Z}[x]$:

$$3 \nmid 1$$
$$3 \mid 12$$
$$3^2 = 9 \nmid 12$$

   3 is a prime. By Eisenstine's Irreducibility criterion, $x^n - 12$ is irreducible in $\mathbb{Q}[x]$.

   (b) $x^3 - 3x^2 + 3x + 4 \in \mathbb{Q}[x]$
   Observe $x^3 - 3x^2 + 3x + 4 \in \mathbb{Z}[x]$. Show irreducibility in $\mathbb{Z}_7$:

$$C_7(x^3 - 3x^2 + 3x + 4) = x^3 - 3x^2 + 3x + 4$$

x	$x^3 - 3x^2 + 3x + 4$
0	4
1	5
2	6
3	5
4	4
5	6
6	4

   Since $x^3 - 3x^2 + 3x + 4$ is of degree 3, it has no zeros in $\mathbb{Z}_7$, hence it is irreducible in $\mathbb{Z}_7$. Since it is irreducible in $\mathbb{Z}_7$ and 7 is a prime, by Eisenstine's Irreducibility Criterion, $x^3 - 3x^2 + 3x + 4$ is irreducible in $\mathbb{Q}$.

   (c) Given $x^p - p + a$ is irreducible in $\mathbb{Z}_p[x]$ if p is prime and $a \in \mathbb{Z}_p \setminus \{0\}$. $x^5 - 10x^3 + 25x^2 - 51x + 2017 \in \mathbb{Q}[x]$
   Observe $x^5 - 10x^3 + 25x^2 - 51x + 2017 \in \mathbb{Z}[x]$, show $x^5 - 10x^3 + 25x^2 - 51x + 2017$ is irreducible in $\mathbb{Z}_5$:

$$C_5(x^5 - 10x^3 + 25x^2 - 51x + 2017) = x^5 - x + 2$$

   Since $2 \in \mathbb{Z}_5 \setminus \{0\}$, by criterion given we know $x^5 - 10x^3 + 25x^2 - 51x + 2017$ is irreducible in $\mathbb{Z}_5[x]$. By Eisenstine's Irreducibility Criterion, $x^5 - 10x^3 + 25x^2 - 51x + 2017$ is irreducible in $\mathbb{Q}[x]$.

(d) $x^4 + 3x^3 + 27x - 12 \in \mathbb{Q}[x]$
Observe $x^4 + 3x^3 + 27x - 12 \in \mathbb{Z}[x]$:

$$\begin{gathered} 3 \nmid 1 \\ 3 \mid 3 \\ 3 \mid 27 \\ 3 \mid -12 \\ 3^2 = 9 \nmid 12 \end{gathered}$$

Since 3 is a prime, by Eisenstine's Irreducibility Criterion, $x^4 + 3x^3 + 27x - 12$ is not reducible in $\mathbb{Q}[x]$.

(e) $x^5 - x + 1 \in \mathbb{Z}_3[x]$

$$C_3(x^5 - x + 1) = x^5 - x + 1$$

x	$x^5 - x + 1$
0	1
1	1
2	1

Hence shown $x^5 - x + 1$ has no zero in $\mathbb{Z}_3$. Check if $x^5 - x + 1$ can be factored into degeree 2 and degree 3 polynomials. We are given the only monic degree 2 polynomials in $\mathbb{Z}_3[x]$ that do not have a zero in $\mathbb{Z}_3$ are x^2+1, x^2+x-1, x^2-x-1. By polynomial long divison, we get the following:

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

Since none of the non zero degreee 2 polynomials cleanly divide $x^5 - x + 1 \in \mathbb{Z}_3[x]$, we know that $x^5 - x + 1$ is irreducible in $\mathbb{Z}_3[x]$.

(f) $x^5 + 2x + 4 \in \mathbb{Q}[x]$

$$C_3(x^5 + 2x + 4) = x^5 - x + 1$$

By part e, $x^5 + 2x + 4$ is irreducible in $\mathbb{Z}_3$, since 3 is a prime, we know that $x^5 + 2x + 4$ is irreducible in $\mathbb{Q}[x]$.

2. Prove that $\mathbb{Z}_3[x] / \langle x^5 - x + 1 \rangle$ is a field of order 3^5.
By part e, we know $x^5 - x + 1$ is irreducible in $\mathbb{Z}_3$, hence we know $\langle x^5 - x + 1 \rangle$ is maximal. Hence the factor ring $\mathbb{Z}_3[x] / \langle x^5 - x + 1 \rangle$ is a field.

Since the factor is a field there exist long division for this field.
For all $f(x) \in \mathbb{Z}_3[x]$:

$$
\begin{aligned}
f(x) &= f(x)(x^5 - x + 1) + r(x) \\
f(x) + \langle x^5 - x + 1 \rangle &= f(x)(x^5 - x + 1) + r(x) + \langle x^5 - x + 1 \rangle \\
f(x) + \langle x^5 - x + 1 \rangle &= r(x) + \langle x^5 - x + 1 \rangle
\end{aligned}
$$

This is true since $f(x)(x^5 - x + 1) \in \langle x^5 - x + 1 \rangle$, the term gets obsorbed. By long division $r(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4$ for some $a_0,\ a_1,\ a_2,\ a_3,\ a_4 \in \mathbb{Z}_4$.
Hence shown for all $f(x) + \langle x^5 - x + 1 \rangle \in {}^{\mathbb{Z}_3[x]}\!\diagup_{\langle x^5 - x + 1 \rangle}$

$$
f(x) + \langle x^5 - x + 1 \rangle = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 \mid a_0,\ a_1,\ a_2,\ a_3,\ a_4 \in \mathbb{Z}_4
$$

Since there are 5 coefficients, each has 3 choices in $\mathbb{Z}_3$ (0, 1, 2), there are 3^5 possible permutations, the order of the field is therefore 3^5.