MAT 150C, Spring 2021
Solutions to homework 5

1. Solve the equation $x^2 + 3x + 1 = 0$ in the field $\mathbb{Z}_{11}$.

Solution: We can make the following table:

x	0	1	2	3	4	5	6	7	8	9	10
x^2	0	1	4	9	5	3	3	5	9	4	1
$x^2 + 3x + 1$	1	5	0	8	7	8	0	5	1	10	10

We see that there are two roots $x = 2$ and $x = 6$ in $\mathbb{Z}_{11}$. Check:

$$(x-2)(x-6) = x^2 - 8x + 12 = x^2 + 3x + 1 \mod 11.$$

2. Solve the equation $(3 + 2\sqrt{2})x = 1$ in the field $\mathbb{Q}[\sqrt{2}]$.

Solution 1: Let $x = a + b\sqrt{2}$, then

$$(3 + 2\sqrt{2})(a + b\sqrt{2}) = (3a + 4b) + (3b + 2a)\sqrt{2},$$

We get $3a + 4b = 1,\ 3b + 2a = 0$, so $a = -\frac{3}{2}b$, and

$$3a + 4b = -\frac{9}{2}b + 4b = -\frac{1}{2}b = 1,\ b = -2, a = 3.$$

Therefore $x = 3 - 2\sqrt{2}$.

Solution 2: Recall that $(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$, so $(3 + 2\sqrt{2})(3 - 2\sqrt{2}) = 9 - 4 \cdot 2 = 1$. Therefore $x = \frac{1}{3+2\sqrt{2}} = 3 - 2\sqrt{2}$.

3. Decompose the polynomial $x^3 - 2$ into irreducible factors over the field $\mathbb{Z}_5$.

Solution: Let us find the roots of this polynomial:

x	0	1	2	3	4
x^2	0	1	4	4	1
x^3	0	1	3	2	4

Therefore $x = 3$ is a single root of this polynomial in $\mathbb{Z}_5$. Let us divide it by $(x - 3)$:

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

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

The polynomial $x^2 + 3x + 4$ has no roots in $\mathbb{Z}_5$ (any such root would be a root of $x^3 - 2$), so it is irreducible.

4. Prove that the polynomial $x^4 - 2$ is irreducible over $\mathbb{Q}$.
Solution: Let us find the roots of this polynomial. We have $x^4 = 2, x^2 = \pm\sqrt{2}$, so there are four roots $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}$ and

$$x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2}).$$

Since all the roots are not rational, we cannot factor the polynomial as a product of degree 1 and degree 3 factors. Assume we can factor it as a product of degree 2 factors, then the roots should be grouped in pairs. One of the factors contains $(x - \sqrt[4]{2})$ and we have the following cases:

1) $(x - \sqrt[4]{2})(x + \sqrt[4]{2}) = x^2 - \sqrt{2}$
2) $(x - \sqrt[4]{2})(x - i\sqrt[4]{2}) = x^2 - (i + 1)\sqrt[4]{2} + i\sqrt{2}$
3) $(x - \sqrt[4]{2})(x + i\sqrt[4]{2}) = x^2 - (-i + 1)\sqrt[4]{2} - i\sqrt{2}$

In all these cases the coefficients of the degree 2 polynomial are not rational, contradiction. Therefore the original polynomial is irreducible.