# MAT 148, Winter 2016
# Solutions to HW 5

1. Using the definition of a field, show that $a \cdot 0 = 0 \cdot a = 0$ for all elements $a$ in a field.

**Solution:** Let us write $1 = 1 + 0$, then

$$a = a \cdot 1 = a \cdot (1 + 0) = a \cdot 1 + a \cdot 0 = a + a \cdot 0.$$

If we add $(-a)$ to both sides, we get

$$0 = (-a) + a = (-a) + (a + a \cdot 0) = ((-a) + a) + a \cdot 0 = 0 + a \cdot 0 = a \cdot 0.$$

4. Find the greatest common divisor of the following pairs of binary (that is, with coefficients in $\mathbb{Z}_2$) polynomials: (a) $x + 1$ and $x^3 + 1$; (b) $x + 1$ and $x^4 + 1$.

**Solution:** One has $x^3 + 1 = (x + 1)(x^2 - x + 1)$, so $x + 1$ divides $x^3 + 1$ and $GCD(x + 1, x^3 + 1) = x + 1$. Similarly, $x^4 + 1 = (x^2 + 1)^2 = (x + 1)^4 \mod 2$, so $GCD(x + 1, x^4 + 1) = x + 1$.

7. List all binary irreducible polynomials of degrees less than or equal to 5.

**Solution:** Remark that a polynomial $f(x)$ is divisible by $x$ if and only if $f(0) = 0$, so the constant term of $f(x)$ equals 0. Similarly, $f(x)$ is divisible by $x + 1$ if and only if $f(1) = 0 \mod 2$, so $f(x)$ has even number of terms. In both cases $f(x)$ is reducible unless it has degree 1, so an irreducible polynomial of degree 2 or higher should have constant term 1 and odd number of terms.

Furthermore, a polynomial of degree 2 or 3 is reducible if and only if it has a linear factor, so it is divisible by $x$ or by $x + 1$. Therefore there is one irreducible polynomial of degree 2: $x^2 + x + 1$, and two irreducible polynomials of degree 3: $x^3 + x + 1, x^3 + x^2 + 1$.

A polynomial of degree 4 or 5 is reducible if and only if it has a linear factor or it can be presented as a product of two irreducible polynomials of degrees 2 or 3:

$$(x^2 + x + 1)^2 = x^4 + x^2 + 1,\ (x^2 + x + 1)(x^3 + x + 1) = x^5 + x^4 + 1,$$

$$(x^2 + x + 1)(x^3 + x^2 + 1) = x^5 + x + 1.$$

All other polynomials are irreducible, so there are 3 irreducible polynomials of degree 4:

$$x^4 + x + 1, x^4 + x^3 + 1, x^4 + x^3 + x^2 + x + 1$$

and 6 irreducible polynomials of degree 5:

$$x^5 + x^2 + 1, x^5 + x^3 + 1, x^5 + x^3 + x^2 + x + 1,$$

$$x^5 + x^4 + x^2 + x + 1, x^5 + x^4 + x^3 + x + 1, x^5 + x^4 + x^3 + 2 + 1.$$

13. If $a(x)$ is a binary polynomial, prove that $(a(x))^2 = a(x^2) \mod 2$.

**Solution:** Let $a(x) = a_n x^n + \ldots + a_0$, then

$$a(x)^2 = a_n^2 x^{2n} + \ldots + a_0^2 + 2 \sum_{i,j} a_i a_j x^{i+j} = a_n^2 x^{2n} + \ldots + a_0^2 \mod 2.$$

Since $0^2 = 0$ and $1^2 = 1$, one has $a_i^2 = a_i \mod 2$, and

$$a(x)^2 = a_n^2 x^{2n} + \ldots + a_0^2 = a_n x^{2n} + \ldots + a_0 = a(x^2) \mod 2.$$