INF 240 - Exercise problems - 5

Nikolay Kaleyski

1 Finding irreducible polynomials

Recall that a polynomial $f(x)$ is called *irreducible* if it cannot be written as a product $f(x) = g(x)h(x)$ of two polynomials $g(x)$ and $h(x)$ with both $\deg(g) < \deg(f)$ and $\deg(h) < \deg(f)$. For example, the polynomial $(x^2 - 1)$ over $\mathbb{R}$ is not irreducible, since it can be decomposed as $(x^2 - 1) = (x + 1)(x - 1)$. On the other hand, the polynomial $(x^2 + 1)$ over $\mathbb{R}$ is indeed irreducible; note that we can write, e.g. $(x^2 + 1) = g(x)h(x)$ for $g(x) = \frac{1}{2}x^2 + \frac{1}{2}$ and $h(x) = 2$, but in this case $\deg(g) = \deg(f)$ (and, by definition, we must be able to find $g(x)$ and $h(x)$ which both have degrees less than that of $f(x)$ in order for $f(x)$ to be reducible).

Irreducible polynomials are very useful for a number of reason, one of which is that they can be used to construct finite fields. Recall that the quotient ring $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible. Thus, being able to find irreducible polynomials is an important problem of practical significance.

In general, it is easy to show that a polynomial $f(x)$ is reducible, since all that is required is to find a concrete decomposition of $f(x)$ into $f(x) = g(x)h(x)$. On the other hand, showing that a polynomial is *not* irreducible is hard; with the exception of some special cases, the only approach that can be used to verify that a given $f(x)$ is irreducible, is to go over all polynomials of degree lower than that of $f(x)$ and to check that they do not divide $f(x)$. In the same vein, one can find *all* irreducible polynomials of a certain degree n by first writing down all polynomials of degree n, then computing the products of each pair of polynomials $g(x)$ and $h(x)$ with $\deg(g) + \deg(h) = n$ and removing them from the list.

In the following exercise, we will find all irreducible polynomials of degree 2 in $\mathbb{F}_3[x]$ using this method. Note that multiplying a polynomial by a constant does not change whether it is reducible or not, so we can assume that all polynomials are monic without losing any information.

Exercise 1. *Consider the finite field $\mathbb{F}_3$ and the univariate polynomial ring $\mathbb{F}_3[x]$ over it.*

1. *Write down all **monic** polynomials of degree 2 in $\mathbb{F}_3[x]$; there should be nine of these.*

2. *Write down all **monic** polynomials of degree 1 in $\mathbb{F}_3[x]$; there should be only three of these. If some polynomial from the "degree 2" list is reducible, it must be the product of two polynomials from the "degree 1" list.*

3. *Consider every pair of polynomials from the "degree 1" list (there should be 9 of these) and compute their product; remove this product from the list*

of "degree 2" polynomials.

4. *The remaining degree 2 polynomials should be precisely all irreducible polynomials of degree* 2 *in* $\mathbb{F}_3[x]$.

NB: In the above example, we only considered products of polynomials of degree 1 because we were looking for irreducible polynomials of degree 2, and the only possible decomposition is $2 = 1 + 1$. If we were looking for irreducible polynomials of degree 4 instead, we would have to consider the decompositions $4 = 3 + 1$ and $4 = 2 + 2$, so we would consider all products of a polynomial of degree 3 with a polynomial of degree 1, and all products of two polynomials of degree 2.

A special case in which irreducibility can be shown without resorting to this "brute force" approach is when the degree of $f(x)$ is 2 or 3. Recall that some $a \in \mathbb{F}$ is a root of a polynomial $f(x)$ in $\mathbb{F}[x]$ if and only if $(x - a)$ divides $f(x)$. Since degree 2 can only decompose as $2 = 1 + 1$ and 3 can only decompose as $3 = 2+1$ (or $3 = 1+2$, which is the same), if $f(x)$ is reducible and $\deg(f) \leq 3$, then $f(x)$ must have a polynomial of degree 1 as a divisor; and, consequently, $f(x)$ must have a root. Therefore, to check whether a given polynomial $f(x)$ with $\deg(f) \leq 3$ is irreducible, it is enough to check that it has no roots, i.e. to go through every element $a \in \mathbb{F}$ and show that $f(a) \neq 0$.

Exercise 2. *By finding all roots of the following polynomials, decide which of them are reducible and which are irreducible in* $\mathbb{F}_3[x]$*:*

- $f_1(x) = x^3 + 2x^2 + 2x + 2$*;*
- $f_2(x) = x^3 + x^2 + 2x + 2$*;*
- $f_3(x) = x^3 + x + 2$*;*
- $f_4(x) = x^3 + 2x + 1$.

NB: When $\deg(f) \geq 4$, this "root method" only provides a necessary (and not a sufficient) condition for a polynomial to be irreducible. For example, a polynomial of degree 4 might have no divisors of degree 1 (and hence no roots), but may decompose as $4 = 2 + 2$.

2 Construction of finite fields

As mentioned in the previous section, one particularly useful application of irreducible polynomials is the construction of extensions of finite fields. Starting with a finite field $\mathbb{F}$, one finds an irreducible polynomial $f(x)$ in $\mathbb{F}[x]$, and constructs the quotient ring $\mathbb{F}[x]/(f(x))$; we know that since $f(x)$ is irreducible, the resulting structure will not only be a ring, but a finite field itself. Intuitively, the elements of the newly constructed finite field correspond to the possible remainders of division by $f(x)$; in particular, they can be identified with all polynomials in $\mathbb{F}[x]$ of degree strictly less than $\deg(f)$. Since the elements of $\mathbb{F}$ can be interpreted as constant polynomials, and since dividing any constant polynomial $c(x)$ by $f(x)$ always leaves $c(x)$ as remainder, the elements of $\mathbb{F}$ are contained in $\mathbb{F}[x]/(f(x))$, so that $\mathbb{F}$ is a *subfield* of $\mathbb{F}[x]/(f(x))$ or, equivalently, $\mathbb{F}[x]/(f(x))$ is an *extension field* of $\mathbb{F}$.

Exercise 3. *Consider the polynomial ring* $\mathbb{F}_3[x]$*, and the irreducible polynomials of degree* 2 *from Exercise 1. Take* $f(x)$ *to be one of these irreducible polynomials (say, the one with the smallest number of terms, although any choice of a polynomial will work as long as it is irreducible). Construct the quotient ring* $\mathbb{F}_3[x]/(f(x))$*, i.e. list all of its elements, and explain how addition and multiplication are performed in it. Is there a correlation between the degree of* $f(x)$ *and the number of elements of* $\mathbb{F}_3[x]/(f(x))$*?*

Exercise 4. *Consider the elements* $[x+2]$ *and* $[2x+1]$ *of* $\mathbb{F}[x]/(f(x))$*. Compute their sum and their product in* $\mathbb{F}[x]/(f(x))$*. Find their additive and multiplicative inverses in* $\mathbb{F}[x]/(f(x))$*.*

Exercise 5. *Consider the polynomials* $x^5 + 2x^3 + 1$ *and* $x^4 + x^2 + x + 1$*. Which elements of* $\mathbb{F}[x]/(f(x))$ *do they correspond to?*