.1 Irreducibility of polynomials

Problem .1.1. Let $f(x) \in \mathbb{C}[x]$. Prove that $a \in \mathbb{C}$ is a root of f with multiplicity r if and only if $f(a) = f'(a) = \cdots = f^{(r-1)}(a) = 0$ and $f^{(r)}(a) \neq 0$, where $f^{(k)}(a)$ denotes the value of the k-th derivative of f at a. Deduce that $f(x) \in \mathbb{C}[x]$ has multiple roots if and only if $\gcd(f(x), f'(x)) \neq 1$.

Solution. First suppose that $f(a) = f'(a) = \cdots = f^{(r-1)}(a) = 0$ and $f^{(r)}(a) \neq 0$. Then $(x-a)^{(r)} \mid f(x)$. If $(x-a)^{(r+1)} \mid f(x)$, then repeated differentiation shows that $(x-a) \mid f^{(r)}(x)$ which we know not to be true. Thus, r is the highest power of $(x-a)$ dividing f, showing that a is a root with multiplicity r. For the other direction, suppose a is a root of f with multiplicity r. Then $(x-a)^r \mid f$. Repeatedly differentiation shows that $(x-a) \mid f^{(i)}$ for $0 \leq i < r$. Furthermore, since $(x-a) \nmid f^{(r)}$, we have $f(a) \neq 0$.

Now let $f(x) \in \mathbb{C}[x]$ with multiple roots (that is, roots with multiplicity > 1). If a is a multiple root of f, then $(x-a) \mid f$. Furthermore, we can write $f = (x-a) \cdot g$. Since a is a multiple root, we also have $(x-a) \mid g$. That is, we can write $g = (x-a) \cdot h$. But then we have

$$f'(x) = g(x) + (x-a) \cdot g'(x) = (x-a) \cdot h + (x-a) \cdot g'$$

That is, $\gcd(f, f') \neq 1$ since $(x-a)$ divides both. To prove the reverse direction, suppose all roots of f are simple. Then $f = (x-a_1)(x-a_2)\cdots(x-a_n)$. Taking the derivative shows that the two have no common factors so $\gcd(f, f') = 1$. The contrapositive yields the desired statement. □

Problem .1.2. Let F be a subfield of $\mathbb{C}$, and let $f(x)$ be an irreducible polynomial in $F[x]$. Prove that $f(x)$ has no multiple roots in $\mathbb{C}$. (Use Exercises 2.22 and 5.1).

Solution. Suppose $f(x)$ is irreducible in $F[x]$. In particular, $\gcd(f, f') = 1$ in $F[x]$. By Exercise 2.22, $\gcd(f, f') = 1$ in $\mathbb{C}[x]$ as well. But then Exercise 5.1 shows that $f(x)$ has no multiple roots. □

Problem .1.3. Let R be a ring, and let $f(x) = a_{2n}x^{2n} + a_{2n-2}x^{2n-2} + \cdots + a_2x^2 + a_0 \in R[x]$ be a polynomial only involving *even* powers of x. Prove that if $g(x)$ is a factor of $f(x)$, so is $g(-x)$.

Solution. Suppose $g(x)$ is a factor of $f(x)$. That is, $f(x) = g(x) \cdot h(x)$. But then

$$f(x) = f(-x) = g(-x) \cdot h(-x)$$

where the first equality follows from the fact that $(-1)^2 = 1$. Thus, $g(-x)$ also divides f. □

Problem .1.4. Show that $x^4 + x^2 + 1$ is reducible in $\mathbb{Z}[x]$. Prove that it has *no* rational roots, without finding its (complex) roots.

Solution. Clearly we have

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

so it is reducible in $\mathbb{Z}[x]$. To see that it has no rational roots, we use the rational roots test. The only potential rational roots are ± 1, and it is easily checked that neither are roots. Thus, its roots are not rational. □

Problem .1.5. Prove Proposition 5.3.

Proposition 5.3. *Let k be a field. A polynomial $f \in k[x]$ of degree 2 or 3 is irreducible if and only if it has no roots.*

Solution. Let f be a polynomial of degree 2 or 3. If f has a root a, then clearly $(x - a) \mid f$ so f is reducible. The contrapositive yields the statement that if f is irreducible then it has no roots. Now suppose f is reducible. If f has degree 2 then its nontrivial factor must be linear of the form $(x - a)$, making a a root of f. If f has degree 3, then it has a nontrivial factor which is either linear or quadratic. If it is linear then it is a root by the above reasoning. If it is quadratic, then the remaining factor is linear so there is a corresponding root. Thus, we have shown that if f has no roots then it is irreducible. □

Problem .1.6. Construct fields with 27 elements and with 121 elements.

Solution. Let $\mathbb{Z}_3$ denote the field with 3 elements and consider the ring $\mathbb{Z}_3[x]$. Consider the polynomial $f(x) = x^3 + 2x + 1$. It can be easily observed that $f(x)$ has no roots in $\mathbb{Z}_3$ and thus is irreducible. Then we can consider the field

$$F := \frac{\mathbb{Z}_3[x]}{x^3 + 2x + 1}.$$

It can be seen to have 27 elements by noting that its elements are quadratic polynomials. That is, each polynomial has three coefficients, and there are three possibilites for each (namely, the elements of $\mathbb{Z}_3$).

Now let $\mathbb{Z}_1 1$ denote the field with 11 elements. Consider the polynomial $f(x) = x^2 + 1$ which has no roots in this field. Then the field

$$F := \frac{\mathbb{Z}_{11}[x]}{x^2 + 1}$$

has elements which are linear polynomials. There are two coefficients in each polynomial and 11 possibilities for each, leading to a total of $11^2 = 121$ elements in this field. □

Problem .1.7. Let R be an integral domain, and let $f(x) \in R[x]$ be a polynomial of degree d. Prove that $f(x)$ is determined by its value at any $d+1$ distinct elements of R.

Solution. Let $g \in R[x]$ be a polynomial of degree d which agrees with f at $d+1$ distinct points. That is, $f(a_1) = g(a_1), \ldots, f(a_{d+1}) = g(a_{d+1})$. Since R is an integral domain, if $f - g$ is nonzero, then it must have degree less than d. Now consider $f - g = c(x - a_1) \cdots (x - a_{d+1})$. We find that $f - g$ has degree $d+1 > d$. Therefore, $f - g = 0$ so $f = g$. □

Problem .1.8. Let K be a field and let $a_0, \ldots, a_d$ be distinct elements of K. Given any elements $b_0, \ldots, b_d$ in K, construct explicitly a polynomial $f(x) \in K[x]$ of degree at most d such that $f(a_0) = b_0, \ldots, f(a_d) = b_d$, and show that this polynomial is unique. (Hint: First solve the problem assuming that only one b_i is not equal to zero.) This process is called *Lagrange interpolation.*

Solution. To do. □

Problem .1.9. Pretend you can factor integers, and then use Lagrange interpolation (cf. Exercise 5.8) to give a finite algorithm to factor *polynomials* with integer coefficients over $\mathbb{Q}[x]$. Use your algorithm to factor $(x-1)(x-2)(x-3)(x-4)+1$.

Solution. To do. □

Problem .1.10. Prove that the polynomial $(x-1)(x-2)\cdots(x-n)-1$ is irreducible in $\mathbb{Q}[x]$ for all $n \geq 1$. (Hint: Think along the lines of Exercise 5.9.)

Solution. To do. □