.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. Consider the polynomial

$$\ell_j(x) = \prod_{\substack{0 \leq i \leq d \\ i \neq j}} \frac{x - a_i}{a_j - a_i}.$$

Then we may define the Lagrange polynomial as

$$L(x) = \sum_{j=0}^{k} b_j \ell_j.$$

Clearly this polynomial satisfies the desired properties. Uniqueness can be verified in a similar manner to the previous problem. □

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. Consider a polynomial $p(x) \in \mathbb{Z}[x]$ of degree d. We can evaluate it at d points, say $p(a_1) = b_1, \ldots, p(a_d) = b_d$. Now factor each b_i over $\mathbb{Z}$. From here, we can use Lagrange Interpolation to construct a polynomial $q(x) \in \mathbb{Q}[x]$ such that $q(a_i) = c_i$ for some factor c_i of b_i. Finally, one may check if $q(x)$ divides p via polynomial division. The key observation is that if q has degree less than d, then it is uniquely determined by the choice of c_i. As a result, there are only finiely many choices for q.

Applying the algorithm to the given polynomial is incredibly tedious but ultimately yields a factorizaiton of $(-x^2 + 5x - 5)^2$. □

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. Note that $f(x) = (x-1)(x-2)\cdots(x-n)-1$ is monic. Suppose $f = gh$ has a nontrivial factorization into two monic polynomials of strictly lower degrees. Then, for $1 \leq k \leq n$, we have $f(k) = g(k)h(k) = -1$ so $g(k), h(k) = \pm 1$ and we must have $g(k) = -h(k)$. Now consider the polynomial $p(x) = g(x) + h(x)$. Clearly p has strictly lower degree than f since we are working over an integral domain. However, $p(k) = 0$ for all $1 \leq k \leq n$ so necessarily $f = -g$, a contradiction since we assumed that f and g were both monic. Thus, f must be irreducible. □

Problem .1.11. Let F be a finite field. Prove that there are irreducible polynomials in $F[x]$ of arbitrarily high degree. (Hint: Exercise 2.24.)

Solution. Suppose otherwise. That is, suppose there are only finitely many irreducible polynomials in $F[x]$, say $p_1(x), \ldots, p_n(x)$. Consider the polynomial $f(x) = p_1(x)\cdots p_n(x) + 1$. By assumption, $f(x)$ is not irreducible so it is divisibly by one of our irreducible polynomials, say $p_i(x)$. But then $p_i(x)$ divides 1, a contradiction. Therefore, there must be infinitely many irreducible polynomials and they are necessarily of arbitrarily high degree since there are only finitely many polynomials of a fixed degree. □

Problem .1.12. Prove that applying the construction in Proposition 5.7 to an irreducible *linear* polynomial in $k[x]$ produces a field isomorphic to k.

Solution. Let f be an irreducible linear polynomial in $k[x]$ and define

$$F = \frac{k[x]}{(f(x))}.$$

Consider the valuation function which sends $g(x) \to g(0) \in F$ (recall that F can be seen as an extension of k). Clearly this mapping preserves sums and products so it suffices to check what the kernel is. The kernel is the set of polynomials such that $g(0) \in (f(x))$. However, note that the valuation functions maps to a constant and the only constant in this ideal is 0. Thus, the kernel is the set of polynomials such that $g(0) = 0$, but this is only the case if $g = 0$ or g has no constant term. Therefore, the kernel is the ideal (x). By the First Isomorphism Theorem, we find

$$F \cong \frac{k[x]}{(x)} \cong k,$$

showing the fields are isomorphic. □

Problem .1.13. Let k be a field, and let $f \in k[x]$ be any polynomial. Prove that there is an extension $k \subseteq F$ in which f factors completely as a product of linear terms.

Solution. We can factor f into a product of irreducibles since $k[x]$ is a UFD. For each irreducible element $g_i(t)$ in the factorization of f, we can consider the quotient

$$F_i := \frac{k[t]}{(g_i(t))}$$

where F_i is an extension of k containing a root of $g_i(t)$. Repeating this process for each irreducible factor of f yields a field extension F in which f factors completely. □

Problem .1.14. How many different embeddings of the field $\mathbb{Q}[t]/(t^3 - 2)$ are there in $\mathbb{R}$? How many in $\mathbb{C}$?

Solution. There is only one embedding of the field in $\mathbb{R}$, namely $\mathbb{Q}[\sqrt[3]{2}]$. This is because there is only one cube root of 2 in $\mathbb{R}$. However, the field $\mathbb{C}$ contains the roots of unity, solutions to the equation $x^n - 1 = 0$. Thus, there are three embeddings of the field in $\mathbb{C}$, namely $\mathbb{Q}[\sqrt[3]{2}], \mathbb{Q}[\zeta\sqrt[3]{2}], \mathbb{Q}[\zeta^2\sqrt[3]{2}]$, where $\zeta^3 = 1$. □

Problem .1.15. Prove Lemma 5.10.

Lemma 5.10. *A field k is algebraically closed if and only if every polynomial $f \in k[x]$ factors completely as a product of linear factors, if and only if every nonconstant polynomial $f \in k[x]$ has a root in k.*

Solution. Suppose k is algebraically closed. That is, every irreducible polynomial has degree 1. Since $k[x]$ is a UFD, every polynomial $f \in k[x]$ factors into irreducibles and thus factors into linear polynomials.

Now suppose that every polynomial $f \in k[x]$ factors completely as a product of linear factors. Then every polynomial has at least one factor of the form $(x-a)$, which occurs if and only if a is a root of f. Therefore, every polynomial has a root in k.

Finally, suppose that every nonconstant polynomial $f \in k[x]$ has a root in k and consider an irreducible polynomial f. Suppose f has degree greater than 1. Since f has a root a, we can factor out a linear polynomial $(x-a)$, contradicting that f is irreducible. Thus f has degree 1 so k is algebraically closed. □

Problem .1.16. If you know about the 'maximum modulus principle' in complex analysis: formulate and prove the 'mimimum modulus princile' used in the sketch of the proof of the fundamental theorem of algebra.

Solution. I do not know complex analysis. □

Problem .1.17. Let $f \in \mathbb{R}[x]$ be a polynomial of *odd* degree. Use the intermediate value theorem to give an 'algebra-free' proof of the fact that f has real roots.

Solution. We have $\lim_{x\to+\infty} f(x) = +\infty$ and $\lim_{x\to-\infty} f(x) = -\infty$. In particular, for some a, $f(a) < 0$ and for some b, $f(b) > 0$. Since f is a polynomial, it is continuous over $[a, b]$. Thus, the intermediate value theorem applies and there exists some $c \in [a, b]$ such that $f(c) = 0$. That is, c is a real root of f. □

Problem .1.18. Let $f \in \mathbb{Z}[x]$ be a cubic polynomial such that $f(0)$ and $f(1)$ are odd and with odd leading coefficient. Prove that f is irreducible in $\mathbb{Q}[x]$.

Solution. Suppose f is reducible. Then it must have a linear factor. However, consider that $x \equiv y \pmod{n} \implies f(x) \equiv f(y) \pmod{n}$. In particular, for any integer x, if $x \equiv 0 \pmod 2$ then $f(x) \equiv 0 \pmod 2$. Similarly, if $x \equiv 1 \pmod 2$ then $f(x) \equiv 1 \pmod 2$. Since $0 \equiv 0 \pmod 2$, it is clear that no integer x is a root of f. Thus, f is irreducible over $\mathbb{Z}[x]$ and hence over $\mathbb{Q}[x]$. □

Problem .1.19. Give a proof of the fact that $\sqrt{2}$ is not rational by using Eisenstein's criterion.

Solution. Suppose $\sqrt{2} \in \mathbb{Q}$. Then $(x + \sqrt{2})(x - \sqrt{2}) = x^2 - 2$ is reducible in $\mathbb{Z}[x]$. However, consider the prime ideal $\mathfrak{p} = (2)$. Since $1 \notin (2)$ and $2 \notin (2)^2$, Eisenstein's criterion applies and the polynomial is irreducible in $\mathbb{Z}[x]$. Thus, it must be the case that $\sqrt{2} \notin \mathbb{Q}$. □

Problem .1.20. Prove that $x^6 + 4x^3 + 1$ is irreducible by using Eisenstein's criterion.

Solution. Note that there is no prime p which divides 1 so Eisenstein's criterion does not apply to this specific polynomial. However, we can make the substitution $x = y+1$ which yields the polynomial $y^6+6y^5+15y^4+24y^3+27y^2+18y+6$. Note that this polynomial *does* satisfy Eisenstein's criterion with the prime ideal $\mathfrak{p} = (3)$. That is, the polynomial after transformation is irreducible in the ring $\mathbb{Q}[y+1]$. However, this ring is isomorphic to $\mathbb{Q}[x]$. Thus, the original polynomial is also irreducible. □

Problem .1.21. Prove that $1 + x + x^2 + \cdots + x^{n-1}$ is reducible over $\mathbb{Z}$ if n is *not* prime.

Solution. Suppose n is not prime so it can be written as $n = pq$. Recall that we have

$$1 + x + x^2 + \cdots + x^{n-1} = \frac{x^n - 1}{x - 1} = \frac{x^{pq} - 1}{x - 1}.$$

However, we find that

$$\frac{(x^p)^q - 1}{x^p - 1} = 1 + x^p + x^{2p} + \cdots + x^{(q-1)p}$$

which yields the factorization

$$\frac{x^n - 1}{x - 1} = \frac{x^n - 1}{x^p - 1} \cdot \frac{x^q - 1}{x - 1}.$$

Thus, the polynomial is reducible over $\mathbb{Z}[x]$. □

Problem .1.22. Let R be a UFD, and let $a \in R$ be an element that is not divisible by the square of some irreducible element in its factorization. Prove that $x^n - a$ is irreducible for every integer $n \geq 1$.

Solution. Let q denote an irreducible element whose square does not divide a. Since R is a UFD, q is also prime. Then we have $1 \notin (q)$ and $a \notin (q)^2$. Therefore, Eisenstein's criterion applies and the polynomial is irreducible for all $n \geq 1$. □

Problem .1.23. Decide whether $y^5 + x^2y^3 + x^3y^2 + x$ is reducible or irreducible in $\mathbb{C}[x, y]$.

Solution. Consider the ideal $\mathfrak{p} = (x)$. Certainly this is a prime ideal since modding out the ideal yields the ring $\mathbb{C}[y]$ which is an integral domain. Furthermore, we have $1 \notin (x)$, $x^2y^3 \in (x)$, $x^3y^2 \in (x)$, and $x \notin (x)^2$. Thus, we may apply Eisenstein's criterion and conclude that the polynomial is irreducible in $\mathbb{C}[x, y]$. □