5. (a) Show that the polynomials X^4+1 and X^6+X^3+1 are irreducible over the rational numbers.

Proof. It suffices to show that $f(X+1)$ is irreducible. For if $f(X)=g(X)h(X)$ with $\deg g \geq 1$ or $\deg h \geq 1$, then we would have $f(X+1)=g(X+1)h(X+1)$, and this transformation has preserved the degrees of g and h. Since $f(X+1)=X^4+4X^3+6X^2+4X+2$, applying Eisenstein's Criterion with $p=2$ suffices.

Applying the same logic to $f(X)=X^6+X^3+1$, we have $f(X+1)=X^6+6X^5+15X^4+21X^3+18X^2+9X+3$, so $p=3$ satisfies Eisenstein's Criterion. □

(c) Show that the polynomial in two variables X^2+Y^2-1 is irreducible over the rational numbers. Is it irreducible over the complex numbers?

Proof. Consider the polynomial as an element of $\mathbf{Z}[X][Y]$. Its image under the homomorphism $Y \mapsto 2$ is X^2+3, which is nonzero and of the same degree. By Eisenstein's Criterion, X^2+3 is irreducible over $\mathbf{Q}$, thus the original polynomial was irreducible over $\mathbf{Z}[X]$. So it is also irreducible over $\mathbf{Q}$.

Suppose that $f(X,Y)=X^2+Y^2-1$ were reducible over $\mathbf{C}$. Then $f=gh$ for some $g,h \in \mathbf{C}[X,Y]$, where neither of g or h is a unit. The units of $\mathbf{C}[X,Y]$ are just the constant polynomials, so neither g nor h is constant. It must then be that g and h both have degree 1 when considered as polynomials WLOG in Y over $\mathbf{C}[X]$. So we have a factorization

$$Y^2+(X^2-1)=(Y+p(X))(Y-p(X))$$

for some $p(X) \in \mathbf{C}[X]$ such that $p(X)^2=X^2-1$. (Write $Y^2+(X^2-1)=(Y+a(X))(Y+b(X))$, since we may assume the coefficients of Y are 1. Expanding shows the factorization must take this form.) $\mathbf{C}$ is factorial, so the only factorization of X^2-1 is $(X+1)(X-1)$ (modulo units and permutation), hence no such $p(X)$ can exist. So f must be irreducible over $\mathbf{C}$. □

7. (a) Let k be a finite field with $q=p^m$ elements. let $f(X_1,\ldots,X_n)$ be a polynomial in $k[X]$ of degree d and assume $f(0,\ldots,0)=0$. An element $(a_1,\ldots,a_n)\in k^{(n)}$ such that $f(a)=0$ is called a zero of f. If $n>d$, show that f has at least one other zero in $k^{(n)}$.

Proof. Consider the polynomials $F(X)=1-f(X)^{q-1}$ and $G(X)=\prod_i(1-X_i^{q-1})$, which have degrees $d(q-1)$ and $n(q-1)$, respectively. These both induce the indicator function that is 1 at $x=0$ and 0 elsewhere. Let $\overline{F}(X)$ be the reduced polynomial belonging to $F(X)$. Then the degree of $\overline{F}(X)-G(X)$ in each variable is $<q$ and this polynomial induces the 0 function on $k^{(n)}$. Thus, $\overline{F}(X)=G(X)$. Since $\overline{F}(X)$ is the reduced version of $F(X)$, we have $n(q-1)=\deg G=\deg\overline{F}\leq \deg F=d(q-1)$. Since $q\geq 2$, this contradicts that $n>d$. □

(b) Refine the above results by proving that the number N of zeros of f in $k^{(n)}$ is $\equiv 0 \pmod p$.

Proof. Define a function on the nonnegative integers by $\psi(i)=\sum\limits_{x\in k} x^i$. Clearly, $\psi(0)=0$, so assume $i>0$. If $q-1 \mid i$ then we have

$$\psi(i)=0+\sum_{x\in k, x\neq 0} x^{i \pmod{q-1}}=0+\sum_{x\in k,x\neq 0}1=q-1=-1.$$

Otherwise, $i>0$. So some g is a generator of $k^\times$, hence $g^i\neq 1$ and multiplication by g is an isomorphism on k, so

$$\psi(i)=\sum_{x\in k}x^i=\sum_{x\in k}(gx)^i=g^i\psi(i)$$

therefore $\psi(i)=0$ (since $g^i\neq 1$). Now, define $\Psi(i_1,\ldots,i_n)=\sum\limits_{x\in k^{(n)}} x_1^{i_1}\cdots x_n^{i_n}$. Then by induction we have

$$\Psi(i_1,\ldots,i_n)=\sum_{x_n\in k}x_n^{i_n}\left(\sum_{x_1\in k}\cdots\sum_{x_{n-1}\in k}x_1^{i_1}\cdots x_{n-1}^{i_{n-1}}\right)$$

$$= \sum_{x_n \in k} x_n^{i_n} \psi(i_1) \cdots \psi(i_{n-1}) = \psi(i_1) \cdots \psi(i_n).$$

The number N of zeros (mod p) that $f(x)$ has in $k^{(n)}$ can be expressed as $N = \sum\limits_{x \in k^{(n)}} (1 - f(x)^{q-1})$. This is because a given term is 1 if $f(x) = 0$ and 0 otherwise, and adding 1s and 0s in k amounts to adding them in its prime subfield $\mathbf{Z}_p$. $1 - f(x)^{q-1}$ is a sum of terms of the form $a_i x_1^{i_1} \cdots x_n^{i_n}$ with $\sum\limits_j i_j \le d(q-1) < n(q-1)$. Thus, each term in $\sum\limits_{x \in k^{(n)}} 1 - f(x)^{q-1}$ contains a factor of $\Psi(i_1, \dots, i_n)$, and furthermore some $i_j < q-1$. Therefore, since either $i_j = 0$ or $q-1 \nmid i_j$ for this j, we know $\psi(i_j) = 0$ and thus, by the result of the last paragraph, the whole term is 0. So this entire sum is 0, meaning $p \mid N$. $\square$

(c) Extend Chevalley's theorem to r polynomials $f_1, \dots, f_r$ of degrees $d_1, \dots, d_r$ respectively, in n variables. If they have no constant term and $n > \sum d_i$, show that they have a non-trivial common zero.

Proof. Suppose the sum of the degrees is less than n. Then the number N of common zeros is congruent to $\prod(1 - f_i(x)^{q-1}) \pmod p$, since x is a common zero if and only if every factor equals 1. We also have

$$\deg \prod (1 - f_i(X)^{q-1}) = \sum_1^r \deg f_i(X)^{q-1} = (q-1) \sum_1^r d_i < n(q-1)$$

therefore every term contains some variable to a power less than $q-1$, so the entire sum is 0. Thus $p \mid N$.

If every polynomial has no constant term, then 0 is a common zero. But 1 is not divisible by any prime, so there must be another zero, which is then non-trivial. $\square$

(d) Show that an arbitrary function $f : k^{(n)} \to k$ can be represented by a polynomial. (As before, k is a finite field.)

Proof. Recall that every polynomial over k has a unique reduced polynomial which gives the same function. Since the multiplicative group of nonzero elements of k is cyclic of order $q-1$, we know that X^v agrees, as a function, with $X^{v \pmod{q-1}}$ as long as $v \ne q-1$. If $v = q-1$, then the two functions agree everywhere except for at 0, however this single point distinguishes them. So a set of representatives for the distinct polynomial functions on $k^{(n)}$ is the set of polynomials whose degree d in each variable satisfies $0 \le d \le q-1$ (by Corollary 1.8, we know that no two of these polynomials give the same function).

This means that there are q^{q^n} distinct polynomial functions $k^{(n)} \to k$. This is also the number of functions $k^{(n)} \to k$. So each of these functions must be given by exactly one of these polynomials. $\square$

8. Let A be a commutative entire ring and X a variable over A. Let $a, b \in A$ and assume that a is a unit in A. Show that the map $X \mapsto aX + b$ extends to a unique automorphism of $A[X]$ inducing the identity on A. What is the inverse automorphism?

Proof. If φ is constrained to fix A, then it obviously extends to the unique homomorphism

$$c_n X^n + \cdots + c_1 X + c_0 \mapsto c_n(aX + b)^n + \cdots + c_1(aX + b) + c_0.$$

This map has an inverse, which is $X \mapsto a^{-1}X - a^{-1}b$ (being of the same form, this also extends to a unique homomorphism fixing A). The composition of these maps clearly gives the identity on X and on A, and so the composition is the unique extension of $X \mapsto X$ fixing A, which is the identity. So this is an automorphism of $A[X]$. $\square$

9. Show that every automorphism of $A[X]$ inducing the identity on A is of the type described in Exercise 8.

Proof. Let φ be an automorphism of $A[X]$ inducing the identity on A. Then for any polynomial we have

$$c_nX^n + \cdots + c_1X + c_0 \mapsto c_np(X)^n + \cdots + c_1p(X) + c_0$$

where $p(X)$ is the image of X. If $\deg p > 1$ then for all nonconstant polynomials f we will have $\deg \varphi f > \deg f$, hence X is not in the image of φ. If $\deg p < 1$ then obviously φ is not injective, since it fixes A. So $p(X) = aX + b$ for some $a, b \in A$.

φ^{-1} satisfies the same hypothesis, and thus must be of the form $cX+d$. Since $c(aX+b)+d = acX + cb + d = X$, we must have $ac = 1$ and $d = -cb$. Thus the inverse map is given by $X \mapsto a^{-1}X + a^{-1}b$, as claimed. □

10. Let K be a field, and $K(X)$ the quotient field of $K[X]$. Show that every automorphism of $K(X)$ which induces the identity on K is of type

$$X \mapsto \frac{aX+b}{cX+d}$$

with $a, b, c, d \in K$ such that $(aX + b)/(cX + d)$ is not an element of K, or equivalently, $ad - bc \neq 0$.

Proof. Let φ be an automorphism fixing K. Let $f(X) = \frac{p(X)}{q(X)}$ be the image of X, where $p(X)$ and $q(X)$ are relatively prime. Then X is a root of $g(Y) = q(Y)f(X) - p(Y) \in K(f(X))[Y]$, hence X is algebraic over $K(f(X))$. This polynomial is also contained in the subring $K[f(X)][Y] = K[Y][f(X)]$, and it is irreducible in $K[Y][f(X)]$ since it is linear in $f(X)$. Thus it is irreducible over $K[f(X)][Y]$. But a polynomial is irreducible over a UFD if and only if it is irreducible over its field of fractions, thus g is irreducible in $K(f(X)[Y]$. Hence it is the minimal polynomial for X over $K(f(X))$, and so its degree (in Y) is the degree of the extension $K(f(X))(X)$ over $K(f(X))$, which is thus $\max\{\deg(p), \deg(q)\}$ (the degrees taken in Y). But $K(f(X))(X) = K(X)$ because $f(X) \in K(X)$, therefore

$$[K(X) : K(f(X))] = \max\{\deg(p), \deg(q)\}.$$

Since φ is surjective, and its image $K(\varphi(X)) = K(f(X))$ must equal $K(X)$. Therefore, the degree of this extension is 1, and so both p and q are either linear or constant. Finally, if $ad - bc = 0$ then we have

$$\frac{c}{a}\varphi(X) = \varphi(\frac{c}{a}X) = \frac{c}{a}\frac{aX+b}{cX+d} = \frac{acX+bc}{acX+ad} = 1$$

and so $\varphi(X) = \frac{a}{c}$, contradicting the injectivity of φ. So $ad - bc \neq 0$.

Next, we will show that all maps of this form are automorphisms. Let φ be the unique extension of $X \mapsto \frac{aX+b}{cX+d}$, fixing K, to a homomorphism $K[X] \to K(X)$. It takes $p(X)$ to $p(\frac{aX+b}{cX+d})$. If $\varphi(p(X)) = p(\frac{aX+b}{cX+d}) = 0$, then $\frac{aX+b}{cX+d}$ is algebraic over K. Now note that

$$\frac{c}{bc-ad}\left(\frac{aX+b}{cX+d} - \frac{a}{c}\right) = \frac{1}{cX+d}$$

because $ad - bc \neq 0$, therefore $K(\frac{aX+b}{cX+d}) = K(\frac{1}{cX+d}) = K(cX+d) = K(X)$ is algebraic, a contradiction. So φ is injective.

Since φ is injective, it extends to a unique endomorphism $K(X) \to K(X)$ (since no denominator can map to 0). Since a field homomorphism is either injective or trivial, this map must be injective. By the discussion in the proof of the other direction, we have

$$[K(X) : \mathrm{Im}] = [K(X) : K(\frac{aX+b}{cX+d})] = \max\{\deg(aX+b), \deg(cX+d)\} = 1$$

since if both polynomials were constant we would have $ad = bd = 0$. Therefore, the image of the map is all of $K(X)$, hence it is surjective.

□