A PRIMER OF FIELD THEORY

These pages contain some useful facts and results about fields and most of them have proofs. The reader is assumed to be familiar with the definitions of rings and fields, ideals, homomorphims and so on. The identity element in a ring or a field will always be denoted by 1. All rings below are assumed to be commutative and with 1. Let R be a ring and I an ideal. Recall the following facts:

- I is a prime ideal if and only if R/I is an integral domain.
- I is a maximal ideal if and only if R/I is a field.
- In a principal ideal domain all prime ideals are maximal.

Also recall the ring morphism theorem:

Theorem 1 *Let $f\colon R \to S$ be a ring homomorphism. Then f is injective if and only if* $\ker f = 0$*. The map $x+\ker f \mapsto f(x)$ is an isomorphism $R/\ker f \to \operatorname{im} f$.*

The kernel of $f\colon R \to S$ is defined as the ideal $\ker f$ in R consisting of all elements that are mapped to 0, i.e. such that $f(x) = 0$. The image $\operatorname{im} f$ is the subset of S of all $f(x)$ as x ranges over R (the image is usually not an ideal). The ideal generated by a set of elements $x_1, x_2, \ldots, x_n$ is denoted by $(x_1, x_2, \ldots, x_n)$, i.e.

$$(x_1, x_2, \ldots, x_n) = Rx_1 + Rx_2 + \ldots + Rx_n = \{\sum_{i=1}^{n} a_i x_i ; a_i \in R\}.$$

1. The characteristic. Let k be a field. When $n > 0$ is an integer, we let $n \cdot 1$ (here 1 is the identity element of k) denote the sum of n 1's in k. We also put $(-n) \cdot 1 = -(n \cdot 1)$ and $0 \cdot 1 = 0$. Then the map $f\colon \mathbf{Z} \to k, f(n) = n \cdot 1$, is a ring homomorphism. The kernel is an ideal in $\mathbf{Z}$ and since this is a Euclidean domain, $\ker f = m\mathbf{Z}$ for some integer $m \geq 0$. There are two possibilities, either $m = 0$ or $m > 0$. In the former case, $\ker f = 0$ and f is injective. Then k contains an isomorphic copy of $\mathbf{Z}$, which we identify with $\mathbf{Z}$. Since k is a field, it contains the inverses of all its non-zero elements, and it follows that $\mathbf{Q} \subseteq k$.

Now assume that $m > 0$. If $m = 1$, the kernel of f is the whole ring $\mathbf{Z}$, so $1 = f(1) = 0$ and k consists of one element only. So assume that $m \geq 2$. The image of f is a subring of k, and since k is a field, $\operatorname{im} f$ is an integral domain. But then $\ker f$ must be a prime ideal, $\ker f = p\mathbf{Z}$ for some prime p. Hence we have $\operatorname{im} f \cong \mathbf{Z}/\ker f = \mathbf{Z}/p\mathbf{Z} = \mathbf{Z}_p$ and k contains the field with p elements. Notice that in this case

$$p \cdot a = (p \cdot 1) \cdot a = 0 \cdot a = 0$$

for all $a \in k$.

If $\mathbf{Q} \subseteq k$, we say that k has *characteristic* 0 and if $\mathbf{Z}_p \subseteq k$, k has characteristic p. All subfields of the complex numbers have characteristic 0, for instance. The characteristic is denoted by char k. The fields $\mathbf{Q}$ and $\mathbf{Z}_p$ are called the *prime fields.*

2. Field extensions. If k is a subfield of another field F, we also say that F is an *extension* of k. Then F is a vector space over k and we denote the dimension of F over k by $[F : k]$, which is often called the *degree* of F over k. The degree might be infinite. If $k \subseteq F$, one often talks about the extension F/k. If $[F : k] < \infty$, then F/k is said to be a finite extension.

We have for instance $[\mathbf{C} : \mathbf{R}] = 2$ since $\{1, i\}$ is a basis. The real numbers is an extension of the rationals, but of infinite dimension. Let $\mathbf{Q}(\sqrt{2})$ denote the set of all real numbers of the form $a + b\sqrt{2}$ with $a, b \in \mathbf{Q}$. This is a field (why?) and its degree over $\mathbf{Q}$ is 2 (for what is a basis?).

Theorem 2 *Suppose that E/k and F/E are two extensions. Then F is an extension of k and $[F : k] = [F : E] \cdot [E : k]$.*

Remark: This should be interpreted as follows. If either side is finite, then so is the other and the equality holds. If either side is infinite, then so is the other.

Proof. First assume that F/E and F/k are finite and let $y_1, \ldots, y_m$ and $x_1, \ldots, x_n$ be bases, respectively. Let $a \in F$. We can write $a = \sum_{i=1}^m a_i y_i$ for some $a_i \in E$. We can also write $a_i = \sum_{j=1}^n b_{ij} x_j$ for some $b_{ij} \in k$, so

$$a = \sum_{i=1}^{m} (\sum_{j=1}^{n} b_{ij} x_j) y_i = \sum_{i,j} b_{ij} x_j y_i.$$

It follows that the products $x_j y_i$ generate F as a vector space over k. We now prove that they are linearly independent. Assume that $\sum_{i,j} b_{ij} x_j y_i = 0$ for some $b_{ij} \in k$. If we rewrite this as $\sum_i (\sum_j b_{ij} x_j) y_i = 0$, we see that $\sum_j b_{ij} x_j = 0$ for all i, since the y_i are linearly independent over E. But the x_j are linearly independent over k, so finally $b_{ij} = 0$ for all i, j. Hence

$$[F : k] = mn = [F : E][E : k].$$

Now suppose that F/k is a finite extension. Then F/E must also be finite, since E is a bigger field than k. Since E is a subspace of F, E/k must also be finite, and we have equality by the first part of the proof.

Let F/k be an extension. When $a_1, \ldots, a_n$ are elements of F, we denote by $k(a_1, \ldots, a_n)$ the smallest subfield of F containing k and the a_i. Such a field is said to be a *finitely generated* extension of k. Its elements are all quotients

$$\frac{p(a_1, \ldots, a_n)}{q(a_1, \ldots, a_n)}$$

where p and q are polynomials in n variables and $q(a_1, \ldots, a_n) \neq 0$. One should notice that finitely generated extensions do not have to be finite. For instance, $\mathbf{Q}(\pi)$ is finitely generated, but not finite (but this is difficult to prove!).

The smallest *subring* of F containing $a_1, \ldots, a_n$ is denoted by $k[a_1, \ldots, a_n]$ and consists of all polynomials in $a_1, \ldots, a_n$. Under certain conditions which we will discuss later $k(a_1, \ldots, a_n) = k[a_1, \ldots, a_n]$.

3. Polynomials and splitting fields. The ring of polynomials in a variable x with coefficients in a ring R is denoted by $R[x]$. Let $\phi\colon R \to S$ be a ring homomorphism. Then we get a homomorphism of the rings of polynomials, also denoted by ϕ, by

$$\phi(a_0 + a_1 x + \ldots + a_n x^n) = \phi(a_0) + \phi(a_1)x + \ldots + \phi(a_n)x^n.$$

If k is a field, then $k[x]$ is a Euclidean domain and so also a principal ideal domain and a unique factorization domain. If $f(x) \in k[x]$ is an irreducible polynomial, then the ideal $(f(x)) = f(x)k[x]$ in $k[x]$ is prime, and also maximal. Hence the quotient $F = k[x]/(f(x))$ is a field. The composition of the map inclusion map $k \to k[x]$ and the quotient map $k[x] \to k[x]/(f(x))$ is injective, which means that k is a subfield of F. Denote the quotient map $k[x] \to k[x]/(f(x))$ by $g(x) \mapsto \overline{g(x)}$. Notice that $\bar{a} = a$ if $a \in k$. Hence, if $g(x) = a_0 + a_1 x + \ldots + a_n x^n$, then

$$\begin{aligned} \overline{g(x)} &= \overline{a_0 + a_1 x + \ldots + a_n x^n} \\ &= \bar{a}_0 + \bar{a}_1 \bar{x} + \ldots + \bar{a}_n \bar{x}^n \\ &= a_0 + a_1 \bar{x} + \ldots + a_n \bar{x}^n = g(\bar{x}). \end{aligned}$$

Since $\overline{f(x)} = 0$, this means that $f(\bar{x}) = 0$, i.e. $f(x)$ has a zero in F. We can construct an extension in which f has a zero even if it is not irreducible; we just work with an irreducible factor of f.

If we repeat this process we sooner or later get a field E over which $f(x)$ splits into linear factors, i.e.

$$f(x) = a(x - \alpha_1) \ldots (x - \alpha_n)$$

where a is the coefficient of x^n and $\alpha_i \in E$. The extension $k(\alpha_1, \ldots, \alpha_n)$ generated by the zeros of f is called a *splitting field for $f(x)$* over k. We have proved the first part of

Theorem 3 *Splitting fields exist. All splitting fields of a polynomial f over a field k are isomorphic.*

We need a lemma:

Lemma 1 *Let $\phi\colon k \to k'$ be a field isomorphism and $f(x) \in k[x]$ an irreducible polynomial. Let α and α' be zeros of f and ϕf, respectively, in some extensions of k and k'. Then ϕ can be extended to an isomorphism $k(\alpha) \to k'(\alpha')$ such that $\phi(\alpha) = \alpha'$.*

Remark: The claim means that there is an isomorphism between $k(\alpha)$ and $k'(\alpha')$ whose restriction to k is ϕ.

Proof. Define $\psi\colon k[x] \to k'(\alpha')$ by $\psi(g(x)) = \phi g(\alpha')$. ψ is clearly surjective. What is the kernel? Well, $g(x)$ is in the kernel if and only if $\phi g(\alpha') = 0$. Let $h(x)$ be the greatest common divisor of ϕf and ϕg. There are polynomials f_1, g_1 such that $h = f_1 \cdot \phi f + g_1 \cdot \phi g$, from which follows that $h(\alpha') = 0$. Now ϕf is irreducible, so either h is constant or $h = \phi f$. But we just saw that h has a zero, and then it cannot be a constant polynomial. Hence $h = \phi f$ and $\phi f | \phi g$, which implies $f|g$ and it follows that ker $\psi = (f(x))$. The homomorphism theorem gives $k[x]/(f(x)) \cong k'(\alpha')$, the isomorphism being given by $\bar{x} \mapsto \alpha'$. In the same way we get $k[x]/(f(x)) \cong k(\alpha)$ and the claim follows.

Proof of the theorem We will prove a somewhat stronger statement, namely the following: *Let $\phi\colon k \to k'$ be an isomorphism and let f be a polynomial over k. Let E and E' be splitting fields for f and ϕf, respectively. Then ϕ can be extended to an isomorphism $E \to E'$.*

We will use induction on the degree of f, the case $\deg f = 1$ being trivial (then ϕ itself is the required morphism). Assume then that the statement is true for polynomials of degree less than $\deg f$. Take an irreducible factor f_1 of f and let α and α' be zeros of f_1 and ϕf_1 in E and E', respectively. By the lemma, ϕ can be extended to an isomorphism $k(\alpha) \to k'(\alpha')$ such that $\phi(\alpha) = \alpha'$. Write

$$f(x) = (x - \alpha)g(x), \quad \phi f(x) = (x - \alpha')\phi g(x)$$

over $k(\alpha)$ and $k'(\alpha')$. The fields E and E' are splitting fields for g and ϕg, respectively, and by the induction hypothesis, ϕ extends to an isomorphism of these. The claim is proved and the theorem follows if we take $\phi\colon k \to k$ to be the identity map.

Remark: If k is a subfield of the complex numbers and we assume that we know the fundamental theorem of algebra, the proof of the existence of a splitting field is much simpler. For if the zeros of f in $\mathbf{C}$ are $\alpha_1, \ldots, \alpha_n$, then $k(\alpha_1, \ldots, \alpha_n)$ is a splitting field.

Example. One way to define $\mathbf{C}$ is as the quotient $\mathbf{R}[x]/(x^2 + 1)$.

Example. The splitting field for $x^2 - 2$ over $\mathbf{Q}$ is clearly $\mathbf{Q}(\sqrt{2})$.

Example. The roots of the equation $x^3 - 2 = 0$ are $\alpha, \omega\alpha, \omega^2\alpha$, where $\alpha = \sqrt[2]{2}$ and $\omega = e^{2\pi i/3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Hence the splitting field of $x^3 - 2$ is

$$k = \mathbf{Q}(\alpha, \omega\alpha, \omega^2\alpha).$$

Clearly $k \subseteq \mathbf{Q}(\alpha, \omega)$. On the other hand, $\omega = \omega^2\alpha/\omega\alpha \in k$, so

$$k = \mathbf{Q}(\alpha, \omega).$$

Example. Consider the polynomial $p(x) = x^n - 1$. Put $\zeta_n = e^{2\pi i/n}$; then the zeros of p are $\zeta_n^k, k = 0, 1, \ldots, n-1$. Hence the splitting field of p over $\mathbf{Q}$ is $\mathbf{Q}(\zeta_n)$. Fields of this form are called *cyclotomic* fields. Cyclotomic derives from Greek and means "to divide a circle".

Example. The roots of the equation $x^4 - 10x^2 + 1 = 0$ are $\pm\sqrt{2} \pm \sqrt{3}$ with all combinations of signs. Hence the splitting field of $x^4 - 10x^2 + 1$ over $\mathbf{Q}$ is

$$k = \mathbf{Q}(\sqrt{2} + \sqrt{3}, \sqrt{2} - \sqrt{3}, -\sqrt{2} + \sqrt{3}, -\sqrt{2} - \sqrt{3}).$$

Obviously $k \subseteq \mathbf{Q}(\sqrt{2}, \sqrt{3})$. But since $\sqrt{2} = ((\sqrt{2} + \sqrt{3}) + (\sqrt{2} - \sqrt{3}))/2$ and analogously for $\sqrt{3}$, we actually have $k = \mathbf{Q}(\sqrt{2}, \sqrt{3})$.

4. Algebraic elements and extensions. Let F/k be a field extension. An element $\alpha \in F$ is said to be *algebraic* over k if there is a (non-zero) polynomial $f(x) \in k[x]$ such that $f(\alpha) = 0$. If $f(x) = a_0 + a_1x + \ldots + a_nx^n$, this means that

$$a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0,$$

in other words that the powers of α are *linearly dependent* over k.

If α is algebraic over k, there is an irreducible polynomial f such that $f(\alpha) = 0$. For if α is a zero of a polynomial, it must be a zero of some irreducible factor of this polynomial. Assume that f and g are irreducible polynomials such that $f(\alpha) = g(\alpha) = 0$. Let h be their greatest common divisor. Since $h = f_1f + g_1g$ for some f_1, g_1, $h(\alpha) = 0$. Hence h is not a constant, and since $h|f$, we must have $h = cf$ for some $c \in k$. But then $f|g$ and finally $g = c'f$. If we require that the coefficient of the highest degree term should be 1, the irreducible polynomial such that $f(\alpha) = 0$ is uniquely determined. It is called the *minimal polynomial* of α over k.

Example. The minimal polynomials of $\sqrt{2}$ and i over $\mathbf{Q}$ are $x^2 - 2$ and $x^2 + 1$, respectively. Put $\alpha = \sqrt{3} + \sqrt{5}$. Then $\alpha^2 = 8 + 2\sqrt{15}$, so $(\alpha^2 - 8)^2 = 4 \cdot 15 = 60$, which simplifies to $\alpha^4 - 32\alpha^2 - 124 = 0$. One can show that $x^4 - 32x^2 - 124$ is irreducible over $\mathbf{Q}$ (try!), so it is the minimal polynomial of $\sqrt{3} + \sqrt{5}$ over $\mathbf{Q}$.

Theorem 4 *Let F/k be an extension and $\alpha \in F$.*

a) α is algebraic over k if and only if $k[\alpha] = k(\alpha)$.

b) α is algebraic over k if and only if $k(\alpha)/k$ is a finite extension.

c) If α is algebraic, then $[k(\alpha) : k] = \deg f$, where f is the minimal polynomial.

Proof. a) Assume that α is algebraic. We always have the inclusion $\subseteq$. To prove the converse, it is enough to prove that $1/q(\alpha) \in k[\alpha]$ for all q with $q(\alpha) \neq 0$. Let f be the minimal polynomial. Since $q(\alpha) \neq 0$, f does not divide q and then their greatest common divisor is 1. There are polynomials such that $f_1(x)f(x) + q_1(x)q(x) = 1$. It we put $x = \alpha$ we get $q_1(\alpha)q(\alpha) = 1$, since $f(\alpha) = 0$. Hence $1/q(\alpha) = q_1(\alpha)$. Notice that this also gives a method to find the inverse!

If $k[\alpha] = k(\alpha)$, then $1/\alpha = p(\alpha)$ for some polynomial p, so $\alpha p(\alpha) - 1 = 0$, which means that α is algebraic.

b and c) If α is algebraic, the elements of $k(\alpha)$ are polynomials in α by a). Let $p(\alpha)$ be such an element. Divide p by the minimal polynomial f:

$p(x) = q(x)f(x) + r(x)$, where $r = 0$ or $\deg r < \deg f$. This gives $p(\alpha) = r(\alpha)$, which means that the elements of $k(\alpha)$ can be written

$$a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1},$$

where $n = \deg f$. Hence $[k(\alpha) : k] \leq n$. On the other hand, there can be no relation of the form $b_0 + b_1\alpha + \ldots + b_m\alpha^m = 0$, not all $b_i = 0$, for any $m < n$, since f is the polynomial of least degree that has the zero α. It follows that the powers $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ are linearly independent, so $[k(\alpha) : k] = n = \deg f$.

Finally assume that $k(\alpha)/k$ is finite and has degree n. Then the powers $1, \alpha, \ldots, \alpha^n$ are linearly dependent over k, so there are $a_i \in k$, not all 0, such that $a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$. Hence α is algebraic (and of degree at most n).

An extension F/k is said to be algebraic if every element of F is algebraic over k.

Corollary 1 *If $\alpha_1, \ldots, \alpha_n$ are algebraic over k, then $k(\alpha_1, \ldots, \alpha_n)/k$ is a finite algebraic extension.*

Remark: It is not true that all algebraic extensions are finite.

Proof. Each step in the chain

$$k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset k(\alpha_1, \alpha_2, \ldots, \alpha_n) = F$$

is finite, so by the multiplicativity of the degree, F is finite over k and hence also algebraic.

Corollary 2 *The sum and product of algebraic elements are algebraic. If $\alpha \neq 0$ is algebraic, then so is $1/\alpha$. Hence in an extension F/k the elements of F that are algebraic over k form a field.*

Proof. Let α, β be algebraic. By Corollary 1, $k(\alpha, \beta)/k$ is algebraic. The claim follows since $\alpha + \beta, \alpha\beta, 1/\alpha \in k(\alpha, \beta)$.

Let α be algebraic over k and $f(x)$ its minimal polynomial. The other roots of $f(x) = 0$ are called the *algebraic conjugates* of α over k. Assume that $\alpha = \alpha_1, \ldots, \alpha_n$ are the conjugates of α and $\beta = \beta_1, \ldots, \beta_m$ are those of β. One can show that

$$h(x) = \prod_{i,j}(x - (\alpha_i + \beta_j)) \in k[x],$$

so that the minimal polynomial of $\alpha + \beta$ is a factor of $h(x)$. It may happen that h is the minimal polynomial, but it is not necessarily so.

"Algebraic" satisfies the transitive property:

Corollary 3 *If E/F and F/k are algebraic extensions, then so is E/k.*

Proof. Let $\alpha \in E$ and let $f(x) = a_0 + a_1x + \ldots + a_nx^n$ be its minimal polynomial over F. The coefficients a_i are algebraic over k, so we have a chain of finite algebraic extensions:

$$k \subset k(a_1, \ldots, a_n) \subset k(a_1, \ldots, a_n, \alpha).$$

Hence α is algebraic over k.

Example. Let k be the splitting field of $x^3 - 2$ over $\mathbf{Q}$. In the chain

$$\mathbf{Q} \subset \mathbf{Q}(\alpha) \subset k,$$

the first step has degree 3. The degree of the second step is at most 2, since ω has degree 2 over $\mathbf{Q}$. But $\mathbf{Q}(\alpha)$ is real, which ω isn't, so the degree must be 2. Hence $[k : \mathbf{Q}] = 3 \cdot 2 = 6$.

Example. Now let $k = \mathbf{Q}(\sqrt{2}, \sqrt{3})$ be the splitting field of $x^4 - 10x^2 + 1$. The first step in the chain

$$\mathbf{Q} \subset \mathbf{Q}(\sqrt{2}) \subset k$$

has degree 2 and the second has degree 1 or 2. If the degree were 1, we would have $\sqrt{3} \in \mathbf{Q}(\sqrt{2})$, i.e. $\sqrt{3} = a + b\sqrt{2}$ for some rational numbers a, b. Squaring gives $3 = a^2 + 2b^2 + 2ab\sqrt{2}$, implying that $\sqrt{2}$ is rational. This is a contradiction, and so the degree is 2. Hence $[k : \mathbf{Q}] = 4$.

5. Algebraically closed fields. The field of complex numbers has the property that all irreducible polynomials have degree 1, or, in other words, that all polynomials with complex coefficients split into linear factors over $\mathbf{C}$. This can also be expressed by saying that $\mathbf{C}$ has no non-trivial algebraic extensions. Fields with this property are said to be *algebraically closed*. The fact that $\mathbf{C}$ is algebraically closed is commonly known as the fundamental theorem of algebra. No purely algebraic proofs of this fact are known. $\mathbf{R}$ is not algebraically closed.

Let $\mathbf{A}$ be the field of all complex numbers that are algebraic over $\mathbf{Q}$ (instead of "algebraic over $\mathbf{Q}$" one usually says just "algebraic"). $\mathbf{A}$ is called the field of algebraic numbers and by Corollary 3 it is algebraically closed. It can be shown that $\mathbf{A}/\mathbf{Q}$ is an extension of infinite degree (the polynomial $x^n - 2$ is irreducible, so $\sqrt[n]{2}$ has degree n over $\mathbf{Q}$).

It can be shown that for each field k there is an algebraic extension $\bar{k}/k$ such that $\bar{k}$ is algebraically closed. The field $\bar{k}$ is called the *algebraic closure* of $\bar{k}$. All algebraic closures of k are isomorphic.

6. The derivative and multiple zeros The derivative of $f(x) = a_0 + a_1x + \ldots + a_nx^n \in k[x]$ is *defined* to be $f'(x) = a_1 + 2a_2x + \ldots + ia_ix^{i-1} + \ldots + na_nx^{n-1}$. By direct computation one easily proves the well-known rules for differentiation:

$$(f(x) + g(x))' = f'(x) + g'(x), \quad (f(x)g(x))' = f'(x)g(x) + f(x)g'(x).$$

Theorem 5 *Let α be a zero of f in some extension of k. If $f'(\alpha) \neq 0$, then α is a simple zero. If char $k = 0$, the converse is true too.*

Proof. Write $f(x) = (x - \alpha)^m g(x)$, where $g(\alpha) \neq 0$. Then

$$f'(x) = (x - \alpha)^{m-1}(mg(x) + (x - \alpha)g'(x)).$$

If $f'(\alpha) \neq 0$, then we must have $m = 1$. If the characteristic is 0 and $m = 1$, then $f'(\alpha) = mg(\alpha) \neq 0$.

If the characteristic is 0, we see that the multiplicity of α as a zero of $f'(x)$ is $m - 1$. If k has prime characteristic one can construct examples in which the multiplicity increases, for instance $f(x) = (x - 1)^p(x^2 - 2x) \in \mathbf{Z}_p[x]$ for $p \geq 3$.

Corollary 4 *If char $k = 0$ and $f(x) \in k[x]$ is irreducible, then f has only simple zeros. In other words f has* $\deg f$ *distinct roots.*

Proof. Assume that f has a zero α of multiplicity ≥ 2. Then $f'(\alpha) = 0$ and α is a zero of the greatest common divisor (f, f'). Hence $(f, f') \neq 1$ and f cannot be irreducible.

The corollary is not true in characteristic $p > 0$. For instance, let $k = \mathbf{Z}_p(t)$, the field of *rational functions* over $\mathbf{Z}_p$. Its elements are "fractions" $f(t)/g(t)$, where f and $g \neq 0$ are polynomials with coefficients in $\mathbf{Z}_p$. The polynomial $x^p - t$ is irreducible over k by e.g. a generalization of Eisenstein's criterion. Let u be a zero in an extension. We have $x^p - t = x^p - u^p = (x - u)^p$, so the irreducible polynomial $x^p - t$ has just one root, which has multiplicity p.

7. Finite fields. A finite field k must have prime characteristic and so be an extension of $\mathbf{Z}_p$ for some prime p. Let $[k : \mathbf{Z}_p] = n$ and let $x_1, \ldots, x_n$ be a basis. The elements of k can be written $a_1x_1 + \ldots + a_nx_n$, where $a_i \in \mathbf{Z}_p$. Hence $|k| = p^n$. This shows that there is no field with 6 elements, for instance. We are going to show that for every prime p and exponent n there is exactly one field with p^n elements (i.e. all fields with p^n elements are isomorphic). This unique field is denoted by $\mathbf{F}_{p^n}$.

Lemma 2 *Let k be a field of characteristic p. Then $(a + b)^{p^n} = a^{p^n} + b^{p^n}$ for all $a, b \in k$.*

Proof. It is enough to prove the formula for $n = 1$. By the binomial theorem

$$(a + b)^p = a^p + \sum_{j=1}^{p-1} \binom{p}{j} a^{p-j}b^j + b^p.$$

In $j!(p - j)!\binom{p}{j} = p!$ the right-hand side is divisible by p. But p is a prime, so p does not divide $j!$ or $(p - j)!$. Hence $p|\binom{p}{j}$ and $(a + b)^p = a^p + b^p$.

Let $f(x) = x^{p^n} - x$ considered as a polynomial over $\mathbf{Z}_p$ and let k be its splitting field. Let α and β be two zeros of f in k. Then

$$f(\alpha + \beta) = (\alpha + \beta)^{p^n} - (\alpha + \beta) = \alpha^{p^n} + \beta^{p^n} - \alpha - \beta = f(\alpha) + f(\beta) = 0$$

and

$$f(\alpha\beta) = (\alpha\beta)^{p^n} - \alpha\beta = \alpha^{p^n}\beta^{p^n} - \alpha\beta = \alpha\beta - \alpha\beta = 0.$$

Also

$$f(\alpha^{-1}) = (\alpha^{-1})^{p^n} - \alpha^{-1} = (\alpha^{p^n})^{-1} - \alpha^{-1} = \alpha^{-1} - \alpha^{-1} = 0$$

and it follows that the zeros of f form a subfield of k. But k is generated by the zeros of f, so in fact k consists exactly of the zeros of f. Since $f'(x) = p^n x^{p^n-1} - 1 = -1 \neq 0$, f has p^n zeros, so k is a field with p^n elements.

Now let F be any field with p^n elements. The group $F^* = F \setminus \{0\}$ has $p^n - 1$ elements, so by Lagrange's theorem, $\alpha^{p^n-1} = 1$ for all $\alpha \in F^*$. It follows that F is a splitting field for f, and since splitting fields are unique up to isomorphism, we have finally proved that there is exactly one field with p^n elements.

Let α be a generator of the multiplicative group $\mathbf{F}_{p^n}^*$. The minimal polynomial of α over $\mathbf{Z}_p$ has degree n, which proves that there are irreducible polynomial of all degrees over $\mathbf{Z}_p$. It is not difficult to find a formula for the number of irreducibles of a certain degree, see below.

Theorem 6 *$\mathbf{F}_{p^d}$ is a subfield of $\mathbf{F}_{p^n}$ if and only if $d|n$.*

Proof. Assume that $\mathbf{F}_{p^d}$ is a subfield of $\mathbf{F}_{p^n}$. Then $\mathbf{F}_{p^d}^*$ is a subgroup of $\mathbf{F}_{p^n}^*$, so by Lagrange's theorem $p^d - 1 | p^n - 1$. Divide n by d: $n = qd + r$, where $0 \leq r < d$. Then

$$\frac{p^n - 1}{p^d - 1} = \frac{p^{qd+r} - 1}{p^d - 1} = \frac{p^r(p^{qd} - 1) + p^r - 1}{p^d - 1} = p^r \cdot \frac{p^{qd} - 1}{p^d - 1} + \frac{p^r - 1}{p^d - 1}.$$

Here the first term is an integer, since $(p^{qd} - 1)/(p^d - 1) = p^{q(d-1)} + p^{q(d-2)} + \ldots + p^q + 1$ and so $r = 0$.

If $d|n$, then $p^d - 1 | p^n - 1$. Let k be the subset of $\mathbf{F}_{p^n}$ consisting of 0 and the elements that have orders dividing $p^d - 1$. Then $|k| = p^d$, for $\mathbf{F}_{p^n}^*$ is a cyclic group of order $p^n - 1$ which is divisible by $p^d - 1$. The same calculations as above show that k is a field, so $k = \mathbf{F}_{p^d}$.

We will finally briefly discuss the factorization of $f(x) = x^{p^n} - x$ into irreducibles over $\mathbf{Z}_p$. Let $g(x)$ be an irreducible factor and α a zero of g. The extension $\mathbf{Z}_p(\alpha) \subseteq \mathbf{F}_{p^n}$ has degree $\deg g$, so $\deg g = d$ for some divisor d of n. On the other hand, let $g(x) \in \mathbf{Z}_p[x]$ be irreducible and of degree d, where $d|n$. Also let α be a zero of g. Then $\mathbf{Z}_p(\alpha)$ has degree d and so is isomorphic to the subfield $\mathbf{F}_{p^d}$ of $\mathbf{F}_{p^n}$. Let $g_1(x)$ be the irreducible factor of f that has the zero α. Then the greatest common divisor (g, g_1) also has the zero α, so $g = g_1$ is a divisor of f. We saw above that f has only simple zeros and it follows that

$$f(x) = x^{p^n} - x = \prod_{d|n} F_d(x),$$

where $F_d(x)$ is the product of all irreducible polynomials over $\mathbf{Z}_p$ of degree d. (Multiplicative) Möbius inversion gives

$$F_n(x) = \prod_{d|n} (x^{p^d} - x)^{\mu(n/d)}.$$

If the number of irreducibles of degree n is N_n, then computing the degree on both sides gives

$$N_n = \frac{1}{n} \sum_{d|n} \mu(n/d) p^d.$$