Chapter II. Rings and polynomials

PREREQUISITES ABOUT RINGS AND IDEALS.

A *ring* R is a non-empty set with two compositions $+$ and $\cdot$ such that

1) $(R, +)$ is an abelian group;
2) $(R, \cdot)$ is associative;
3) The distributive laws hold:
   $a \cdot (b + c) = a \cdot b + a \cdot c$
   $(a + b) \cdot c = a \cdot c + b \cdot c.$

The neutral element in R with respect to addition $+$ is denoted by 0. A neutral element with respect to multiplication $\cdot$ is uniquely determined and is called the *identity element* or *unit element* and is usually denoted by 1 (or sometimes by e).

If $(R, \cdot)$ is commutative, R is called *commutative*

In the following we shall only consider commutative rings with identity element.

We recall some basic definitions and theorems which should be known from Anders Thorup Mat 2ALG.

For any element a of R the distributive law implies:

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0,$$

hence $a \cdot 0 = 0$. Thus $a \cdot b = 0$ if either $a = 0$ or $b = 0$.

A commutative ring for which the converse holds, i.e. a commutative ring for which the product of two elements a and b can only be 0 if either $a = 0$ or $b = 0$, is called an *integral domain.*

A commutative ring R (with at least two elements) is called a *field*, if every non-zero element a in R has an inverse, i.e. an element $a^{-1} \in R$ such that $a \cdot a^{-1} = 1$. Such an inverse is necessarily uniquely determined. (Why?) A field is necessarily an integral domain. Indeed, assume $a \neq 0$ and $a \cdot b = 0$. If a has an inverse a^{-1} the equation $a \cdot b = 0$ implies $1 \cdot b = a \cdot a^{-1} \cdot b = 0$; hence $b = 0$.

Exercise 2.1. Prove that an integral domain R (with at least two elements) is a field if R has only finitely many elements. (Hint: if a is a non-zero element prove that the mapping $x \mapsto a \cdot x$ from R into itself is injective.)

For any integral domain R there exists a *fraction field* K, i.e. a field K containing R as a subring such that every element $x \in K$ is a quotient between two elements of R, i.e. there exist elements a and b of R, $a \neq 0$ for which $a \cdot x = b$.

Example 2.2. The rational numbers form a field $\mathbb{Q}$ which is the fraction field of the integral domain $\mathbb{Z}$ of all ordinary integers.

Example 2.3. Let K be a field. The polynomial ring $K[x]$ is an integral domain. $K[x]$ is not a field; the field of rational functions $K(x)$ is the fraction field of $K[x]$.

The notion of "ideal" is fundamental in ring theory.

Definition 2.4. An additive subgroup I of $(R, +)$, R being a commutative ring with an identity element, is called an *ideal*, if $RI \subseteq I$, i.e. if $r \cdot a \in I$ for every $r \in R$ and every $a \in I$.

If I is an ideal of R the cosets (or residue classes) $r + I = \{r + a \mid a \in I\}$ form a commutative ring, called the *residue class ring* (or *quotient ring*) of R with respect to I. This ring is denoted R/I.

If r is an element of R the residue class containing r is often denoted by $\bar{r}$. If $\bar{r}$ and $\bar{s}$ are residue classes containing the elements r and s from R the sum, resp. product of $\bar{r}$ and $\bar{s}$ is defined by $\bar{r} + \bar{s} = \overline{r + s}$, resp. $\bar{r} \cdot \bar{s} = \overline{r \cdot s}$.

A map ϕ from one ring R to another ring S is called a homomorphism if ϕ sends sums into sums and products to products: $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$ and $\phi(r_1 \cdot r_2) = \phi(r_1) \cdot \phi(r_2)$ for all r_1 and r_2 in R.

The subset $I := \{r \in R \mid \phi(r) = 0\}$ of R is an ideal of R, called the *kernel* of ϕ and denoted by $Ker(\phi)$.

For elements in the residue class ring R/I we use the bar notation (as in group theory (cf. Remark 1.51) by letting $\bar{r}$ denote the residue class $r + I$

The map $R \mapsto R/I$, defined by $r \mapsto \bar{r}$ is obviously a homomorphism whose kernel is I. This map is called the *canonical epimorphism* from R to R/I.

For ring homomorphisms there is an isomorphism theorem quite analogous to Theorem 1.65 for groups. The proof is omitted since it is an obvious modification of the corresponding proof in the group theoretical case.

Theorem 2.5. *Let ϕ be a surjective homomorphism from the ring R onto the ring S. If I is the kernel of ϕ, then there is an isomorphism ψ from R/I to S. If κ is the canonical homomorphism from R to R/I the isomorphism ψ can be chosen such that $\psi = \phi \circ \kappa$.*

Exercise 2.6. In every ring R clearly R and the set $\{0\}$ are ideals. Prove that a commutative ring R (with at least two elements) is a field if and only if R and $\{0\}$ are the only ideals of R.

Definition 2.7. An ideal I of R is called a *principal ideal* if there exists an element a in I such that $I = \{ra \mid r \in R\}$. This is usually written $I = Ra$.

Example 2.8. In the ring $\mathbb{Z}$ of integers, every ideal has the form $\mathbb{Z}n$ for some n in $\mathbb{Z}$. Hence every ideal of $\mathbb{Z}$ is principal.

Example 2.9. If K is a field every ideal in the polynomial ring $K[x]$ has the form $K[x] \cdot f(x)$ for some polynomial $f(x)$ in $K[x]$. Hence every ideal of $K[x]$ is principal.

Definition 2.10. R is called a *principal ideal ring* ("PIR") if every ideal of R is a principal ideal.

Definition 2.11. R is called a *principal ideal domain*, (" PID") if R is an integral domain and every ideal of R is a principal ideal.

Example 2.12. $\mathbb{Z}$ and the polynomial ring $K[x]$ over a field K are principal ideal domains. The residue class ring $\mathbb{Z}/4\mathbb{Z}$ is not an integral domain, but every ideal is principal. Hence $\mathbb{Z}/4\mathbb{Z}$ is a principal ideal ring, but not a principal ideal domain.

While the polynomial ring in one variable over a field is a principal deal domain, the polynomial ring in more than one variable is not a principal ideal domain. Actually, in that case the ideal consisting of all polynomials with constant term 0 is not principal.

Next we introduce some important notions for ideals reflecting properties of the corresponding residue class rings.

Definition 2.13. An ideal I of the ring R, $I \neq R$, is called a *prime ideal* if the product of two elements a and b in R can only belong to I if either $a \in I$ or $b \in I$.

Theorem 2.14. *An ideal I of the ring R is a prime ideal if and only if R/I is an integral domain.*

Proof. "if": Assume R/I is an integral domain. Let a and b be any two elements of R not lying in I. The corresponding residue classes in R/I represented by a and b are non-zero in R/I; since R/I is an integral domain the product of these two residue classes is non-zero. This product is represented by $a \cdot b$, which therefore cannot lie in I. Hence I is a prime ideal.
"only if": Assume I is a prime ideal. Let a and b in R represent two non-zero residue classes $\bar{a}$ and $\bar{b}$ in R/I. Since I is a prime ideal, $a \cdot b$ is not in I. Now $a \cdot b$ represents the product $\bar{a} \cdot \bar{b}$ of the two residue classes which cannot be zero because $a \cdot b \notin I$. Hence R/I is an integral domain. $\square$

Example 2.15. In the ring $\mathbb{Z}$ of ordinary integers the prime ideals are the principal ideals generated by prime numbers and the zero ideal.

Definition 2.16. An ideal I of the ring R, $I \subsetneqq R$, is called *maximal*, if I is maximal among the ideals of R that are $\neq R$.

Theorem 2.17. *An ideal I of the ring R is a maximal ideal if and only if R/I is a field.*

Proof. "if": Assume R/I is a field. Let M be an ideal of R containing I as a proper subset. Choose an element $a \in M \setminus I$. The residue class $\bar{a}$ (with respect to I) is $\neq 0$, hence has an inverse, say $\bar{b}$, ($b \in R$) in the field R/I. Therefore $a \cdot b$ can be written as 1+(an element $\in I$). But this means that M contains 1 and therefore equals R.
"Only if": Assume I is a maximal ideal. Let $\bar{a}$, ($a \in R$) be a non-zero residue class in R/I. Clearly a is not in I. The set M of elements of the form $a \cdot r + c$, r running through the elements of R and c running through the elements of I, is an ideal M of R. Since a is not in I, the ideal M contains I strictly and hence $M = R$. This

implies that $1 = a \cdot r + c$ for some r in R and some c in I. But this in turn means that $\bar{1} = \bar{a} \cdot \bar{r}$ in R/I which therefore is a field. $\square$

Example 2.18. In the ring $R = \mathbb{Z}[x]$ the ideal $I = \{f(x) \in \mathbb{Z}[x] \mid f(0) = 0\}$ is a non-maximal prime ideal.

In this connection the following holds. We omit the proof.

Theorem 2.19. *Every non-zero prime ideal in a principal ideal domain is maximal.*

Important example 2.20 In the ring $\mathbb{Z}$ every non-zero prime ideal is the principal ideal generated by a prime number p. By the above result the residue class ring $\mathbb{Z}/\mathbb{Z}p$ is a field. This can also be checked immediately since every finite integral domain (with more than one element) is necessarily a field. This field is sometimes denoted $\mathbb{Z}_p$ and sometimes $\mathbb{F}_p$.

We shall also need the concept "factorial ring" or "ring with unique factorization", denoted by UFD. We shall refrain from giving detailed proofs, but just explain the notions and the basic results in this subject.

Let R be an integral domain. A non-zero element a in R which is not invertible is called an *irreducible element* if a has only trivial factorizations, i.e. $a = r \cdot s$, $r, s \in R$ implies that either r or s is invertible in R.

Two non-zero elements a and b of an integral domain R are called *associate* if they generate the same principal ideal, i.e. if $Ra = Rb$. It is easily checked that a and b are associate if and only if $a = b\cdot$(an invertible element) if and only if $b = a\cdot$(an invertible element).

R is called a UFD, if R is an integral domain and every non-invertible non-zero element in a "basically unique" way can be written as a product of irreducible elements. Here "basically unique" means the following: Assume an element a has two factorizations of irreducible elements:

$$a = \pi_1 \cdot \pi_2 \cdots \pi_n$$

and

$$a = \tilde{\pi_1} \cdot \tilde{\pi_2} \cdots \tilde{\pi_m},$$

then $m = n$ and after a suitable permutation of the π's every π_i , $i = 1, 2, \ldots, n$, is associate to $\tilde{\pi_i}$.

A characteristic property of UFD's is the following: If an irreducible element π divides a product $a \cdot b$ then π divides one of the factors a and b. In other words the principal ideal generated by an irreducible element is a prime ideal.

The classical examples of UFD's are the ring $\mathbb{Z}$ of ordinary integers and the ring of polynomials in one variable over a field.

Those two rings are PID's. A general result is the following which we state without proof:

Theorem 2.21. *Every principal ideal domain is a unique factorization domain.*

Remark 2.22. The converse is not true. The ring of polynomials in more than one variable over a field is not a principal ideal domain, but it can be shown to be a unique factorization domain.

In a UFD the principal ideal generated by an irreducible element is a non-zero prime ideal. If R is a PID an ideal I of R is a non-zero prime ideal exactly when $I = R\pi$ for some irreducible element π in R. Combining this remark with Theorem 2.19 we get:

Theorem 2.23. *Let R be a principal ideal domain. A non-zero ideal of R is a prime ideal if and only if it has the form $R\pi$ for some irreducible element π. For any non-zero prime ideal $R\pi$ the residue class ring $R/R\pi$ is a field.*

FACTORIZATIONS OF POLYNOMIALS.

We consider the polynomial ring $R[x]$, where R is either a field or a PID, (in particular for instance R being the ring of integers).

The following observation is often useful: Let φ be a homomorphism of R onto R^*, where R and R^* are commutative rings. The mapping

$$\Phi(r_0 + r_1x + \cdots + r_nx^n) = \varphi(r_0) + \varphi(r_1)x + \cdots + \varphi(r_n)x^n$$

defines a homomorphism Φ of $R[x]$ onto $R^*[x]$. □

Definition 2.24. A polynomial $f(x) = a_0 + \cdots + a_nx^n \in \mathbb{Z}[x]$ is called *primitive*, if the greatest common divisor $(a_0, \ldots, a_n)$ is 1. In particular, if $f(x) = a_0 + \cdots + a_nx^n \in \mathbb{Z}[x]$, is monic, i.e. $a_n = 1$, then $f(x)$ is primitive.

Theorem 2.25. *(Gauss). The product of two primitive polynomials $f(x)$ and $g(x)$ is primitive.*

Proof. Indirectly. Assume $f(x) \cdot g(x)$ were not primitive; then there would exist a prime number p such that p divides all coefficients of $f(x)g(x)$.

Consider the homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}_p = \mathbb{F}_p$ defined by sending an integer into its residue class modulo p. Then $\Phi(f) \neq 0$ and $\Phi(g) \neq 0$, but $\Phi(f \cdot g) = 0$, which is a contradiction since Φ is a homomorphism and $\mathbb{Z}_p[x]$ is an integral domain. □

Lemma 2.26. *Let $f(x)$ be a primitive polynomial in $\mathbb{Z}[x]$, and $q \in \mathbb{Q}$. Then $q = \pm 1$ if $qf(x)$ is a primitive polynomial.*

Proof. Write $q = \frac{r}{s}$, where r and s are mutually prime integers. Let $f(x) = a_0 + \cdots + a_nx^n$. Then $\frac{r}{s}(a_0 + \cdots + a_nx^n) = \frac{ra_0}{s} + \cdots + \frac{ra_n}{s}x^n \in \mathbb{Z}[x] \Rightarrow s|ra_i \ \forall i \Rightarrow s|a_i \ \forall i \Rightarrow$

$s = \pm 1$ (since $f(x)$ is primitive). Hence $\frac{r}{s} f(x) = r\left(\frac{a_0}{s} + \cdots + \frac{a_n}{s} x^n\right)$ is primitive $\Rightarrow r = \pm 1$. $\square$

The proofs of the following lemmas are quite straightforward and are left to the reader.

Lemma 2.27. *For any non-zero polynomial $f(x)$ in $\mathbb{Q}[x]$ there exists a rational number q such that $qf(x)$ is primitive.*

Lemma 2.28. *Let $f(x)$ be a polynomial in $\mathbb{Z}[x]$. If q is a rational number such that $qf(x)$ is primitive then $1/q$ is an integer.*

Lemma 2.29. *If $f(x)$ is primitive and $f(x) = g(x)h(x)$, $g(x)$ and $h(x)$ being polynomials in $\mathbb{Z}[x]$, then $g(x)$ and $h(x)$ are primitive.*

Remark 2.30. The invertible elements in $\mathbb{Z}[x]$ are ± 1.

Theorem 2.31. *Let $f(x)$ be a polynomial in $\mathbb{Z}[x]$. Then:*

i) *Degree $f(x) = 0$: $f(x)$ is irreducible in $\mathbb{Z}[x] \Leftrightarrow f(x) = \pm p$, p for a prime number p.*
ii) *Degree $f(x) > 0$: $f(x)$ is irreducible in $\mathbb{Z}[x] \Leftrightarrow f(x)$ is primitive and $f(x)$ is irreducible in $\mathbb{Q}[x]$.*

Proof. i) is clear.

ii) $\Leftarrow$ assume $f(x)$ had a non-trivial factorization $f(x) = g(x)h(x)$, $g(x)$ and $h(x) \in \mathbb{Z}[x]$, where $g(x)$, $h(x)$ are not invertible i $\mathbb{Z}[x]$.

Since $f(x)$ is primitive the degrees of $g(x)$ and $h(x)$ must be > 0, hence $f(x)$ would have a non-trivial decomposition in $\mathbb{Q}[x]$. Contradiction!

$\Rightarrow$ It is clear, that $f(x)$ must be primitive. Assume $f(x)$ had a non-trivial factorization in $\mathbb{Q}[x]$: $f(x) = g(x)h(x)$, $g(x)$ and $h(x)$ not being constants.

By lemma 2.27 there exist rational numbers q_1 and q_2 such that $q_1 g(x)$ and $q_2 h(x)$ are primitive.

$$q_1 q_2 f(x) = [q_1 g(x)][q_2 h(x)]\,.$$

By Gauss' theorem $q_1 q_2 f(x)$ is primitive. Since $f(x)$ is primitive, lemma 2.26 implies that $q_1 q_2 = \pm 1$, and hence

$$f(x) = (\pm\, q_1 g(x)) \cdot (q_2 h(x))$$

Thus $f(x)$ would have a non-trivial factorization in $\mathbb{Z}[x]$. Consequently $f(x)$ must be irreducible as an element in $\mathbb{Q}[x]$. $\square$

Theorem 2.32. *$\mathbb{Z}[x]$ is a UFD.*

Proof. 1) Every $f(x) \in \mathbb{Z}[x]$ is a product of irreducible polynomials. Indeed, if $f(x)$ is constant, i.e. is an ordinary integer, then the assertion follows since $\mathbb{Z}$ is a UFD. If a polynomial in $\mathbb{Z}[x]$ has positive degree, it can be written as (a non-zero integer)$\cdot$(a primitive polynomial). Therefore it suffices to show that any primitive polynomial $f(x)$ is a product of irreducible polynomials. We proceed by induction on the degree of the polynomial. If the degree is one the assertion is clear. Assume the assertion has been proved for all primitive polynomials of degree $< n$. Let $f(x)$ be a primitive polynomial of the degree n. If $f(x)$ is irreducible we are done. Otherwise $f(x)$ is a product of two polynomials of degrees $< n$. By lemma 2.29 these polynomials are primitive. By the inductive assumption each of the polynomials are products of irreducible polynomials. But then $f(x)$ is also a product of irreducible polynomials in $\mathbb{Z}[x]$.

2) To prove the uniqueness it suffices to show, that if $p(x)$ is irreducible in $\mathbb{Z}[x]$, then
$p(x)|f(x) \cdot g(x),\ f(x), g(x) \in \mathbb{Z}[x] \Rightarrow p(x)|f(x)$ or $p(x)|g(x)$.

There are two possibilities for $p(x)$:

i) $p(x) = \pm p$, where p is a prime number.
ii) $p(x)$ has positive degree, $p(x)$ is primitive and irreducible in $\mathbb{Q}[x]$.

ad i) $p|f(x)g(x)$; consider

$$\begin{array}{lll} \text{the homomorphism} & \varphi : \mathbb{Z} \to \mathbb{Z}_p & \text{and} \\ \text{the homomorphism} & \Phi : \mathbb{Z}[x] \to \mathbb{Z}_p[x] & \end{array}$$

Then $0 = \Phi(f(x)g(x)) = \Phi(f(x)) \cdot \Phi(g(x))$.

Since $\mathbb{Z}_p[x]$ is an integral domain, $\Phi(f(x))$ or $\Phi(g(x))$ must be 0, i.e.: $p|f(x)$ or $p|g(x)$.

ad ii) Since $p(x)|f(x)g(x)$ in $\mathbb{Z}[x]$ it follows that $p(x)|f(x)g(x)$ in $\mathbb{Q}[x]$.

Because $p(x)$ is irreducible in $\mathbb{Q}[x]$ and $\mathbb{Q}[x]$ is UFD, we conclude that $p(x)|f(x)$ or $p(x)|g(x)$ in $\mathbb{Q}[x]$. Assume for instance that $p(x)|f(x)$ in $\mathbb{Q}[x]$. Then we have

$$f(x) = p(x)h(x)\,, \quad h(x) \in \mathbb{Q}[x]\,.$$

By lemma 2.27 there exists q in Q such that $qh(x)$ is primitive. Consequently we get

$$qf(x) = p(x) \cdot (qh(x))\,.$$

As before (Gauss' Theorem) $qf(x)$ must be primitive. By lemma 2.28 we can write $q = 1/s$ for some integer s. Hence: $h(x) = s(qh(x)) \in \mathbb{Z}[x]$, and thus $p(x)|f(x)$ in $\mathbb{Z}[x]$.

Similarly if $p(x)|g(x)$ in $\mathbb{Q}[x]$ we conclude that $p(x)|g(x)$ in $\mathbb{Z}[x]$. $\square$

Remark 2.33. With minor obvious modifications the above proof carries over to the case where $\mathbb{Z}$ is replaced by an arbitrary UFD. In other words, generally we have:

Theorem 2.34. *R is a UFD $\Rightarrow$ $R[x]$ is a UFD.*

Corollary to Theorem 2.34. *For any field K the polynomial ring $K[x_1, \ldots, x_n]$ is a UFD.*

Remark 2.35. For later explicit applications a special case of Theorem 2.31 is very important: A monic polynomial in $\mathbb{Z}[x]$ is irreducible as an element in $\mathbb{Q}[x]$ if and only if it irreducible as an element in $\mathbb{Z}[x]$.

Theorem 2.36 (Schönemann-Eisenstein's irreducibility criterion). *A polynomial $f(x) \in \mathbb{Z}[x]$ of the form $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ is irreducible in $\mathbb{Q}[x]$, if there exists a prime number p, such that $p|a_{n-1}, \ldots, p|a_1$, $p|a_0$, $p^2 \nmid a_0$.*

Proof. By Theorem 2.31 (cf. the above remark 2.35) it suffices to show, that $f(x)$ is irreducible in $\mathbb{Z}[x]$.

Assume there were a factorization $f(x) = g(x) \cdot h(x)$, where $g(x)$ and $h(x) \in \mathbb{Z}[x]$ and $g(x)$ and $h(x)$ both were of degree $< n$.

We may assume that $g(x)$ and $h(x)$ were monic, i.e. had highest coefficient $= 1$. For the homomorphism $\mathbb{Z} \xrightarrow[\varphi]{} \mathbb{Z}_p$ and its induced homomorphism $\mathbb{Z}[x] \xrightarrow[\Phi]{} \mathbb{Z}_p[x]$ we get

$$\Phi(f(x)) = x^n = \Phi(g(x)) \cdot \Phi(h(x)) \Rightarrow \Phi(g(x)) = x^m\,;\ \Phi(h(x)) = x^{n-m}$$

for a suitable m, $1 \leq m \leq n-1$. This implies that all coefficients of $g(x)$ and $h(x)$ except the highest one are divisible by p; in particular p would divide $g(0)$ and $h(0)$ and thereby $p^2 | g(0)h(0) = f(0) = a_0$. Contradiction! $\square$

Example 2.37 . $\frac{x^n-1}{x-1}$ is irreducible in $\mathbb{Q}[x] \Leftrightarrow n =$ prime number.

Proof. $\Rightarrow$: assume n is composite $n = n_1 n_2$, $1 < n_1 < n$. Then

$$\frac{x^n - 1}{x - 1} = \frac{x^{n_1 n_2} - 1}{x - 1} = \frac{x^{n_1} - 1}{x - 1}\left[(x^{n_1})^{n_2 - 1} + \cdots + x^{n_1} + 1\right]$$

is reducible.

$\Leftarrow$ assume n is a prime number p. Then $f(x) = \frac{x^p-1}{x-1}$ is irreducible $\Leftrightarrow f(x+1)$ is irreducible.

Now by explicit expansion we get

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

Since p is a prime number, p divides $\binom{p}{j}$ for $1 \leq j \leq p-1$, and $p^2 \nmid \binom{p}{p-1} = p$. Hence Theorem 2.36 shows the irreducibility of $\frac{x^p-1}{x-1}$. $\square$

Remark 2.38. Theorem 2.36 easily carries over to polynomials over a UFD:

Let R be UFD and K its field of fractions. Let π be an irreducible element in R and $f(x) = x^n + r_{n-1}x^{n-1} + \cdots + r_0$ a polynomial in $R[x]$ for which π divides r_i, $0 \leq i \leq n-1$, while r_0 is not divisible by π^2, then $f(x)$ is irreducible in $K[X]$.

Example 2.39. $f(x,y) = x^n + y^n - 1$ is irreducible in $\mathbb{Q}[x,y]$ for any natural number n. Indeed, just consider $f(x, y+1)$ as an element of $(\mathbb{Q}[y])[x]$ and use the above remark with $\pi = y$.

Exercise 2.40. $f(x) = \Pi_{i=1}^n (x - a_i) - 1$, where $a_1, \ldots, a_n$ are distinct numbers in $\mathbb{Z}$, is irreducible in $\mathbb{Q}[x]$. (Is there a similar result for $\Pi_{i=1}^n (x - a_i) + 1$?)

Finally we give an example where we use that every polynomial over $\mathbb{Q}$ has roots in the complex field $\mathbb{C}$:

Example 2.41. Let $f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x \pm p$ be a polynomial in $\mathbb{Z}[x]$ where p is a prime number. Then $f(x)$ is irreducible, if $p > 1 + \mid a_1 \mid + \cdots + \mid a_{n-1} \mid$.

Proof. Assume $f(x)$ had a non-trivial factorization $f(x) = g(x)h(x)$ in $\mathbb{Z}[x]$. Then $f(0) = g(0)h(0) = \pm p$ would imply that one of the factors $g(0)$ or $h(0)$, say $g(0)$, were ± 1. The product of the roots of $g(x)$ would then be ± 1. In particular, there would be at least one root α of absolute value $\leqq 1$ .Since α is also a root of $f(x)$ we would get: $\alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha = \pm p$, which - by taking absolute values - would imply $1 + \mid a_1 \mid + \cdots + \mid a_{n-1} \mid \geqq p$. Contradiction!

Two philosophical questions:

Let n be a "random" natural number. What is most probable: That n is a prime number or that n is a composite number?

Let $f(x)$ be a "random" polynomial in $\mathbb{Q}[x]$. What is most probable: That $f(x)$ is an irreducible polynomial or that $f(x)$ is a reducible polynomial?

SYMMETRIC POLYNOMIALS.

Let K be a field. A polynomial $f(x_1, ..., x_n) \in K[x_1, ..., x_n]$ is called symmetric, if it is invariant under every permutation of the indeterminates $x_1, ...x_n$, i.e. if

$$f(x_1, ..., x_n) = f(x_{\sigma(1)}, ..., x_{\sigma(n)})$$

for every permutation $\sigma \in S_n$.

Example 2.42. The polynomials

$s_1 = x_1 + \cdots + x_n$ $\binom{n}{1}$ terms

$s_2 = x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n$ $\binom{n}{2}$ terms

$s_3 = x_1x_2x_3 + \cdots + x_{n-2}x_{n-1}x_n$ $\binom{n}{3}$ terms

...

$s_n = x_1x_2 \cdots x_n$ $\binom{n}{n}$ terms

are symmetric.

This may either been seen directly or by considering the polynomial

$$(T-x_1)(T-x_2)\cdots(T-x_n) = T^n - s_1T^{n-1} + s_2T^{n-2} + \cdots + (-1)^n s_n$$

which is invariant under every permutation of $x_1 ..., x_n$; therefore all the coefficients are also invariant under every permutation of $x_1, ..., x_n$.

These polynomials $s_1, ..., s_n$ are called the *elementary symmetric polynomials* in $x_1, ..., x_n$.

It is clear, that every polynomial in the elementary symmetric polynomial is symmetric in $x_1, ..., x_n$.

The converse also holds true, as the following important theorem shows.

Theorem 2.43. The main theorem about symmetric polynomials.

Every symmetric polynomial $f(x_1, ..., x_n) \in K[x_1, ..., x_n]$, where K is an arbitrary field, can in exactly one way be written as a polynomial (with coefficients in K) in the elementary symmetric polynomials $s_1, ..., s_n$. In other words: for every symmetric polynomial $f(x_1, .., x_n) \in K[x_1, .., x_n]$ there exists a unique polynomial $g(y_1, ..., y_n) \in K[y_1, ..., y_n]$, such that

$$f(x_1, ..., x_n) = g(x_1 + \cdots + x_n, x_1x_2 + \cdots, ..., x_1 \cdots x_n).$$

Before giving the proof here are some general remarks about polynomials in several indeterminates.

Every polynomial in $x_1, ..., x_n$ can be written

$$f(x_1, ..., x_n) = \sum_{i_1,...,i_n} a_{i_1,...,i_n} x_1^{i_1} ... x_n^{i_n}$$

where $a_{i_1,\cdots,i_n}$ are elements in K.

The *degree* of a term $a_{i_1,...,i_n} x_1^{i_1} ... x_n^{i_n}$, $a_{i_1,...,i_n} \neq 0$ is defined as $i_1 + \cdots + i_n$.

By the *degree* of a non-zero polynomial f we mean the highest degree of a term $(\neq 0)$ in f.

For polynomials in more than one indeterminate the degree of the terms is not enough to determine an ordering of these. Therefore we introduce the concept *signature.* By the signature of a term $a_{i_1,...,i_n} x_1^{i_1} \cdots ... x_n^{i_n}$ we mean the n-tuple $\mathbf{i} = (i_1, ..., i_n)$.

We order the set of signatures by first ordering them according to the degree and then ordering terms of the same degree lexicographically. This means that for two different signatures $(i_1, ..., i_n)$ and $(j_1, ..., j_n)$ we have

$$(i_1, ..., i_n) \prec (j_1, ..., j_n)$$

if either $i_1 + \cdots + i_n < j_1 + \cdots + j_n$ or if $i_1 + \cdots + i_n = j_1 + \cdots + j_n$ then $i_\nu < j_\nu$ for the smallest ν for which $i_\nu \neq j_\nu$.

Lemma 2.44. *The product of two non-zero polynomials in $K[x_1, ..., x_n]$, where K is a field, is non-zero, and the term of highest signature in product is the product of the terms of highest signature in the two polynomials.*

Proof. Exercise.

We now return to the proof of the main theorem.

First *the existence:*

Let $f \in K[x_1, ..., x_n]$ be symmetric. We may assume $f \neq 0$.

Let $\mathcal{A} = cx_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$ be the term in f of highest signature.

We remark that since f is symmetric, we get $i_1 \geq i_2 \geq ... \geq i_n$. Indeed, assume $i_\mu > i_\nu$ for some $\mu > \nu$. Since f is left fixed when permuting x_μ and x_ν the polynomial f must also contain the term $cx_1^{i_1} x_2^{i_2} \cdots x_\nu^{i_\mu} \cdots x_\mu^{i_\nu} \cdots x_n^{i_n}$. But the signature of that term is higher than that of $\mathcal{A} = cx_1^{i_1} x_2^{i_2} \cdots x_\nu^{i_\nu} \cdots x_\mu^{i_\mu} \cdots x_n^{i_n}$.

The terms of highest signature in the elementary symmetric polynomials $s_1, s_2, ..., s_n$ are x_1, x_1x_2,..., $x_1x_2 \cdots x_n$.

By virtue of the above lemma for any non-negative integers $j_1, j_2, ..., j_n$ the term of highest signature in the product $s_1^{j_1} s_2^{j_2} \cdots s_n^{j_n}$, viewed as a polynomial in $x_1, x_2, ..., x_n$, is

$$x_1^{j_1} (x_1x_2)^{j_2} \cdots (x_1x_2 \cdots x_n)^{j_n}$$

The corresponding signature is

$$(j_1 + j_2 + \cdots + j_n, j_2 + \cdots + j_n, ..., j_n)$$

If we now choose $j_1 = i_1 - i_2, j_2 = i_2 - i_3, ..., j_{n-1} = i_{n-1} - i_n$ and $j_n = i_n$, (which in view of the above remark are non-negative integers), this signature is just $(i_1, i_2, ..., i_n)$.

The difference $f - cs_1^{j_1} s_2^{j_2} ... s_n^{j_n}$ therefore is either 0 or a symmetric polynomial ($\neq 0$) for which the term of highest signature is less than $(i_1, i_2, ..., i_n)$. If this difference is 0 the proof is done. Otherwise we apply the same procedure on $f - cs_1^{j_1} s_2^{j_2} ... s_n^{j_n}$ etc.. In this way we eventually reach the zero polynomial, since there are only finitely many signatures less than a given one.

Now *the uniqueness*:

It clearly suffices to show that for $g(y_1, ..., y_n) \in K[y_1, ..., y_n], g(y_1, ..., y_n) \neq 0$ the polynomial $g(s_1, ..., s_n) = g(x_1 + x_2 + \cdots + x_n, x_1x_2 + \cdots, ..., x_1x_2 \cdots x_n)$ is not the zero polynomial.

Let $dy_1^{t_1} y_2^{t_2} ... y_n^{t_n}, d \neq 0$ be a term in g. If we for $y_1, y_2, ..., y_n$ substitute the elementary symmetric polynomials $s_1, s_2, ... s_n$ the argument above shows that we get a polynomial in $x_1, x_2, ..., x_n$ in which the term of highest signature is

$$dx_1^{t_1} (x_1x_2)^{t_2} \cdots (x_1x_2 \cdots x_n)^{t_n}.$$

The signature of this term is

$$(t_1 + t_2 + \cdots + t_n, t_2 + \cdots + t_n, ..., t_n).$$

If we now first consider the terms in g for which $t_1 + t_2 + \cdots + t_n$ is biggest, then among these terms those for which $t_2 + \cdots + t_n$ is biggest, etc. in g we get separated a certain term $dy_1^{t_1} y_2^{t_2} ... y_n^{t_n}$ with the property that this and only this term by substitution of the elementary symmetric polynomials gives rise to a term with signature $(t_1 + t_2 + \cdots + t_n, t_2 \cdots + t_n, ..., t_n)$.

This term can not be cancelled away against any other term. Consequently $g(x_1 + x_2 + \cdots + x_n, x_1x_2 + \cdots ..., ..., x_1x_2 \cdots x_n)$ is not the zero polynomial. $\square$

ALGEBRAIC EXTENSIONS.

Let K be a subfield of the field L. For an element $\alpha \in L$ we denote by $K[\alpha]$ *the smallest subring of* L *containing* K *and* α. The ring $K[\alpha]$ consists of all elements in L that can be written in the form $k_0 + k_1\alpha + \cdots + k_n\alpha^n$, $k_i \in K$, $n \in \mathbb{N}$.

By $K(\alpha)$ we denote *the smallest subfield of* L *containing* K *and* α. The field $K(\alpha)$ consists of all elements in L that can be written in the form

$$\frac{k_0 + k_1\alpha + \cdots + k_n\alpha^n}{k_0' + k_1'\alpha + \cdots + k_n'\alpha^n},$$

k_i, $k_i' \in K$, $n \in \mathbb{N}$ and the denominator $\neq 0$.

$K(\alpha)$ is clearly the field of fractions of $K[\alpha]$.

For a given $\alpha \in L$, $L \supseteqq K$ we consider the homomorphism $\Phi : K[x] \to K[\alpha]$ defined by $\Phi(f(x)) = f(\alpha)$. Clearly Φ is surjective.

We distinguish between two cases:

1) $\operatorname{Ker}\Phi = 0$, i.e. $K[\alpha] \simeq K[x]$ which is not a field. In this case $K(x)$ is isomorphic to $K(\alpha)$ and we say that α is *transcendent over* K.

2) $\operatorname{Ker}\Phi \neq 0$. Since $\operatorname{Ker}\Phi$ is an ideal in $K[x]$ and $K[x]$ is a PID, the kernel $\operatorname{Ker}\Phi$ is the principal ideal $K[x]p(x)$ generated by a polynomial $p(x) \neq 0$. By the epimorphism theorem for rings (Theorem 2.5) we get

$$K[x]/\operatorname{Ker}\Phi \simeq K[\alpha].$$

$\operatorname{Ker}\Phi$ is therefore a prime ideal $\neq 0$. Since $K[x]$ is a PID, $\operatorname{Ker}\Phi$ is a maximal ideal (Theorem 2.19), therefore (Theorem 2.17) $K[\alpha]$ is a field and hence $K(\alpha) = K[\alpha]$.

In this case α is called *algebraic over* K. That α is algebraic over K thus means, that α is root of a proper polynomial (i.e. $\neq 0$) with coefficients in K.

Now $\operatorname{Ker}\Phi = K[x]p(x)$, where $p(x)$ is uniquely determined up to an invertible factor in $K[x]$, i.e.: up to an constant in K. The uniquely determined monic (i.e.: highest coefficient $= 1$) polynomial in $K[x]$ generates $\operatorname{Ker}\Phi$ and is denoted $\operatorname{Irr}(\alpha, K)$. This polynomial is irreducible in $K[x]$, (cf. Theorem 2.23).

Let $f(x) \in K[x]$ be a polynomial for which $f(\alpha) = 0$. Then $f(x) = \operatorname{Irr}(\alpha, K) \cdot g(x)$ for some $g(x) \in K[x]$. This implies, that $\operatorname{Irr}(\alpha, K)$ *can be characterized as the uniquely determined monic irreducible polynomial in* $K[x]$ *having* α *as a root.*

$\operatorname{Irr}(\alpha, K)$ can also be characterized as the uniquely determined monic polynomial in $K[x]$ of lowest degree having α as a root. Therefore $\operatorname{Irr}(\alpha, K)$ is sometimes called α's minimal polynomial w.r.t. K.

From the above we, in particular, conclude that a polynomial in $K[x]$ has α as a root if and only if it is divisible by $\operatorname{Irr}(\alpha, K)$.

Using the division algorithm every polynomial $f(x) \in K[x]$ can be written uniquely in the form

$$f(x) = \mathrm{Irr}(\alpha, K) \cdot g(x) + r(x)\,, \quad \text{degree } r(x) < n := \text{degree}\,\mathrm{Irr}(\alpha, K).$$

If we in this equation insert α for x we get $f(\alpha) = r(\alpha)$, hence every element in $K[\alpha]$ can be written

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}\,, \quad a_0, \ldots, a_{n-1} \in K\,.$$

This representation is unique. Indeed, assume that an element β in $K[\alpha]$ had the representations

$$\beta = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$$

and

$$\beta = a'_0 + a'_1\alpha + \cdots + a'_{n-1}\alpha^{n-1},$$

where $a_0, a_1, ..., a'_0, a'_1, ...$ belong to K, then α would be root of the polynomial $a_0 - a'_0 + (a_1 - a'_1)x + \cdots + (a_{n-1} - a'_{n-1})x^{n-1}$. But α is not a root in any non-zero polynomial i $K[x]$ of degree $< n$; this implies that $a_0 - a'_0 = a_1 - a'_1 = \cdots = a_{n-1} - a'_{n-1} = 0$ and thus $a_0 = a'_0, a_1 = a'_1, \cdots, a_{n-1} = a'_{n-1}$.

Thus every element in $K[\alpha] = K(\alpha)$ can be written uniquely as a K-linear combination of $1, \alpha, \ldots, \alpha^{n-1}$. We may express this by saying that $K[\alpha] = K(\alpha)$ viewed as a vector space over K has $1, \alpha, \ldots, \alpha^{n-1}$ as a basis, in particular, this vector space has dimension n. This dimension is denoted $[K(\alpha) : K]$ and thus equals degree$(\mathrm{Irr}(\alpha, K))$, which is called α's *degree w.r.t. K*.

Definition 2.45. An extension $L \supseteq K$ of fields is called *algebraic*, if every element in L is algebraic over K. We often just write: L/K is algebraic.

Before continuing we bring some general remarks, which we shall need a lot of times.

If L is an extension field of K and $\alpha_1, \cdots, \alpha_s$ are elements in L we denote by $K(\alpha_1, \ldots, \alpha_s)$ the smallest subfield of L containing K and $\alpha_1, \ldots, \alpha_s$. It is clear, that $K(\alpha_1, \ldots, \alpha_s) = K(\alpha_1) \ldots (\alpha_s)$.

An extension field L of K can be considered as a vector space over K and thus has a dimension (i.e. the number of elements of a basis), which is denoted $[L : K]$. If this dimension is a finite number n any family of m elements $\omega_1, \ldots, \omega_m$, $m > n$, will be linearly dependent over K, i.e. there exist elements $k_1, \cdots, k_m \in K$, not all 0 such that $k_1\omega_1 + \cdots + k_m\omega_m = 0$.

Theorem 2.46. *Let L be a field extension of K for which $[L:K] < \infty$. Then L/K is algebraic.*

Proof. Assume $[L:K] = n < \infty$. For every element α in L the elements $1, \alpha, \alpha^2, \ldots, \alpha^n$ are linearly dependent over K; hence there exist elements $k_0, k_1, \ldots, k_n$ in K, not all 0, such that

$$k_0 + k_1\alpha + \cdots + k_n\alpha^n = 0\,.$$

Consequently α is a root of the non-zero polynomial

$$k_0 + k_1x + \cdots + k_nx^n \in K[x]\,.$$

Thus every element α in L is algebraic over K. □

Theorem 2.47. (Transitivity Theorem). *Let $K \subseteqq L \subseteqq M$ be fields. Then $[M:K] = [M:L]\,[L:K]$, where $[M:L]$ and $[L:K]$ are assumed to be finite.*

Proof. If $\alpha_1, \alpha_2, \ldots, \alpha_s$ form a K-basis for L and $\beta_1, \beta_2, \ldots, \beta_t$ a L-basis for M, then $\alpha_i\beta_j$, $1 \leqq i \leqq s$, $1 \leqq j \leqq t$, form a K-basis for M.

For this we have to show two things:

i) The elements $\alpha_i\beta_j$, $1 \leqq i \leqq s$, $1 \leqq j \leqq t$, are linearly independent over K.

ii) Every element in M can be written as a K-linear combination of the elements $\alpha_i\beta_j$, $1 \leqq i \leqq s$, $1 \leqq j \leqq t$.

Ad i) Assume

$$\sum_{i,j} k_{ij}\alpha_i\beta_j = 0,$$

where the k_{ij}'s belong to K. This equation can be written

$$\sum_j (\sum_i k_{ij}\alpha_i)\beta_j = 0$$

For each j the inner sum is an element in L. Since the elements $\beta_j, 1 \leqq j \leqq n$, are independent over L, we get

$$\sum_i k_{ij}\alpha_i = 0$$

for every j, $1 \leqq j \leqq n$.

Since the elements $\alpha_i, 1 \leqq i \leqq s$, are linearly independent over K, we conclude that $k_{ij} = 0$ for all $i, 1 \leqq i \leqq s$ and all $j, 1 \leqq j \leqq t$.

Ad ii) Let ξ be an element in M. Since $\beta_j, 1 \leqq j \leqq t$ form a L-basis for M, we can write ξ as

$$\xi = \sum_j \ell_j\beta_j,$$

where each ℓ_j lies in L. Since $\alpha_i, 1 \leqq i \leqq s$, form a K-basis for L, each ℓ_j can be written

$$\ell_j = \sum_i k_{ij}\alpha_i,$$

where every k_{ij} lies in K. This implies

$$\xi = \sum_{i,j} k_{ij}\alpha_i\beta_j.$$

Thus ii) has been proved. □

Remark 2.48. The transitivity theorem is extremely important in explicit computations. A particular application is the following: Let M/K be a finite extension and L any field between K and M, $K \subseteqq L \subseteqq M$. Then $[L : K]$ divides $[M : K]$.

To take an explicit example let α be the real root of any irreducible polynomial in $\mathbb{Q}[x]$ of degree 3. Then $\sqrt{2}$ is not contained in $\mathbb{Q}(\alpha)$. (A direct verification without use of the above remark is not completely trivial.)

Another example is the following. Let a and b be rational numbers such that neither a, b or ab is the square of a rational number. Then $\sqrt{a} \notin \mathbb{Q}$ and $\sqrt{b} \notin (\mathbb{Q}(\sqrt{a}))$ (why?). This implies that
$[\mathbb{Q}(\sqrt{a}, \sqrt{b}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{a}, \sqrt{b}) : \mathbb{Q}(\sqrt{a})] \cdot [\mathbb{Q}(\sqrt{a}) : \mathbb{Q}] = 2 \cdot 2 = 4.$

Theorem 2.49. *Let L be a field extension of K, and let α and β be elements in L which are algebraic over K. Then $\alpha + \beta$, $\alpha - \beta$, $\alpha \cdot \beta$ and α/β, ($\beta \neq 0$) are also algebraic over K.*

Proof. $K(\alpha) = K[\alpha]$ is a finite dimensional vector space over K. Since β in particular is algebraic over $K(\alpha) = K[\alpha]$, it follows that $(K(\alpha))(\beta) = K(\alpha, \beta)$ is finite dimensional over $K(\alpha)$. By theorem 2.47 $K(\alpha, \beta)$ has finite dimension over K. Therefore by theorem 2.46 the field $K(\alpha, \beta)$ is algebraic over K.

Since $\alpha + \beta$, $\alpha - \beta$, $\alpha \cdot \beta$ and α/β, ($\beta \neq 0$) lie in $K(\alpha, \beta)$, these elements are algebraic over K. □

Definition 2.50. Let L be a field extension of K. The subset of L consisting of the elements that are algebraic over K (which by the above theorem is a subfield of L) is called the *algebraic closure of* K in L and is denoted $\overline{K}$.

Example 2.51. There exist infinite dimensional algebraic field extensions. Let $L = \mathbb{R}$ and $K = \mathbb{Q}$. For every natural number n theorem 2.36 implies that $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$. Therefore the algebraic closure of $\mathbb{Q}$ in $L = \mathbb{R}$ has infinite dimension over $\mathbb{Q}$.

Theorem 2.52. *Let $K \subseteq L \subseteq M$ be fields. If L/K is algebraic, every element $\xi \in M$ that is algebraic over L is also algebraic over K.*

Proof. ξ is root of a non-zero polynomial in $L[x]$:

$$\xi^n + a_0\xi^{n-1} + \cdots + a_{n-1} = 0\,, \quad a_0, \ldots, a_{n-1} \in L\,.$$

Since a_0 is algebraic over K, the dimension $[K(a_0) : K]$ is finite.

Since a_1 is algebraic over K, in particular over $K(a_0)$, the dimension $[K(a_0, a_1) : K(a_0)]$ is finite.

Since a_2 is algebraic over K, in particular over $K(a_0, a_1)$, the dimension $[K(a_0, a_1, a_2) : K(a_0, a_1)]$ is finite.

etc.

Since a_{n-1} is algebraic over K, in particular over $K(a_0, \ldots, a_{n-2})$, the dimension $[K(a_0, \ldots, a_{n-1}) : K(a_0, \ldots, a_{n-2})]$ is finite.

Since ξ is algebraic over $K(a_0, \ldots, a_{n-1})$, the dimension $K(\xi, a_0, \ldots, a_{n-1}) : K(a_0, \ldots, a_{n-1})]$ is finite.

By successive application of the transitivity theorem it follows that the dimension $[K(\xi, a_0, \ldots, a_{n-1}) : K]$ is finite; therefore Theorem 2.46 shows that ξ is algebraic over K. $\square$

Corollary 2.53. (Transitivity for algebraic extensions). *Let $K \subseteq L \subseteq M$ be fields. Then M/L algebraic $\wedge$ L/K algebraic $\Rightarrow$ M/K algebraic.*

Corollary 2.54.. *Let $K \subseteq L$ be fields. Then $\overline{\overline{K}} = \overline{K}$.*

Exercise 2.55. Let α and β be complex numbers, that are algebraic over $\mathbb{Q}$ of degree p, resp. q. Show that $\alpha + \beta$ is algebraic over $\mathbb{Q}$ of degree pq, if p and q are distinct prime numbers.

– – – – – – – – – – – – – – – – –

ADJUNCTION OF A ROOT. SPLITTING FIELDS.

So far we have considered given existing field extensions and looked at polynomials vanishing on certain elements. Now we conversely consider a field K and a polynomial $p(x) \in K[x]$ and are looking for extensions of K in which $p(x)$ has a root.

Theorem 2.56. Existence theorem concerning adjunction of a root of an irreducible polynomial. *Let K be an arbitrary field and $p(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n$ an irreducible monic polynomial in $K[x]$. Then there exists a field L^* containing a subfield K^* with the following properties:*

1) *there exists an element α^* in L^* which is algebraic over K^* such that $L = K^*(\alpha^*)$;*
2) *there exists an isomorphism φ of K onto K^* such that $\operatorname{Irr}(\alpha^*, K^*) = \Phi(p(x))$, where Φ is the isomorphism of $K[x]$ onto $K^*[x]$ induced by φ.*

Proof. Let L^* be the residue class ring $K[x]/K[x]p(x)$, which is a field, since $p(x)$ is irreducible and $K[x]$ is an PID. For a polynomial $f(x) \in K[x]$ the corresponding residue class in L^* is denoted $\overline{f(x)}$. Then:

$$\begin{aligned} L^* &= \{\overline{k_0 + k_1 x + \cdots + k_{n-1}x^{n-1}} \mid k_0, k_1, \ldots, k_{n-1} \in K\} \\ &= \{\overline{k}_0 + \overline{k}_1\overline{x} + \cdots + \overline{k}_{n-1}\overline{x}^{n-1} \mid k_0, k_1, \ldots, k_{n-1} \in K\}. \end{aligned}$$

We set $K^* = \{\overline{k} \mid k \in K\}$, which becomes a subfield of L^*. The map defined by $\varphi(k) = \overline{k}$ is an isomorphism of K onto K^*. Now $\overline{x}$ is a root of the polynomial

$$\overline{a}_0 + \overline{a}_1 x + \cdots + \overline{a}_{n-1}x^{n-1} + x^n$$

which is irreducible in $K^*[x]$; hence

$$\operatorname{Irr}(\overline{x}, K^*) = \overline{a}_0 + \overline{a}_1 x + \cdots + \overline{a}_{n-1}x^{n-1} + x^n = \Phi(p(x)).$$

This proves the theorem, since $\overline{x}$ can be used as α^*. □

Remark to theorem 2.56 By identifying K with K^* we may consider L^* as an extension field of K in which $p(x)$ has a root. An extension (in the more immediate sense of the word) can be obtained by considering the (set theoretical) disjoint union of K and $L^* \setminus K^*$ and by the above construction "transplanting" the operations addition and multiplication in this union; in this way one obtains a field containing K as a subfield and containing a root of $p(x)$.

Theorem 2.57. Uniqueness concerning adjunction of a root of an irreducible polynomial. *Assume we have fields L, K, L^*, K^*, such that $L \supseteq K$, $L^* \supseteq K^*$, $L = K(\alpha)$, $L^* = K^*(\alpha^*)$, where α is algebraic over K and α^* algebraic over K^*. Assume further that there is an isomorphism φ from K onto K^* such that $\Phi \operatorname{Irr}(\alpha, K) = \operatorname{Irr}(\alpha^*, K^*)$, where Φ denotes the isomorphism from $K[x]$ onto $K^*[x]$ induced by φ. Then there exists a uniquely determined isomorphism $\widetilde{\varphi}$ from L onto L^* such that*

1) $\widetilde{\varphi}_{\mathrm{Res},K} = \varphi$;
2) $\widetilde{\varphi}(\alpha) = \alpha^*$.

Proof. Let $p(x) = \operatorname{Irr}(\alpha, K)$ and $p^*(x) = \operatorname{Irr}(\alpha^*, K^*)$ and assume these polynomials have the degree n.

We first prove the uniqueness of $\widetilde{\varphi}$. Evidently

$$L = \{k_0 + k_1\alpha + \cdots + k_{n-1}\alpha^{n-1} \mid k_0, k_1, \ldots, k_{n-1} \in K\}.$$

If there exists an isomorphism $\widetilde{\varphi}$ with the properties 1) and 2), then

$$\widetilde{\varphi}(k_0 + k_1\alpha + \cdots + k_{n-1}\alpha^{n-1}) = \varphi(k_0) + \varphi(k_1)\alpha^* + \cdots + \varphi(k_{n-1})(\alpha^*)^{n-1}.$$

Therefore there is at most one possibility for $\widetilde{\varphi}$.

Next we prove the existence of $\widetilde{\varphi}$.

There is an isomorphism

$$\varphi_1 : K[x]/(p(x) \to L$$

defined by $\varphi_1(\overline{f(x)}) = f(\alpha)$, $f(x) \in K[x]$ and an isomorphism

$$\varphi_2 : K^*[x]/(p^*(x)) \to L^*$$

defined by $\varphi_2(\overline{g(x)}) = g(\alpha^*)$, $g(x) \in K^*[x]$. Further the isomorphism

$$K[x] \xrightarrow{\Phi} K^*[x]$$

induces an isomorphism

$$K[x]/(p(x)) \xrightarrow{\widetilde{\Phi}} K^*[x]/(p^*(x))$$

by

$$\widetilde{\Phi}(\overline{f(x)} \text{ modulo } p(x)) = \overline{\Phi f(x)} \text{ modulo } p^*(x)\,,$$

thus in particular we have

$$\widetilde{\Phi}((\overline{x}) \text{ modulo } p(x)) = \overline{x} \text{ modulo } p^*(x)\,.$$

The composite mapping $\varphi_2 \circ \widetilde{\Phi} \circ \varphi_1^{-1}$ from L to L^* can be used as $\widetilde{\varphi}$ since

$$\varphi_2 \circ \widetilde{\Phi} \circ \varphi_1^{-1}(\alpha) = \alpha^*\,,$$

and $\varphi = \mathrm{Res}_K(\varphi_2 \circ \widetilde{\Phi} \circ \varphi_1^{-1})$. □

By successive applications of the existence theorem (Theorem 2.56) we get

Theorem 2.58. *Let K be a field and $f(x)$ an arbitrary polynomial in $K[x]$ of positive degree. Then there exists an extension field M of K in which $f(x)$ splits completely into linear factors (i.e. polynomials of degree one).*

Proof. We prove the assertion by induction on the degree n of the prescribed polynomium. If $n = 1$ the assertion is clear: We can use K itself.

Now let n be > 1. If $f(x)$ splits into linear factors in $K[x]$ there is nothing to prove. Otherwise $f(x)$ must be divisible by at least one polynomial $p(x)$ in $K[x]$ which is irreducible of degree > 1. By Theorem 2.56 there exists an extension field L of K in which $p(x)$ and thereby also $f(x)$ has a root α. In $L[x]$ we therefore can write $f(x) = (x - \alpha)g(x)$, where $g(x)$ is a polynomial in $L[x]$ of degree $n - 1$. By the inductive assumption there exists an extension field M of L in which $g(x)$ splits into

linear factors. But M is also an extension field of K, and in this extension field $f(x)$ splits into linear factors. $\square$

If $f(x)$ is a polynomial in $K[x]$ of positive degree n an extension field of K in which $f(x)$ splits into linear factors must contain elements $\alpha_1, \ldots, \alpha_n$, such that $f(x)$ up to a constant factor in K equals a product $(x-\alpha_1)\cdots(x-\alpha_n)$. The field generated over K by these elements is an extension field $M = K(\alpha_1, \ldots, \alpha_n)$ of K with the following two properties:
1) $f(x)$ splits into linear factors in $M[x]$.
2) $f(x)$ does not split completely into linear factors in any proper subfield of M containing K.
Definition. Let K be a field and $f(x)$ a polynomial in $K[x]$. An extension field M of K is called a *splitting field* for $f(x)$ over K, if $f(x)$ splits into linear factors in $M[x]$, while no proper subfield of M containing K has this property.

Theorem 2.58 implies that there exists a splitting field for every polynomial (of positive degree) over any field.

Remark 2.59. In general there will be a proper subset, $\{\alpha_1, \ldots, \alpha_t\}$, of the roots of $f(x)$, such that a splitting field equals $K(\alpha_1, \ldots, \alpha_t)$. In other words, for the formation of a splitting field some of the roots may be superfluous in the sense, that they "automatically follow suit" by adjunction of the other roots. If the degree n of $f(x)$ is > 1, the sum of the roots $\alpha_1 + \alpha_2 + \cdots + \alpha_n = -$ (the coefficient of x^{n-1}) and hence is an element in the base field K. Therefore $K(\alpha_1, \ldots, \alpha_{n-1}) = K(\alpha_1, \ldots, \alpha_n)$. Often even more roots may be superfluous. If e.g. $f(x) = x^4 - 2$ a splitting field (over $\mathbb{Q}$) can be obtained just by adjoining the roots $\sqrt[4]{2}$ og $\sqrt[4]{2} \cdot i$ where $i = \sqrt{-1}$.

We shall now prove the uniqueness of splitting fields.

Theorem 2.60. *Let K be a field and $f(x)$ a polynomial in $K[x]$ of positive degree, M a splitting field for $f(x)$ over K. Let K^* be a field isomorphic to K and let $\varphi : K \to K^*$ be an isomorphism. Let $f^*(x) = \Phi(f(x))$, where Φ is the isomorphism of $K[x]$ onto $K^*[x]$ induced by φ. Let M^* be a splitting field for $f^*(x)$ over K^*. Then φ can be extended to an isomorphism of M onto M^*.*

Proof. We use induction on the number of roots in the relative complement {the splitting field \ the base field}, i.e. the number of roots lying in the splitting field but not in the base field.

Let us first assume that this number is $= 0$. In that case $f(x)$ splits into linear factors in K and hence $M = K$ and $f^*(x)$ splits into linear factors in K^* so that $M^* = K^*$.

Assume now the theorem has been proved when the number of roots in the above set { splitting field \ base field } is $< n$. We must then prove that the theorem also holds when this number is $= n$.

So let the number of roots in $M \setminus K$ be n.

If $\alpha \in M \setminus K$, α is a root of $f(x)$ then $p(x) = \mathrm{Irr}(\alpha, K)$ divides $f(x)$ i.e.: $f(x) = p(x) \cdot h(x)$, where degree$(p(x))$ is > 1 and $h(x)$ is a polynomial in $K[x]$. In $K^*[x]$ we get a analogous splitting

$$f^*(x) = p^*(x) \cdot h^*(x)\,, \quad p^*(x) \text{ irreducible of the same degree as } p(x)\,.$$

Let $\alpha^* \in M^*$ be a root of $p^*(x)$. By the uniqueness theorem concerning adjunction of a root (Theorem 2.57) there exists a prolongation (actually uniquely determined) φ' of $\varphi : K(\alpha) \xrightarrow[\varphi']{} K^*(\alpha^*)$ such that $\varphi'(\alpha) = \alpha^*$.

In $K(\alpha)[x]$ the linear polynomial $x - \alpha$ divides $f(x)$:

$$f(x) = (x - \alpha) \cdot \cdots\cdots\,.$$

Similarly in $K^*(\alpha^*)[x]$ we have:

$$f^*(x) = (x - \alpha^*) \cdot \cdots\cdots\,.$$

Now we notice

M is a splitting field for $f(x)$ over $K(\alpha)$
and

M^* is a splitting field for $f^*(x)$ over $K^*(\alpha^*)$.

The number of roots of $f(x)$ in $(M \setminus K(\alpha)) <$ the number n of roots of $f(x)$ in $(M \setminus K)$. For the isomorphism Φ' of $K(\alpha)[x]$ onto $K^*(\alpha^*)[x]$ induced by φ' we get $\Phi'(f(x)) = f^*(x)$.

We now apply the inductive assumption on $f(x)$ over $K(\alpha)$ and conclude that φ' can be prolonged to an isomorphism from M onto M^*. $\square$

Comforting remark. The introduced abstract field extensions may at first seem a bit strange. However, in most cases (except the section about finite fields) one may assume that everything takes places inside the field $\mathbb{C}$ of complex numbers. In view of "the fundamental theorem of algebra" (every non-constant polynomial over $\mathbb{C}$ splits into linear factors over $\mathbb{C}$) the existence theorem concerning adjunction of roots and splitting fields become trivial. Hence, if we later consider splitting fields for polynomials over $\mathbb{Q}$ we may think of these fields as being subfields of the field of complex numbers.

GREATEST COMMON DIVISOR FOR POLYNOMIALS.

Let K be a field and $f(x)$ and $g(x)$ polynomials in $K[x]$. Since $K[x]$ is a PID, $f(x)$ and $g(x)$ has a greatest common divisor which we – to emphasize that $f(x)$ and $g(x)$ are viewed as polynomials in $K[x]$ – denote $(f(x), g(x))_K$. A priori the greatest common divisor is only determined up to a constant factor in K. To make it uniquely defined we require $(f(x), g(x))_K$ to be monic, i.e. such that the highest coefficient is 1.

For an extension $K \subseteq L$ of the base fields the following holds:

Theorem 2.61. *If K is a subfield of the field L, then $(f(x), g(x))_K = (f(x), g(x))_L$ for all polynomials $f(x)$, $g(x)$ in $K[x]$.*

Remark. Roughly speaking Theorem 2.61 says that greatest common divisor of two polynomials does not change by base field extension.

Proof of Theorem 2.61. Let $d_K = (f(x), g(x))_K$ and $d_L = (f(x), g(x))_L$. By the above definition both of them are monic. In $K[x]$ we have $d_K | f(x)$ and $d_K | g(x)$ and this also holds in $L[x]$. Therefore $d_K | d_L$ (in $L[x]$). Since d_K generates the ideal in $K[x]$ generated by $f(x)$ and $g(x)$, we conclude that $d_K = f(x)a(x) + g(x)b(x)$ for some polynomials $a(x)$ and $b(x)$ in $K[x]$. In $L[x]$ the polynomials $f(x)$ and $g(x)$ are divisible by d_L; consequently the above equation implies that $d_L | d_K$ (in $L[x]$). Thus d_K and d_L are monic polynomials for which $d_K | d_L$ and $d_L | d_K$. Therefore $d_K = d_L$. $\square$

Corollary 2.62. *Let K be a subfield of the field L and $f(x)$ and $g(x)$ polynomials in $K[x]$. If $f(x)$ divides $g(x)$ inside $L[x]$, then $f(x)$ also divides $g(x)$ inside $K[x]$.*

Proof. W.l.o.g. we may assume that $f(x)$ and $g(x)$ are monic. If $f(x)$ divides $g(x)$ in $L[x]$ then $(f(x), g(x))_L = f(x)$. By the above theorem $(f(x), g(x))_K = (f(x), g(x))_L$ and thus $(f(x), g(x))_K = f(x)$ implying that $f(x)$ divides $g(x)$ in $K[x]$. $\square$

CHARACTERISTIC OF A FIELD.

We briefly recall the notion of and basic facts about the characteristic of a field K.

For an integer $n \in \mathbb{Z}$ and an element $k \in K$ we define

$$nk = \begin{cases} k + \cdots + k \quad (n \text{ terms}) & \text{for} \quad n > 0 \\ 0 & \text{for} \quad n = 0 \\ (-n)(-k) & \text{for} \quad n < 0\,. \end{cases}$$

For these the following rules hold:

$$(n_1 + n_2)k = n_1 k + n_2 k \text{ for all } n_1, n_2 \in \mathbb{Z},\ k \in K$$

$$n(k_1 + k_2) = nk_1 + nk_2 \text{ for all } n \in \mathbb{Z}, k_1, k_2 \in K$$

$$(n_1 k_1)(n_2 k_2) = (n_1 n_2)(k_1 k_2) \text{ for all } n_1, n_2 \in \mathbb{Z}, k_1, k_2 \in K$$

Now let e denote the identity element in the field K. The mapping ϕ from $\mathbb{Z}$ to K defined by $\phi(n) = ne$ is in view of the above rules a ring homomorphism.

Since the image $\phi\mathbb{Z}$ is a subring of the field K, it must be an integral domain. By the isomorphism theorem for rings (cf. Anders Thorup RNG 3.7 i 2AL) $\mathbb{Z}/Ker(\phi) \simeq \phi\mathbb{Z}$; therefore $Ker(\phi)$ is a prime ideal of $\mathbb{Z}$.

There are two possibilities:

1) $Ker(\phi) = 0$.

2) $Ker(\phi)$ is the principal ideal $\mathbb{Z}p$ generated by a a prime number p.

ad 1). In this case ϕ is injective and:

$$nk = (ne)k = 0 \Leftrightarrow n = 0 \text{ or } k = 0.$$

In this case we say that K has characteristic 0.

Now $\phi\mathbb{Z} \simeq \mathbb{Z}$ and K must contain the fraction field of $\phi\mathbb{Z}$. This fraction field is isomorphic to the field of rational numbers $\mathbb{Q}$.

ad 2). In this case ϕ is not injective and:

$nk = (ne)k = 0 \Leftrightarrow n \in \mathbb{Z}p$ or $k = 0 \Leftrightarrow p \mid n$ or $k = 0$.

In this case we say that K has characteristic p.

Here $\phi\mathbb{Z} \simeq \mathbb{Z}/\mathbb{Z}p$ and K thus contains a subfield called *the prime field*, with exactly p elements.

An important rule for fields of characteristic p is the following:

Theorem 2.63. ("Freshman's dream"). *Let x and y be two arbitrary elements in a field of characteristic p. Then*

$$(x+y)^p = x^p + y^p$$

Proof.

$$(x+y)^p = x^p + \binom{p}{1}x^{p-1}y + \cdots + \binom{p}{p-1}xy^{p-1} + y^p.$$

Since p divides $\binom{p}{i}$ for $1 \leqq i \leqq p-1$ we get $(x+y)^p = x^p + y^p$. □

Remark 2.64.For a field K of characteristic p the mapping σ of K into itself defined by $\sigma(x) = x^p$ is a homomorphism, both w.r.t $+$ and $\cdot$ and thus a ring homomorphism of K into itself.

Since the kernel $Ker(\sigma)$ clearly is 0, the above mapping σ is an injective ring homomorphism of K into itself. If K is a finite field σ will also be surjective and hence an isomorphism (an automorphism) of K onto itself. σ is called *the Frobenius automorphism* of the finite field. If K is not a finite field σ does not have to be surjective.

MULTIPLE ROOTS, FORMAL DIFFERENTIATION AND SEPARABILITY.

We briefly recall the notions "multiple roots" and "multiplicity". If α is an element in the field K and is a root of the polynomial $f(x) \in K[x]$ there exists a uniquely determined number t such that

$$f(x) = (x - \alpha)^t \cdot g(x)$$

where $g(x)$ is a polynomial in $K[x]$ which does not have α as a root. This number t is called *the multiplicity* of α as a root of $f(x)$. If $t = 1$ we call α a *simple root* of $f(x)$; if $t > 1$ we call α a *multiple root* of $f(x)$.

For further investigation concerning the occurence of multiple roots we introduce the concept *formal differentiation.*

Let K be any field. For a polynomial $f(x) \in K[x]$

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

we define the *formal derivative* $f'(x)$ by setting

$$f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$$

The following rules which are analogous to those known from classical calculus can immediately be verified:

$$\begin{aligned} (f+g)' &= f' + g' \,, \quad (kf)' = kf' \quad \text{for all } k \in K \\ (f \cdot g)' &= f \cdot g' + f' \cdot g \,. \end{aligned}$$

Many of the results concerning differentiation in classical calculus also hold for the above formal derivatives. But in some cases, in particular for fields of prime characteristic, one has to be more careful.

Theorem 2.65. *Let K be a field and*

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

a polynomial in $K[x]$.

1) If K has characteristic 0 then $f'(x) = 0 \Leftrightarrow a_i = 0$ for all $i > 0$.

2) If K has characteristic p then $f'(x) = 0 \Leftrightarrow a_i = 0$ for all i, which are not divisible by p.

Proof.

ad 1)

$$f'(x) = \sum_{i>0} i a_i x^{i-1} = 0 \Leftrightarrow \; a_i = 0 \text{ for all } i > 0,$$

where we have used the rules for ia_i being 0 when K has characteristic 0.

ad 2)

$$f'(x) = \sum_{i>0} ia_i x^{i-1} = 0 \Leftrightarrow \ a_i = 0 \text{ for all } i \text{ which are not divisible by } p,$$

where we have used the rules for ia_i being 0 when K has characteristic p.

□

The following theorem holds for fields of arbitrary characteristic.

Theorem 2.66. *Let K be any field. If the polynomial $f(x) \in K[x]$ has a multiple root α in some extension field M of K then α is also a root of $f'(x)$.*

Proof. We can write

$$f(x) = (x-\alpha)^\nu g(x), \text{ where } \nu > 1$$

and get

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

which shows that α is a root of $f'(x)$.

□

Theorem 2.67. *Let K be a field of characteristic 0. An irreducible polynomial $f(x) \in K[x]$ has no multiple roots in any extension field of K, in particular not in the splitting field for $f(x)$ over K.*

Proof. Assume α were a multiple root of $f(x)$ in some extension field M of K. Theorem 2.66 implies that $(x-\alpha)$ is a divisor of $f'(x)$ in $M[x]$. The greatest common divisor $d_M = (f(x), f'(x))_M$ therefore has degree at least 1. By theorem 2.61 the greatest common divisor does not change by extension of the base field. Therefore $d_M = d_K = (f(x), f'(x))_K$. Since the degree of d_K thus is ≥ 1 and $f(x)$ is irreducible in $K[x]$, then d_K (up to a constant factor in $K \setminus \{0\}$) must be $f(x)$. In particular, $f(x)$ must divide $f'(x)$. But this is impossible since K has characteristic 0 and $f'(x)$ therefore (in view of theorem 2.65) a non-zero polynomial, whose degree is smaller than the degree of $f(x)$.

□

Theorem 2.68. *Let K be field of characteristic p. An irreducible polynomium $f(x)$ in $K[x]$ has multiple roots in its splitting field over $K \Leftrightarrow f'(x) = 0$.*

Proof. "$\Rightarrow$"

If $f'(x)$ were a proper polynomial we could in exactly the same way as in the proof of Theorem 2.67 conclude that $f(x)$ has no multiple roots in any extension field of K.

"$\Leftarrow$" If $f'(x) = 0$, Theorem 2.65 implies that $f(x)$ has the form:

$$f(x) = a_0 + a_p x^p + a_2 x^{2p} + \cdots + a_{kp} x^{kp} .$$

It is enough to show that $f(x)$ has multiple roots in some "suitably big" field, in which $f(x)$ splits into linear factors.

We now adjoin to K elements $b_0, b_1, ..., b_k$ such that $b_0^p = a_0$, $b_1^p = a_p, \ldots, b_k^p = a_{kp}$. In $K(b_0, b_1, \ldots, b_k)$ we then have

$$f(x) = b_0^p + b_1^p x^p + \cdots + b_k^p x^{kp} = (b_0 + b_1 x + \cdots + b_k x^k)^p .$$

Let L be the splitting field for $g(x) = b_0 + b_1 x + \cdots + b_k x^k$ over $K(b_0, b_1, \ldots, b_k)$, so that we in L have the splitting $g(x) = b_k(x - \beta_1) \cdots (x - \beta_k)$ and thus $f(x) = a_{kp}(x - \beta_1)^p \cdots (x - \beta_k)^p$ (in $L[x]$).

The above decomposition for $f(x)$ also holds in the splitting field for $f(x)$ over K. We see, that actually *all* roots of $f(x)$ are multiple roots.

□

Definition 2.69. An irreducible polynomial $f(x)$ in $K[x]$ is called *separable* if $f(x)$ has no multiple root in its splitting field over K (and thereby no multiple root in *any* extension field of K). An arbitrary polynomial $f(x)$ in $K[x]$ is called separable if each of its irreducible factors is separable in the above sense.

Remark 2.70. Let $f(x)$ be irreducible. Theorems 2.67 and 2.68 imply that $f(x)$ is separable $\Leftrightarrow f'(x) \neq 0$. In particular every polynomial in $K[x]$ is separable if the characteristic of K is 0.

Definition 2.71 . A field K is called *perfect* if all polynomials in $K[x]$ are separable.

The above theorems in particular imply that every field of characteristic 0 is perfect.

Theorem 2.72. *Let K be a field of prime characteristic p. Then: K is perfect $\Leftrightarrow$ the mapping $\sigma : \alpha \to \alpha^p$ which sends every element in K into its p-th power is surjective.*

Proof. $\Rightarrow$: Let $\beta \in K$ and $f(x) = x^p - \beta$.

Let γ be a root of $f(x)$ in its splitting field over K. Then: $x^p - \beta = (x - \gamma)^p$.

Now $\mathrm{Irr}(\gamma, K)$ is irreducible and by assumption it has no multiple roots in the above splitting field. Since moreover $\mathrm{Irr}(\gamma, K)$ divides $x^p - \beta$ we conclude that $\mathrm{Irr}(\gamma, K) = x - \gamma$; therefore γ must belong to K, in other words $\beta = \gamma^p$.

$\Leftarrow$: It suffices to prove that every polynomial $f(x) \in K[x]$ of positive degree is reducible if $f'(x) = 0$. From theorem 18 it follows that $f'(x) = 0$ implies that $f(x)$ has the form

$$f(x) = a_0 + a_1 x^p + \cdots + a_k x^{kp} .$$

Since the mapping $\sigma : \alpha \to \alpha^p$ is surjective there exist elements $b_0, \ldots, b_k \in K$ such that $a_0 = b_0^p$, $a_1 = b_1^p, \ldots, a_k = b_k^p$, and therfore

$$f(x) = (b_0 + b_1 + \cdots + b_k x^k)^p ,$$

showing that $f(x)$ is reducible. $\square$

Remark 2.73. Since the mapping $\sigma : \alpha \to \alpha^p$ is injective for every field of characteristic p (cf. earlier remark) the above theorem implies that every finite field is perfect.

Example 2.74. A non-perfect field. Let $K = \mathbb{Z}_p(t)$ (i.e. the field of all rational functions in one indeterminate over the field $\mathbb{Z}_p$). The element t is not a p-th power of an element in K since every p-th power must be of the form

$$\frac{a_0 + a_1 t^p + a_2 t^{2p} + \ldots}{b_0 + b_1 t^p + b_2 t^{2p} + \ldots}$$

$(a_i, b_i \in \mathbb{Z}_p)$.

Definition 2.75. Let $L \supseteqq K$ be fields. An element $\alpha \in L$ is called *separable* over K if α is algebraic over K and $\mathrm{Irr}(\alpha, K)$ is a separable polynomial in $K[x]$. $L \supseteq K$ is called a *separable* extension if all elements in L are separable over K.

ABEL-STEINITZ'S THEOREM.

Most of the field extensions that we are going to consider are "simple". The precise definition is the following.

Definition. An algebraic extension L/K is called *simple* if there is an $\alpha \in L$ such that $L = K(\alpha)$. Such an α is called a *primitive element* for L/K.

Theorem 2.76 (Abel, Steinitz). *Let L/K be a finite (and thus in particular an algebraic) extension which is separable. Then L/K is simple, i.e. there exists a primitive element for the extension L/K.*

Proof. If K is finite so is L. As known from group theory $L \setminus \{0\}$ is a cyclic group. If α is a generator for $L \setminus \{0\}$, then in particular $L = K(\alpha)$.

We may therefore assume that K has infinitely many elements. In this case Abel-Steinitz's theorem can be obtained by succesive applications of

If $K \subset M$, $\alpha, \beta \in M$ and α and β are separable over K then there exists $\gamma \in M$ such that $K(\alpha, \beta) = K(\gamma)$.

Proof. Let $f(x) = \mathrm{Irr}(\alpha, K)$, $g(x) = \mathrm{Irr}(\beta, K)$. We now work inside an extension field N of M in which $f(x)$ and $g(x)$ splits into linear factors. We may e.g. for N choose the splitting field for $f(x) \cdot g(x)$ over M. In N we may therefore write

$$\begin{aligned} f(x) &= (x-\alpha_1)\dots(x-\alpha_n)\,, \qquad \text{where we may assume } \alpha = \alpha_1 \\ g(x) &= (x-\beta_1)\dots(x-\beta_m)\,, \qquad \text{where we may assume } \beta = \beta_1\,. \end{aligned}$$

Since β is separable, the elements $\beta_1, \dots, \beta_m$ are distinct. Since K has infinitely many elements there is an element $c \in K$ such that

$$\gamma = \alpha + c\beta \neq \alpha_i + c\beta_j \qquad \begin{matrix} 1 \leqq i \leqq n \\ 2 \leqq j \leqq m \end{matrix} \qquad \left(\begin{matrix} c \text{ chosen such that } c \neq \frac{\alpha-\alpha_i}{\beta_j-\beta} \\ 1 \leq i \leq n\,, \qquad 2 \leq j \leq m \end{matrix} \right)$$

We claim $K(\gamma) = K(\alpha, \beta)$.

It is clear that $K(\gamma) \subseteqq K(\alpha, \beta)$.

To show the inverse inclusion we notice that $f(\gamma - cx)$ has β as a root. Because of the choice of c no β_j, $2 \leq j \leq m$, is a root of $f(\gamma - cx)$. Therefore we may write:

$$f(\gamma - cx) = (x-\beta)^t \cdot h(x)\,, \quad \text{where } t \text{ is an integer} \geq 1$$

and $h(x)$ is a polynomial for which no β_j, $1 \leq j \leq m$, is a root.

In N we thus have

$$(f(\gamma - cx), g(x))_N = (x - \beta)\,.$$

Now $g(x) \in K[x] \subseteq K(\gamma)[x]$ and $f(\gamma - cx) \in K(\gamma)[x]$. By Theorem 2.61 we get $(f(\gamma - cx), g(x))_{K(\gamma)} = (f(\gamma - cx), g(x))_N = x - \beta$. This means that $\beta \in K(\gamma)$.

Since $\alpha = \gamma - c\beta \in K(\gamma)$ we conclude that $K(\alpha, \beta) \subseteq K(\gamma)$; this taken together with the inverse (trivial) inclusion yields $K(\gamma) = K(\alpha, \beta)$. □

Remark 2.77. The assumption about separability in Abel-Steinitz's theorem is important. Let $L = \mathbb{Z}_2(x, y)$ (i.e. the field of rational functions in two indeterminates x og y over the field $\mathbb{Z}_2$) and $K = \mathbb{Z}_2(x^2, y^2)$ (i.e. the subfield of rational functions in x^2 and y^2). Here $[L : K] = 4$ since 1, x, y, xy is a basis for L viewed as a vector space over K. But L/K is not simple. Indeed $\alpha^2 \in K$ for every element $\alpha \in L$, hence $[K(\alpha) : K] \leqq 2$.

– – – – – – – – – – – – – – – – –

FINITE FIELDS.

We first prove a theorem about the number of elements in a finite field.

Theorem 2.78. *The number of elements in a finite field K is the power of a prime number.*

Proof. Since K is finite the characteristic of K must be a prime number p. Therefore the field K must contain the field $\mathbb{Z}_p$ as a subfield. Viewed as a vector space over $\mathbb{Z}_p$ the field K has a finite dimension n where n is a natural number.

Let $\omega_1, \dots, \omega_n$ be a basis for K over $\mathbb{Z}_p$. Every element in K has a unique representation of the form $a_1\omega_1 + \cdots + a_n\omega_n$ where $a_1, \dots, a_n$ run through $\mathbb{Z}_p$. The field K thus has exactly p^n elements.

□

As a kind of converse we now prove:

Theorem 2.79. *For every power p^n of a prime number p there exists one and up to isomorphism just one field with p^n elements.*

Proof. 1) *Existence.* Let M be the splitting field for the polynomial $f(x) = x^{p^n} - x$ over $\mathbb{Z}_p$. Since $f'(x) = -1$ by Theorem 2.66 $f(x)$ has exactly p^n distinct roots in M.

Let α and β be two such roots of $f(x)$. Then $\alpha^{p^n} = \alpha$ and $\beta^{p^n} = \beta$. By repeated application of "Freshman's dream" (Theorem 2.63) we get $(\alpha+\beta)^{p^n} = \alpha+\beta$, hence $\alpha+\beta$ is a root of $f(x)$. Similarly we get that $\alpha-\beta$ is a root of $f(x)$. Furthermore from $\alpha^{p^n} = \alpha$ and $\beta^{p^n} = \beta$ we conclude that $(\alpha\cdot\beta)^{p^n} = \alpha\cdot\beta$. Hence $\alpha\cdot\beta$ is a root of $f(x)$. If $\beta \neq 0$ then $\beta^{p^n} = \beta$ implies $(1/\beta)^{p^n} = 1/\beta$ meaning that $1/\beta$ is a root of $f(x)$.

Consequently the p^n roots of $f(x)$ form a subfield K of M. Thus K is a field with exactly p^n elements. This completes the existence proof. (Actually $K = M$; in fact $f(x)$ splits into linear factors in K and since $f(x)$ has p^n distinct roots and $|K| = p^n$ there is no proper subfield of K in which $f(x)$ splits into linear factors. K must then be the splitting field M of $f(x)$.)

2) *Uniqueness.* Let K be a field with p^n elements. The characteristic of K must be a prime number q . The additive group $(K,+)$ of K must contain the additive group $(\mathbb{Z}_q,+)$ of the prime field $\mathbb{Z}_q$. Thus the order q of $(\mathbb{Z}_q,+)$ divides the order p^n of $(K,+)$. Hence $p = q$ and the prime field of K equals $\mathbb{Z}_p$.

The elements of $K^* = K \setminus \{0\}$ form a multiplicative group of order $p^n - 1$. By Lagrange's theorem $\alpha^{p^n-1} = 1$ for all $\alpha \in K$, $\alpha \neq 0$. This means that all elements in K are roots of the polynomial $x^{p^n} - x$. This polynomial has at most (actually exactly) p^n roots. Therefore K consists exactly of the roots of $x^{p^n} - x$. Consequently K is a splitting field for $x^{p^n} - x$ over $\mathbb{Z}_p$. By the uniqueness (up to isomorphism) of a splitting field (Theorem 2.60) K is uniquely determined up to isomorphism. □

Definition 2.80. For a power p^n of a prime number p the above field with p^n elements is denoted $\mathrm{GF}(p^n)$ or $\mathbb{F}_{p^n}$. (For $n = 1$ there are thus three notations for the field with p elements: $\mathbb{Z}_p$, $\mathrm{GF}(p)$ og $\mathbb{F}_p$!)

Theorem 2.81. *For a given prime p we have the inclusions: $\mathbb{F}_{p^m} \subseteqq \mathbb{F}_{p^n} \Leftrightarrow m|n$. Here ("$\subseteqq$" should be read: "is isomorphic to a subfield of").*

Proof. "$\Rightarrow$": Let d be the dimension of $\mathbb{F}_{p^n}$ viewed as a vector space over $\mathbb{F}_{p^m}$. Then the number of elements in $\mathbb{F}_{p^n}$ is $(p^m)^d = p^{md}$ (cf. the proof of Theorem 2.78). Hence $n = md$, i.e. $m \mid n$.

"$\Leftarrow$": $m|n \Rightarrow p^m - 1 | p^n - 1 \Rightarrow (x^{p^m-1} - 1) \mid (x^{p^n-1} - 1) \Rightarrow (x^{p^m} - x) \mid (x^{p^n} - x) \Rightarrow$ the splitting field (over $\mathbb{Z}_p$) for $(x^{p^n} - x) \supseteqq$ the splitting field (over $\mathbb{Z}_p$) for $(x^{p^m} - x)$. Hence (cf. the proof of theorem 2.79) $\mathbb{F}_{p^n} \supseteqq \mathbb{F}_{p^m}$. $\square$

– – – – – – – – – – – – – – – – –

We give a quite concrete number theoretic application of the theorem above. We derive an explicit formula for the number $\pi(n)$ of monic irreducible polynomials in $\mathbb{Z}_p$ of degree n.

Let $x^{p^n} - x = \Pi\, p(x)$ where $p(x)$ runs through the monic irreducible factors (in $\mathbb{Z}_p[x]$) of $x^{p^n} - x$.

$\mathbb{F}_{p^n}$ is the splitting field for $x^{p^n} - x$ over $\mathbb{Z}_p$. If $\alpha \in \mathbb{F}_{p^n}$ and $p(\alpha) = 0$ then $[\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] =$ the degree d of $p(x)$, hence: $[\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = d$ and thus $|\mathbb{Z}_p(\alpha)| = p^d \Rightarrow d|n$.

Conversely every irreducible monic polynomial $q(x) \in \mathbb{Z}_p[x]$ whose degree d divides n will be a divisor of $x^{p^n} - x$. Indeed: Let $L = \mathbb{Z}_p(\alpha)$ where α is a root of $q(x)$ (or equivalently $q(x) = \mathrm{Irr}(\alpha, \mathbb{Z}_p)$). Then $[L : \mathbb{Z}_p] = d \Rightarrow |L| = p^d$. But then α is a root of $x^{p^d} - x$ and thus $q(x) = \mathrm{Irr}(\alpha, \mathbb{Z}_p) | x^{p^d} - x | x^{p^n} - x$.

Since $x^{p^n} - x$ has no multiple factors, the irreducible factors $p(x)$ in the product $x^{p^n} - x = \Pi\, p(x)$ are just the monic irreducible polynomials whose degrees divide n.

In this way we obtain the formula $p^n = \sum_{d|n} d \cdot \pi(d)$.

To find an explicit formula for $\pi(n)$ we shall need the number theoretical function, the *Möbius-function* $\mu(n)$, defined on $\mathbb{N}$ in the following way:

$$\mu(n) = \begin{cases} 1 & \text{for} \quad n = 1, \\ 0 & \text{if } n \text{ is divisible by a square} > 1, \\ (-1)^r & \text{if } n = p_1 \cdots p_r, \text{ where } p_1, \ldots, p_r \text{ are distinct prime numbers.} \end{cases}$$

Exampl 2.82
$\mu(1) = 1,\ \mu(2) = \mu(3) = -1,\ \mu(4) = 0,\ \mu(5) = -1,\ \mu(6) = 1,\ \mu(7) = -1,\ \mu(8) = \mu(9) = 0,\ \mu(10) = 1.$

Theorem 2.83.

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \textit{for } n = 1 \\ 0 & \textit{for } n > 1. \end{cases}$$

where the summation is extended over all positive divisors of n.

Proof. For $n = 1$ the assertion is clear. For $n > 1$, let $n = p_1^{a_1} \dots p_r^{a_r}$ $p_i \neq p_j$ for $i \neq j$; we only have to consider the square-free divisors of n and find:

$$\sum_{d|n} \mu(d) = \sum_{\nu=0}^{r} (-1)^\nu \binom{r}{\nu} = (1-1)^r = 0\,.$$

□

From Theorem 2.83 we obtain

$$\sum_{d|n} p^{\frac{n}{d}} \mu(d) = \sum_{d|n} \mu(d) \cdot \left\{ \sum_{\delta|\frac{n}{d}} \delta\pi(\delta) \right\} =$$

$$\sum_{\substack{d,\delta \\ d\cdot\delta|n}} \delta\pi(\delta)\mu(d) = \sum_{\delta|n} \delta\pi(\delta) \cdot \left\{ \sum_{d|\frac{n}{\delta}} \mu(d) \right\} =$$

$$n \cdot \pi(n)\,.$$

Consequently we find the following explicit expression for $\pi(n)$:

$$\pi(n) = \frac{1}{n} \cdot \sum_{d|n} p^{\frac{n}{d}} \mu(d)\,.$$

This in particular shows that $\pi(n)$ is positive for every natural number n.

DISCRIMIMANT OF A POLYNOMIAL.

We now introduce a classical invariant which is of great importance for explicit questions concerning the roots of a polynomial.

For this purpose we first consider the following polynomial in n indeterminates $x_1, \cdots, x_n$:

$$\Delta(x_1, x_2, \dots, x_n) = \prod_{n \geq i > j \geq 1} (x_i - x_j) = \begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \cdots & & & & \\ 1 & x_n & x_n^2 & & x_n^{n-1} \end{vmatrix}$$

which plays an important role by the introduction of discriminants. The explicit computation of the above determinant (called *Vandermondes determinant*) can be found in an appendix of these notes.

Clearly for every permutation $\sigma \in S_n$ we get

$$\Delta(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = \begin{cases} \Delta(x_1, x_2, \ldots, x_n) & \text{when } \sigma \text{ is even} \\ -\Delta(x_1, x_2, \ldots, x_n) & \text{when } \sigma \text{ is odd} \end{cases}$$

In particular $d(x_1, x_2, \ldots, x_n) = [\Delta(x_1, x_2, \ldots, x_n)]^2$ is a symmetric polynomial.

Now let K be an arbitrary field and $f(T) = T^n + b_1 T^{n-1} + \cdots + b_n$ a *monic* polynomial in $K[T]$. If $\beta_1, \beta_2, \ldots, \beta_n$ are the roots of $f(T)$ in its splitting field K we define *the discriminant*, $\operatorname{discrim}(f)$, for f as

$$d(\beta_1, \beta_2, \ldots, \beta_n) = \prod_{n \geq i > j \geq 1} (\beta_i - \beta_j)^2 .$$

$d(x_1, x_2, \ldots, x_n)$ is a symmetric polynomial; the main theorem about symmetric polynomials implies that it can be written as a polynomial (with coefficients in K) of the elementary symmetric polynomials of $x_1, x_2, \ldots, x_n$. By substituting β_1 for x_1, β_2 for x_2, etc. we see that $d(\beta_1, \beta_2, \ldots, \beta_n)$ becomes a polynomial (with coefficients in K) of $b_1, b_2, \ldots, b_n$ since the elementary symmetric polynomials of $x_1, x_2, \ldots, x_n$ by substitution of β_1 for x_1, β_2 for x_2, etc. up to factors ± 1 just give b_1, b_2 etc.

In particular it follows that the discriminant $\operatorname{discrim}(f)$ of a polynomial f with coefficients in the field K is an element of K. From the definition it is clear that all roots of f are simple if and only if $\operatorname{discrim}(f) \neq 0$.

The following simple observation is often quite useful

Theorem 2.84. *Let K be a field and M the splitting field over K for a monic polynomial $f(x) \in K[x]$ of degree n. Then $\sqrt{\operatorname{discrim}(f)}$ is an element of M.*

Proof. Let $\beta_1, \ldots, \beta_n$ be the roots of $f(x)$. Clearly $\Delta(\beta_1, \ldots, \beta_n)$ is an element of M. Since $\operatorname{discrim}(f) = [\Delta(\beta_1, \ldots, \beta_n)]^2$, the square root $\sqrt{\operatorname{discrim}(f)}$ lies in M. $\square$

Let us compute the discriminants of quadratic and cubic polynomials.

It is immediate to check that $\operatorname{discrim}(T^2 + a_1 T + a_2) = a_1^2 - 4a_2$.

Among the cubic polynomials we just consider those of the form $T^3 + pT + q$. If β_1, β_2 and β_3 are the roots we find

$$\begin{aligned} &\beta_1 + \beta_2 + \beta_3 = 0 \\ &\beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3 = p \\ &\beta_1\beta_2\beta_3 = -q \ . \end{aligned}$$

For the power sums

$$P_t = \beta_1^t + \beta_2^t + \beta_3^t$$

we find

$$\begin{aligned} P_1 &= 0 \\ P_2 &= -2p \end{aligned}$$

and since

$$\sum_{i=1}^{3} \left(\beta_i^3 + p\beta_i + q\right) = 0$$

and

$$\sum_{i=1}^{3} (\beta_i^4 + p\beta_i^2 + q\beta_i) = 0$$

we conclude $P_3 = -3q$ og $P_4 = 2p^2$.

Furthermore

$$\begin{aligned}
&\operatorname{discrim}(T^3 + pT + q) = [(\beta_2 - \beta_1)(\beta_3 - \beta_2)(\beta_3 - \beta_1)]^2 = \\
&\begin{vmatrix} 1 & \beta_1 & \beta_1^2 \\ 1 & \beta_2 & \beta_2^2 \\ 1 & \beta_3 & \beta_3^2 \end{vmatrix}^2 = \begin{vmatrix} 3 & P_1 & P_2 \\ P_1 & P_2 & P_3 \\ P_2 & P_3 & P_4 \end{vmatrix} = \begin{vmatrix} 3 & 0 & -2p \\ 0 & -2p & -3q \\ -2p & -3q & 2p^2 \end{vmatrix} \\
&= -27q^2 - 4p^3 \ .
\end{aligned}$$

For a cubic polynomial with real coefficients the number of real roots is determined by the discriminant. Indeed:

Theorem 2.85. *Let $f(x)$ be a monic cubic polynomial with real coefficients. Then:*

$\operatorname{discrim}(f) > 0 \Leftrightarrow f$ *has three distinct real roots;*
$\operatorname{discrim}(f) = 0 \Leftrightarrow f$ *has a multiple root;*
$\operatorname{discrim}(f) < 0 \Leftrightarrow f$ *has exactly one real root.*

Proof. Exercise.

More generally the following holds:

Theorem 2.86. *Let $f(x)$ be a monic polynomial in $\mathbb{R}[x]$ of degree n.*

i) $\operatorname{discrim}(f) = 0$ *exactly when $f(x)$ has a multiple root.*

Assume all roots of $f(x)$ are simple. Let r_1 be the number of real roots and r_2 the number of pairs of complex conjugate roots (i.e. $r_1 + 2r_2 = n$).

ii) $\operatorname{discrim}(f)$ *is positive exactly when r_2 is even.*

iii) $\operatorname{discrim}(f)$ *is negative exactly when r_2 is odd.*

Proof. The assertion i) is clear.

Assume now $f(x)$ has n simple roots $\beta_1, \dots, \beta_n$. Then the discriminant $\operatorname{discrim}(f) = [\Delta(\beta_1, \dots, \beta_n)]^2$.

Now we have

$$\Delta(\beta_1, \dots, \beta_n) = \begin{vmatrix} 1 & \beta_1 & \beta_1^2 & \cdots & \beta_1^{n-1} \\ 1 & \beta_2 & \beta_2^2 & \cdots & \beta_2^{n-1} \\ \cdots & & & & \\ 1 & \beta_n & \beta_n^2 & & \beta_n^{n-1} \end{vmatrix}$$

Application of complex conjugation on $\Delta(\beta_1, \dots, \beta_n)$ gives rise to transpositions of r_2 rows in the above determinant.

If r_2 is even $\Delta(\beta_1, \dots, \beta_n)$ will be invariant under complex conjugation and therefore a real number. The square $\operatorname{discrim}(f) = [\Delta(\beta_1, \dots, \beta_n)]^2$ is then a positive number.

If r_2 is odd $\Delta(\beta_1, \dots, \beta_n)$ will change sign by complex conjugation and therefore of the form $\sqrt{-1}\cdot$ (a real number). The square $\operatorname{discrim}(f) = [\Delta(\beta_1, \dots, \beta_n)]^2$ must then be a negative number. □

For explicit computation of discriminants the following is often quite useful

Theorem 2.87. *Let $f(T) = T^n + b_1 T^{n-1} + \cdots + b_n$ be a polynomial with the roots $\beta_1, \dots, \beta_n$. Then we have* $\operatorname{discrim}(f) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} f'(\beta_i)$.

Proof. From the rules for formal differentiation we get for $f(T) = \prod_{i=1}^{n} (T - \beta_i)$

$$\begin{aligned} f'(T) &= (T-\beta_2)\cdots(T-\beta_n) + (T-\beta_1)(T-\beta_3)\cdots(T-\beta_n) \\ &+ \cdots + (T-\beta_1)(T-\beta_2)\cdots(T-\beta_{n-1}) \ . \end{aligned}$$

Hence for the product $\prod_{i=1}^{n} f'(\beta_i)$ we find

$$\begin{gathered} (\beta_1-\beta_2)\cdot(\beta_1-\beta_3)\cdots(\beta_1-\beta_n) \\ (\beta_2-\beta_1)\cdot(\beta_2-\beta_3)\cdots(\beta_2-\beta_n) \\ \cdots \\ (\beta_n-\beta_1)\cdot(\beta_n-\beta_2)\cdots(\beta_n-\beta_{n-1}) \end{gathered}$$

$$= (-1)^{\frac{n(n-1)}{2}} d(\beta_1, \dots, \beta_n) = (-1)^{\frac{n(n-1)}{2}} \operatorname{discrim}(f) \ .$$

□

Theorem 2.88. *The discriminant of the polynomial $f(T) = T^n - 1$ is $n^n(-1)^{\frac{(n-1)(n-2)}{2}}$.*

Proof. Clearly $f'(T) = nT^{n-1}$. For the roots $\beta_1, \dots, \beta_n$ the product $\beta_1 \cdots \beta_n$ is $(-1)^{n-1}$, so theorem 31 yields

$$\begin{aligned} \operatorname{discrim}(f) &= (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} f'(\beta_i) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} (n\beta_i^{n-1}) \\ &= (-1)^{\frac{n(n-1)}{2}} n^n \left(\prod_{i=1}^{n} \beta_i \right)^{n-1} = n^n (-1)^{\frac{n(n-1)}{2}} (-1)^{(n-1)^2} \\ &= n^n (-1)^{\frac{(n-1)(n-2)}{2}} . \end{aligned}$$

$\square$

Exercise 2.89. Show that the discriminant of the polynomial $T^4 + aT^2 + b$ is $16(a^2 - 4b)^2 b$.