03/02/2016 Test 1

03/03/2016

5.1.1 Irreducibility Criteria

Proposition 5.1.23 *Let D be a UDF, and Q its field of fractions. Let S a commutative ring, and $\varphi : D \to S$ a ring homomorphism. Let $\overline{\varphi} : D[x] \to S[x]$ be the induced homomorphism on polynomialas, i.e $\overline{\varphi}(r) = \varphi(r)$ for $r \in R$, and $\overline{\varphi}(x) = x$. let $f \in D[x]$ be non-constant and let $\overline{f} = \overline{\varphi}(f)$. If the leading coefficient of f is not in the kernel of φ, and $\overline{f}$ is irreducible in $S[x]$, then f is irreducible in $Q[x]$.*

Proof. ■

Example 5.1.8. Let $f = x^4 + 2x^2 + 2x - x + 1 \in \mathbb{Z}[x]$. Reducing the coefficients (mod2), we get $\overline{f} = x^4 + x + 1 \in \mathbb{Z}_2[x]$ which is irreducible, as we have seen. Therefore f is irreducible in $\mathbb{Q}[x]$. Since f is primitive, it is also irreducible in $\mathbb{Z}[x]$.

Proposition 5.1.24 *[Eisenstein Criterion] Let D be an integral domain, P a prime ideal of D and $f \in D[x]$. Write*

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

If $a_0, \ldots, a_{n-1} \in P$, $a_n \notin P$ and $a_0 \notin P^2$, then f is irreducible in $D[x]$.

Proof. ■

03/04/2016 Problem Set 5 board presentations

Part III

Fields

Vector space
subspace
linear combination
linearly dependent

Chapter 6

Fields

6.1 Vector Spaces

See Textbook §6.1

03/07/2016

Definition 6.1.1. *Vector space*, *subspace*.

Lemma 6.1.1 *Let F be a field, V a vector space over F, $x \in V$ and $\lambda \in F$. If $\lambda x = 0$ then either $\lambda = 0$ or $x = 0$.*

Definition 6.1.2. Let F be a field, V be a vector space over F, and X a subset of V. A *linear combination* of X over F is an expression of the form

$$\lambda_1 x_1 + \cdots + \lambda_n x_n \tag{6.1}$$

where $x_1, \ldots, x_n \in X$ and $\lambda_1, \ldots, \lambda_n \in F$.

Definition 6.1.3. Let F be a field, V be a vector space over F, and X a subset of V. We say that X is *linearly dependent* over F, (l.d. for short) if there are $n \geq 1$, $x_1, \ldots, x_n \in X$, and $\lambda_1, \ldots, \lambda_n \in F^*$ such that

$$\lambda_1 x_1 + \cdots + \lambda_n x_n = 0, \tag{6.2}$$

i.e. a linear combination with non-zero coefficients, equal to 0. We call the Equation 6.2 a witness to the dependency of X, and say that the subset

$\{x_1, \ldots, x_n\}$ witnesses that dependency.
We say that X is *linearly independent* over F (l.i. for short), if it is not linearly dependent over F.

linearly independent
spans
spanning set

To say that X is linearly independent means that there is no witness to dependence, in other words, that whenever we have

$$\lambda_1 x_1 + \cdots + \lambda_n x_n = 0$$

where $x_1, \ldots, x_n \in X$, and $\lambda_1, \ldots, \lambda_n \in F$, then all of the λ_i must be outside F^*, i.e. all of the λ_i must be equal to 0. Otherwise, we would drop those $\lambda_i = 0$, keeping those $\lambda_i \neq 0$, to get a witness to dependence. We can write this as an implication For $x_1, \ldots, x_n \in X$, and $\lambda_1, \ldots, \lambda_n \in F$,

$$(\lambda_1 x_1 + \cdots + \lambda_n x_n = 0) \Rightarrow (\lambda_1 = \lambda_2 = \cdots = \lambda_n = 0.$$

Definition 6.1.4. Let V be a v.s. over F and $X \subseteq V$. We define $\mathrm{Span}(X)$ as the set of all linear combinations of X over F. We say that X *spans* V if $\mathrm{Span}(X) = V$. We also say that X is a *spanning set* of V.

Lemma 6.1.2 *Let V be a v.s. over F and $X \subseteq V$. Then* $\mathrm{Span}(X)$ *is a subspace of V.*

Proposition 6.1.3 *Let V be a v.s. over F, $X \subseteq Y \subseteq V$.*

1. *If Y is l.i. then X is l.i.*
2. $\mathrm{Span}(X) \leq span(Y)$.
3. *If X spans V then Y spans V.*

Theorem 6.1.4 *Let V be a v.s. over F, $I \subseteq T \subseteq V$, such that I is l.i. and T spans V. There is $B \subset V$ such that $I \subseteq B \subseteq T$ and B is both l.i. and spanning set.*

Definition 6.1.5. Let V be a v.s. over F, and $B \subseteq V$. We say that B is a basis for V over F if B is both linearly independent over F, and a spanning set for V over F.

The following theorem states that any two bases for a v.s. have the same cardinality.

Theorem 6.1.5 *Let V be a v.s. over F. If B_1 and B_2 are bases for V over F, then $|B_1| = |B_2|$.*

finite dimensional
linear transformation

Definition 6.1.6. Let V be a v.s. over F. We denote by $\dim_F(V)$ the cardinality of any basis for V. We say that V is *finite dimensional* over F if $\dim_F(V)$ is finite, i.e. if V has a finite basis.

Examples 6.1.1.

1. $F[x]$ is a countably infinite dimensional v.s. over F, with basis $\{1, x, x^2, \dots\}$, the set of all powers of x.
2. $F_n[x] = \{f \in F[x] | \deg(f) < n\}$ is an n-dimensional v.s. over F, with basis $\{1, x, x^2, \dots, x^{n-1}\}$.
3. $\dim_F(F) = 1$, with basis $\{1\}$.
4. $\dim_F(\{0\}) = 0$, with empty basis.

03/09/2016

Example 6.1.2. $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$.

Definition 6.1.7. Homomorphisms of vector spaces are called *linear transformation*.

Theorem 6.1.6 *Two vector spaces over a field F are isomorphic iff they have the same dimension.*

Exercise 6.1.1. Let W be a subspace of a vector space V.

1. Prove that $\dim(W) \leq \dim(V)$.
2. If V is finite dimensional and $\dim(W) = \dim(V)$ then $W = V$.
3. Show, with a counterexample, that part (2) does not hold without the finite dimensional hypothesis.

There are isomorphism theorems similar to those of groups and rings. In particular, the first isomorphism theorem for vector spaces can be phrased as follows:

03/14/07

Theorem 6.1.7 *Let V, W be vector spaces over F, and $\varphi : V \to W$ a linear transformation. Then*

$$V/\ker(\varphi) \approx \mathrm{Im}(\varphi)$$

and $\dim_F(V) = \dim_F(\ker(\varphi)) + \dim_F(\mathrm{Im}(\varphi))$.

Proposition 6.1.8 *Let V be a finite-dimensional vector space over F. Let $n = \dim_F(V)$ and let $B \subseteq V$. Any two of the following three conditions implies that B is a basis, and hence imply the third condition.*

1. *B is linearly independent.*
2. *B is a spanning set for V.*
3. *B has n elements.*

Proposition 6.1.9 *If V is f.d. with $dim_F(V) = n$ then V is isomorphic to F^n.*

Corollary 6.1.10 *If F is countable and V is f.d. over F, then V is countable.*

It follows from this corollary that $\mathbb{R}$ is not finite dimensional as a vector space over $\mathbb{Q}$.

03/10/2016

Corollary 6.1.11 *If F is finite and V is f.d. over F, then V is finite. More precisely, if $|F| = q$ and $\dim_F(V) = n$ then $|V| = q^n$.*

Corollary 6.1.12 *If F is finite then $|F|$ is a power of a prime.*

Proof. Since F is finite, its characteristic cannot be zero. By Theorem **??** its prime subfield is isomorphic to $\mathbb{Z}_p$ where $p = \mathrm{char}(F)$. The result now follows from the Corollary 6.1.11. ■

Unlike what happens with groups and rings, where we have groups and rings of all finite cardinalities, the only finite cardinalities where we can have fields are the prime powers. There is no field of cardinality 6. More on finite fields in Section 6.4.

Exercise 6.1.2. Let V be a v.s. over F, $I, D \subseteq V$.

1. If I is l.i., and $v \in V$ is such that $v \notin \text{Span}(I)$, Then $I \cup \{v\}$ is l.i.
2. $D \subseteq V$ is l.d. iff $(\exists v \in S)(v \in \text{Span}(S - \{v\}))$.

field extension
extension
degree
index
finite extension
extension!finite
infinite extension
extension!infinit

6.2 Field Extensions

Definition 6.2.1. Let F be a subfield of E. We say that E is a *field extension* of F, or just an *extension* of F. The dimension $\dim_F(E)$ of E as a vector space over F is called the *degree* or *index* of the extension, and it is denoted by $[E : F]$. We often refer to the pair of fields E and F as the "extension E/F". In this context, the bar / does **not** denote a quotient. Sometimes we picture this situation as follows:

$$\begin{array}{c} E \\ | \\ F \end{array} \qquad \text{or as} \qquad \begin{array}{c} E \\ | \, d \\ F \end{array}$$

where $d = [E : F]$.

We say that E is a *finite extension* of F, if it is an extension of finite degree. Otherwise we say that it is an *infinite extension*.

Examples 6.2.1. 1. E/F is an extension of degree 1 iff $E = F$.

2. As we have seen in Example **??**

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Q}\}$$

is a field. It clearly contains $\mathbb{Q}$ as a subfield, so $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is a field extension. It is easy to see that $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$, so we have an extension of degree 2.

3. $\mathbb{R}/\mathbb{Q}$ is an infinite field extension.

4. $\mathbb{C}/\mathbb{R}$ is an extension of degree 2, with basis $\{1, i\}$.

6.3 Algebraic Extensions

algebraic
transcendental
algebraic
transcendental
algebraic numbers
transcendental numbers

Proposition 6.3.1 *Let E/F be a finite extension with $n = [E : F]$. For each $\alpha \in E$, there is $f \in F[x]$ such that $f(\alpha) = 0$. Moreover, f can be chosen such that $\deg(f) \leq n$ and f is monic.*

Definition 6.3.1.

- Given $\alpha \in E/F$, we say that α is *algebraic* over F, if there is $f \in F[x]$ such that $f(\alpha) = 0$. When f is of smallest possible degree k, we say that α has degree k over F, and write $\deg_F(\alpha) = k$.
- If α is not algebraic over F, we say that it is *transcendental* over F.
- We say that the extension E/F is *algebraic* is every $\alpha \in E$ is algebraic over F, otherwise we say that the extension is *transcendental*.

Examples 6.3.1.

1. $\sqrt{2}$ is a root of $x^2 - 2 \in \mathbb{Q}[x]$, so $\sqrt{2}$ is algebraic over $\mathbb{Q}$. Complex numbers that are algebraic over $\mathbb{Q}$ are called *algebraic numbers*
2. The imaginary number i is a root of $x^2 + 1 \in \mathbb{R}[x]$, so it is algebraic over $\mathbb{R}$. It is also algebraic over $\mathbb{Q}$, so it is an algebraic number.
3. The numbers π and e are transcendental over $\mathbb{Q}$. We say they are *transcendental numbers*. We omit the proof here.

Remark 6.3.1. Algebraic v/s transcendenta, can be seen in terms of the evaluation homomorphism $\mathrm{ev}_\alpha : F[x] \to E$. For $\alpha \in E$, α is transcendental over F iff ev_α is injective.

We can rephrase part of Proposition 6.3.1 as follows.

Theorem 6.3.2 *Every finite extension is algebraic.*

03/11/2016

Proposition 6.3.3 *Let E/F be an extension and $\alpha \in E$. The kernel of the evaluation homomorphism ev_α,*

$$\{f(x) \in F[x] | f(\alpha) = 0\}$$

is an ideal of $F[x]$. Since $F[x]$ is a PID, this kernel is a principal ideal. When this kernel is non-zero, for $0 \neq f \in F[x]$ TFAE:

i) $\ker(\mathrm{ev}_\alpha) = \langle f \rangle$,

minimal polynomial

ii) $f(\alpha) = 0$ *and* f *is irreducible over* F*, (i.e. irreducible in* $F[x]$*)*

iii) f *is a polynomial of minimal degree in* $F[x]$ *having* α *as a root,*

and there is a unique monic polynomial satisfying these equivalent properties.

Proof. (*i* $\iff$ *iii*) Follows from the proof of Proposition 5.1.2.
(*iii* $\Rightarrow$ *ii*) Since $F[x]$ is a UFD, f has an irreducible factor which has α as a root. By minimality of $\deg(f)$, f and this irreducicible factor must have the same degree, hence they are associates. That makes f irreducible by Lemma **??**.
(*ii* $\Rightarrow$ *i*) $p(\alpha) = 0$ yields $p(x) \in \ker(\mathrm{ev}_\alpha)$, hence $\langle p(x) \rangle \leq \ker(\mathrm{ev}_\alpha)$. ■

Definition 6.3.2. For $\alpha \in E/F$, algebraic over F, the unique monic polynomial satisfying the properties in Proposition 6.3.3 is called the *minimal polynomial* of α over F, and it is denoted $\min_F(\alpha)$.

Examples 6.3.2.

1. Since $x^2 - 2$ has no rational roots, it is irreducible over $\mathbb{Q}$, and $\min_{\mathbb{Q}}(\sqrt{2}) = x^2 - 2$. Moreover, $\deg_{\mathbb{Q}}(\sqrt{2}) = 2$.

2. Since $x^2 + 1$ has no real roots, it is irreducible over $\mathbb{R}$, and $\min_{\mathbb{R}}(i) = x^2 + 1$. Moreover, $\deg_{\mathbb{R}}(i) = 2$.

3. Find the minimal polynomial and the degree of $\alpha = \sqrt{1 + \sqrt{3}}$ over Q. Since $\alpha^2 = 1 + \sqrt{3}$, we have $(\alpha^2 - 1)^2 = 3$, i.e. $\alpha^4 - 2\alpha^2 - 2 = 0$, so α is a root of $x^4 - 2x^2 - 2 \in \mathbb{Q}[x]$. This polynomial is irreducible by Eisenstein's criterion, so $\min_{\mathbb{Q}}(\alpha) = x^4 - 2x^2 - 2$, and $\deg_{\mathbb{Q}}(\alpha) = 4$.

4. Find the minimal polynomial and the degree of $\alpha = \sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$. We have already seen in Example , that $\alpha = \sqrt{2} + \sqrt{3}$ is a root of $f = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$. Let's show that this polynomial is irreducible, hence it is the minimal polynomial, and $\deg_{\mathbb{Q}}(\alpha) = 4$. Note first, that by Proposition **??** f has no rational roots, hence no linear factors. That still leaves the possibility of f factoring as a product $f = gh$ of two quadratic factors. That means that the four roots of f split into two for g and the other two for h. The four roots of f are $\pm\sqrt{2} \pm \sqrt{3}$, and the two that go with g must be such that their sum and their product

are rational. One can easily check that there is no such pair. So f is irreducible over $\mathbb{Q}$.

03/14/2016

In Proposition 6.3.1 we begin with an element α of a finite extension of F, and find a polynomial $f \in F[x]$ that has α as a root. We now want to go in the opposite direction. Given a polynomial $f \in F[x]$ we want to find a root α in some finite extension of F. We need some preparation work before we get there.

Proposition 6.3.4 *Let D be a PID and $p \in D$. p is irreducible iff $\langle p \rangle$ is a maximal (proper) ideal of D.*

Proof. ($\Rightarrow$)

($\Leftarrow$) ■

Note that the hypothesis of D being a PID is used only in one direction. For an arbitrary ID we have:

$$\begin{array}{c} p \text{ is prime} \Leftrightarrow \langle p \rangle \text{ is a prime ideal} \\ \Downarrow \\ p \text{ is irreducible} \Leftarrow \langle p \rangle \text{ is a maximal ideal} \end{array}$$

When D is a PID, the one-way implications become equivalences and we have.

$$\begin{array}{ccc} p \text{ is prime} & \Leftrightarrow & \langle p \rangle \text{ is prime ideal} \\ \Updownarrow & & \Updownarrow \\ p \text{ is a irreducible} & \Leftrightarrow & \langle p \rangle \text{ is a maximal ideal} \end{array}$$

Corollary 6.3.5 *Let F be a field, and $f \in F[x]$. If f is irreducible over F then $F[x]/\langle f \rangle$ is a field.*

Examples 6.3.3. 1. $x^2 - 2 \in \mathbb{Q}[x]$ is irreducible, so $\mathbb{Q}[x]/\langle x^2 - 2\rangle$ is a field. But we can do better. Note that $x^2 - 2 = \min_{\mathbb{Q}}(\sqrt{2})$, so $\langle x^2 - 2\rangle$ equals the kernel of the evaluation homomorphism $\mathrm{ev}_{\sqrt{2}} : \mathbb{Q}[x] \to \mathbb{R}$. By the first isomorphism theorem $\mathbb{Q}[x]/\langle x^2 - 2\rangle$ is isomorphic to the image of $\mathrm{ev}_{\sqrt{2}}$, which is $\mathbb{Q}[\sqrt{2}]$. By Lemma **??**, we have $\mathbb{Q}[\sqrt{2}]$ is a subring of $\mathbb{Q}(\sqrt{2})$. But since we just showed that $\mathbb{Q}[\sqrt{2}]$ is a field, then we get that $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$.

2. $x^2 + 1$ is irreducible over $\mathbb{R}$. A similar argument shows that

$$\mathbb{R}[i] = \mathbb{R}(i) = \mathbb{C} \approx \mathbb{R}[x]/\langle x2 + 1\rangle.$$

3. The polynomial $x^2+x+1 \in \mathbb{Z}_2[x]$ is irreducible. Therefore, $\mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$ is a field. We will say more on this example.

The following lemma follows immediately from the fact that a field F is a simple ring, i.e. has no ideals other that F and $\{0\}$.

Lemma 6.3.6 *Let F be a field, R a non-trivial ring, and $\varphi : F \to R$ a ring homomorphism. Then φ is injective, and R contains a subfield $\varphi(F)$ isomorphic to F.*

Example 6.3.4. This is a continuation of Example 6.3.3.3. Let $f = x^2+x+1$, $I = \langle f\rangle$, and $E = Z_2[x]/\langle f\rangle$. The composition of the inclusion and quotient maps

$$\mathbb{Z}_2 \overset{\iota}{\hookrightarrow} Z_2[x] \overset{q}{\twoheadrightarrow} Z_2[x]/\langle f\rangle$$

is a injective homomorphism, so we want to think of $E = Z_2[x]/\langle f\rangle$ as a field extension of Z_2. If we let $\alpha = x + I$, then $f(\alpha) = (x^2 + x + 1) + I = I$, so $\alpha \in E$ is a root of f. Morevoer, $f(\alpha + 1) = (\alpha + 1)^2 + (\alpha + 1) + 1 = \alpha^2 + 1 + \alpha + 1 + 1 = 0$, so $(\alpha + 1) \in E$ is the other root of f. By the division algorithm, for any $g \in F[x]$ there are $q, r \in F[x]$ such that $f = gq + r$ and $r = 0$ or $\deg(r) < \deg(f) = 2$. This means that $f + I = r + I$, so the elements of E are represented by polynomials of degree less than 2. This yields

$$E = \{0 + I, 1 + I, x + I, x + 1 + I\} = \{0, 1, \alpha, \alpha + 1\},$$

so E is a field with 4 elements, and $E/\mathbb{Z}_2$ is an extension of degree 2.

Lemma 6.3.7 *Let $f \in F[x]$ be irreducible of degree n. There is an extension E of F of degree n such that f has a root $\alpha \in E$.*

extension homomorphism

03/16/2016

Proof. ■

Example 6.3.5. Consider the polynomial $f = x^2 + x + 1 \in \mathbb{Z}_2[x]$. It is irreducible since it has degree 2 and no roots in $\mathbb{Z}_2$. If we denote set $\alpha = x + \langle f \rangle$, the root of f in $E = \mathbb{Z}_2[x]/\langle f \rangle$, then $\alpha^2 + \alpha + 1 = 0$, i.e. $\alpha^2 = \alpha + 1$ $(*)$. The degree $[E : \mathbb{Z}_2] = 2$ and $\{1, \alpha\}$ is a basis for E over $\mathbb{Z}_2$. So, $E = \{0, 1, \alpha, \alpha + 1\}$ has four elements. The multiplication table can be computed using $(*)$.

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha=1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

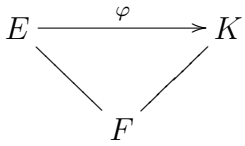
Remark 6.3.2. When f is a linear polynomial, i.e. of degree 1, then $E = F$. When $n := \deg(f) > 1$, E is a proper extension of F, and f is not irreducible over E, since it has a root, hence a linear factor. Factoring out this linear factor, the rest can be factored into irreducible factors, and we could apply the lemma again to one of this irreducible factors, to get an extension of E that has a second root of f. Repeating the process we can get an extension of F where f has n roots, counting multiplicities. We will do this more carefully in Corollary 6.3.15 to get an upper bound on the degree of the extension.

Next, we consider homomorphisms of field extensions. Recall from Lemma **??** that a field F has no ideals other than F and 0, and the only unitary homomorphisms from F to any non-trivial ring have to be one-to-one. When we consider two field extensions with the same field F at the bottom, we want to consider homomorphisms at the top that fix the bottom. More precisely,

Definition 6.3.3. Given two field extensions E/F and K/F, an *extension homomorphism* from E/F to K/F is a field homomorphism $\varphi : E \to K$ such that $\varphi|_F = \mathrm{id}_F$, i.e. $\varphi(a) = a$ for all $a \in F$. By Lemma **??.??** any field

extension homomorphism is injective. But just like in Definition **??** we have special names for extension homomorphisms that are bijective, i.e. *extension isomorphism*; from an extension to itself, i.e. *extension endomorphism*; and *extension automorphism* a bijective homomorphism form an extension to itself.

extension isomorphism
extension endomorphism
extension automorphism



Note that an extension morphism $\varphi : E/F \to K/F$ is not only a field homomorphism from E to K, but it is also a linear transformation of F-vector spaces.

Theorem 6.3.8 *Let $f \in F[x]$ be irreducible of degree n. There is an extension E of F of degree n such that f has a root in E. Such extension is unique, up to isomorphism.*

Proof. The existence part was already established in Lemmma **??**. Suppose K is an extension of F of degree n, and with a root β of $p(x)$. The evaluation homomorphism

$$\begin{array}{rccc} \mathrm{ev}_\beta : & F[x] & \to & K \\ & g & \mapsto & g(\beta) \end{array}$$

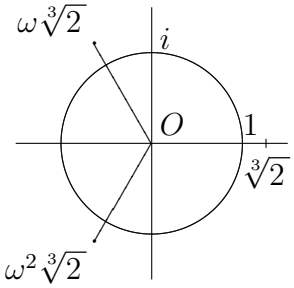
is a non-zero homomorphism, whose kernel contains f and is generated by a single polynomial q. Since q divides f, by irreducibility of f, they must be associates, so $\ker(\mathrm{ev}_\beta) = \langle f \rangle$. Clearly, $\mathrm{Im}(\mathrm{ev}_\beta) = F(\beta)$, so $\widehat{\mathrm{ev}_\beta} : F[x]/\langle f \rangle \to F(\beta)$ is an isomorphism of fields. Note, however, that $\widehat{\mathrm{ev}_\beta}$ fixes the elements of F, so it is an extension isomorphism, hence a vector space isomorphism. By dimension consideration, using Exercise 6.1.1.2, we must have $F(\beta) = K$. ■

Scholium 6.3.9 *If $f \in F[x]$ is irreducible of degree n, and β is a root of f in an extension K of F, then $F(\beta)/F$ is an extension of degree n with basis $\{1, \beta, \beta^2, \ldots, \beta^{n-1}\}$. Moreover, $F[\beta] = F(\beta)$ is isomorphic to $F[x]/\langle p(x) \rangle$ with isomorphism given by*

$$\begin{array}{rccc} \hat{\varphi} : & F[x]/\langle p(x) \rangle & \to & F(\beta) \\ & g + \langle f \rangle & \mapsto & g(\beta) \end{array}$$

splits over E
splitting field

Note that in this scholium the degree $[K : F]$ is at least n, so the extension $E = F[x]/\langle p(x)\rangle$ in Theorem 6.3.8 is of minimum degree possible.



Remark 6.3.3. The uniqueness up to isomorphism of the extension in Theorem 6.3.8, should not be confused with equality. The polynomial $x^3 - 2$ is irreducible over $\mathbb{Q}$ (Eisenstein criterion). It has a single real root $\sqrt[3]{2}$, and two non real roots, $\sqrt[3]{2}\omega$, and $\sqrt[3]{2}\omega^2$, where $\omega = \text{cis}(2\pi/3)$. Even though $\mathbb{Q}(\sqrt[3]{2}) \approx \mathbb{Q}(\sqrt[3]{2}\omega)$ as fields, they are not equal, since the first one is contained in $\mathbb{R}$, but the second one is not.

Exercise 6.3.1. Show that the polynomial $f = x^5 + 2x + 4$ is irreducible over $\mathbb{Q}$, and it has exactly one real root. Show that f has roots α_1 and α_2 such that $\mathbb{Q}(\alpha_1) \approx \mathbb{Q}(\alpha_2)$, but $\mathbb{Q}(\alpha_1) \neq \mathbb{Q}(\alpha_2)$.

Corollary 6.3.10 [Kronecker, 1887] *Let $f(x) \in F[x]$ be a polynomial of degree $n > 0$. There is a finite extension E of F of degree $\leq n$ such that $f(x)$ has a root in E.*

Proof. Apply the theorem to any irreducible factor of $f(x)$. ■

03/17/2016

Definition 6.3.4. When $f \in F[x]$ factors into linear factors over an extension E of F, we say that f *splits over* E. If moreover, E is minimal with this property, i.e. no proper subfield of E has the property, then we say that E is a *splitting field* for f over F.

Corollary 6.3.11 *Let $f \in F[x]$ be a polynomial of degree $n > 0$. There is an extension K of F where f has n roots, counting multiplicities. i.e. f factors into linear factors in $K[x]$.*

Exercise 6.3.2. Prove Corollary 6.3.11. Hint: use induction on n.

Corollary 6.3.11 tells us that for any polynomial $f \in F[x]$ there is an extension K of F where it splits. Note, however, that it says nothing about the degree of such extension, or about the existence of a splitting field. We now discuss these two issues. First, to say something about the degree, we will need Theorem 6.3.13 below. We will consider the existence and uniqueness of splitting field after that.

Proposition 6.3.12 *Let E/F be an extension with basis $B = \{b_i | i \in I\}$ and K/E an extension with basis $C = \{c_j | j \in J\}$. Then the extension K/F has basis $D = \{b_i c_j | i \in I, j \in J\}$.*

multiplicative property of extension degrees

Proof of Proposition 6.3.12. To see that D is a spanning set for K over F, note that each element of $\alpha \in K$ can be written as a (finite) linear combination

$$\alpha = \sum_{j \in J} \beta_j c_j$$

of elements of C with coefficients $\beta_j \in E$. But each of these coefficients β_j can be written as a (finite) linear combination

$$\beta_j = \sum_{i \in I} \gamma_{i,j} b_i$$

of elements in B with coefficents $\gamma_{i,j} \in F$. Combining these equations we get

$$\alpha = \sum_{j \in J} \sum_{i \in I} \gamma_{i,j} b_i c_j$$

To see that D is linearly independent, suppose there is a (finite) linear combination of elements of D equal to 0.

$$\sum_{j \in J} \sum_{i \in I} \gamma_{i,j} b_i c_j = 0$$

then grouping terms

$$\sum_{j \in J} \left(\sum_{i \in I} \gamma_{i,j} b_i \right) c_j = 0$$

and using the linear independence of C we get that for each $j \in J$,

$$\sum_{i \in I} \gamma_{i,j} b_i = 0$$

Now the linear independence of B implies that each $\gamma_{i,j} = 0$. ■

As an immediate consequence of this proposition and the definition of extension degree we get the *multiplicative property of extension degrees*.

Theorem 6.3.13 *[Multiplicative Property of Extension Degrees] Let E/F and K/E be field extensions. Then* extension tower

$$[K : F] = [K : E][E : F]$$

When the extensions are finite, the statement of this theorem deals with the product of natural numbers. However, if any of the extensions is infinite, then this result should be interpreted as dealing with product of cardinals. The same comment applies to Corollary 6.3.14 below.

Definition 6.3.5. An *extension tower* is a sequence of fields extensions $F_0 \leq F_1 \leq \cdots \leq F_n$. We say that this tower has height n.

$\mathbb{Q}(\sqrt{2}, \sqrt{3})$
$\mid$
$\mathbb{Q}(\sqrt{2})$
$\mid$
$\mathbb{Q}$

Example 6.3.6. Consider the tower $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. We have seen that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, and since $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ (why?), we must have $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] > 1$. But $\sqrt{3}$ is a root of $x^2 - 3 \in \mathbb{Q}(\sqrt{2})[x]$, so we get $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$. By the multiplicative property of extension degrees, we conclude that

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

Exercise 6.3.3. Show that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$, and find $\min_{\mathbb{Q}}(\sqrt{2} + \sqrt{3})$.

Using the multiplicative property in Theorem 6.3.13, and induction, we get:

Corollary 6.3.14 *Let $F_0 \leq F_1 \leq \cdots \leq F_n$ be an extension tower. Then*

$$[F_n : F_0] = \prod_{i=1}^{n} [F_i : F_{i-1}]$$

In particular, the overall extension F_n/F_0 is a finite extension iff each step F_{i+1}/F_i is a finite extension.

We can now improve on Corollary 6.3.11 by giving an upper bound on the degree of the extension.

Corollary 6.3.15 *Let $f(x) \in F[x]$ be a polynomial of degree n. There is an extension K of F where $f(x)$ splits and has degree $[K : F] \leq n!$.*

Exercise 6.3.4. Prove Corollary 6.3.15. Hint: use induction on n. See Remark 6.3.2.

We now consider the existence of a splitting field. Later in this section we will consider uniqueness. Let's begin with an extension of Lemma **??**.

Proposition 6.3.16 *Let E/F be a field extension, and $\alpha_1, \ldots, \alpha_n \in E$. The intersection of all subfields of E that contain $\alpha_1, \ldots, \alpha_n$ and F is itself a subfield of E; it contains $\alpha_1, \ldots, \alpha_n$ and F, and it is minimal with this property.*

Definition 6.3.6. The field constructed in Proposition 6.3.16 is called the subextension of E/F generated by $\alpha_1, \ldots, \alpha_n$ and we denote it by $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Proposition 6.3.17 *Let $f \in F[x]$, and K an extension of F where f splits. There is a unique splitting field E of f over F contained in K.*

Proof. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of f in K. Take $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. ■

Note that Proposition 6.3.17 tells us of the uniqueness of a splitting field for f inside K, where f splits. However, f may split in several extensions $K_1, K_2, \ldots$, of F, and in each one of them there will be a splitting field for f. Corollary 6.3.25 will show us that any two such splitting fields will be isomorphic as extensions of F.

Proposition 6.3.18 *Let $f \in F[x]$. There is a splitting field E for f over F.*

Proof. By Corollary 6.3.15 there is an extension K/F where f splits. Apply now Proposition 6.3.17. ■

03/18/2016 Problem Set 6 board presentations

03/21/2016 Class cancelled due to medical emergency

03/23/2016 Problem Set 7 board presentations

03/24/2016 The example $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ shows that the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ generated by two elements $\sqrt{2}$ and $\sqrt{3}$ can also be generated by a single element, i.e. $\sqrt{2} + \sqrt{3}$.

Definition 6.3.7. Let F be a field and u an element in some extension of F. The extension $F(u)/F$ is called a *simple extension*. The element u is called a *primitive element* of the extension.

simple extension
primitive element
algebraic numbers

For a simple extension, a primitive element is not necessarily unique. For example, the extensiion $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ has primitive element $\sqrt{2}+\sqrt{3}$, but it is easy to see that $\sqrt{2}-\sqrt{3}$ is also a primitive element for this extension.

Not every extension is simple, not even the finite ones. We will see a counterexample later on. However, many finite extensions are simple, in particular every finite extension over $\mathbb{Q}$ is simple as we will prove in the Primitive Element Theorem **??**.

Example 6.3.7. $\mathbb{Q}(\sqrt[3]{2},\omega)$, the splitting field of $x^3-2\in\mathbb{Q}[x]$ in $\mathbb{C}$ is an extension of $\mathbb{Q}$ of degree 6. Take $u=\sqrt[3]{2}+\omega$. Then $(u-\omega)^3=2$, i.e. $u^3-3u^2\omega+3u\omega^2-3=0$. But $\omega^2+\omega+1=0$, so we get

$$\omega=\frac{u^3-3u-3}{3(u^2+u)}\in\mathbb{Q}(u),$$

and $\sqrt[3]{2}=u-\omega\in\mathbb{Q}(u)$. Thus, we get $\mathbb{Q}(\sqrt[3]{2},\omega)=\mathbb{Q}(u)$.

Exercise 6.3.5. Find the minimal polynomial $\min_{\mathbb{Q}}(u)$, where $u=\sqrt[3]{2}+\omega$.

Proposition 6.3.19 *An extension E/F is finite iff $E=F(\alpha_1,\ldots,\alpha_n)$ for some $\alpha_1,\ldots,\alpha_n\in E$ algebraic over F.*

Proof. ■

The following corollary extends Corollary **??** to algebraic extensions, and can be easily extended to towers.

Corollary 6.3.20 *Let $K/E/F$ be an extension tower. K/F is algebraic iff K/E and E/F are algebraic.*

Proof. ■

As mentioned earlier, not all algebraic extensions are finite extensions.

Definition 6.3.8. Those complex numbers which are algebraic over $\mathbb{Q}$ are called *algebraic numbers*. The set of all algebraic numbers is denoted by $\mathbb{A}$.

Corollary 6.3.21 *The set $\mathbb{A}$ of all algebraic numbers is a subfield of $\mathbb{C}$, the field of complex numbers. It is an infinite, algebraic extension of $\mathbb{Q}$.*

Proof. ■

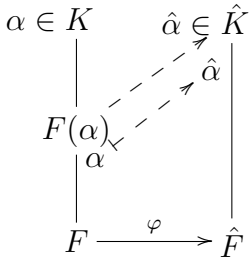
The same argument used to prove that $\mathbb{A}$ is a subfield of $\mathbb{C}$ can be used to show.

Corollary 6.3.22 *Let E/F be a field extension. The set*

$$A = \{a \in E | a \text{ is algebraic over } F\}$$

is a subfield of E that contains F, and it is an algebraic extension of F.

03/25/2016



Lemma 6.3.23 *Let F and $\hat{F}$ be fields, and $\varphi : F \to \hat{F}$ a homomorphism. Denote also by φ the homomorphism induced on the polynomial rings $\varphi : F[x] \to \hat{F}[x]$, according to Lemma* **??**. *Let $p(x) \in F[x]$ be an irreducible polynomial, and denote by $\hat{p}(x)$ its image $\varphi(p(x)) \in \hat{F}[x]$. Let α be a root of $p(x)$ in some extension K of F, and $\hat{\alpha}$ a root of $\hat{p}(x)$ in some extension $\hat{K}$ of $\hat{F}$. There is a homomorphism from $F(\alpha)$ to $\hat{K}$ which agrees with φ on F and maps α to $\hat{\alpha}$.*

Proof. Consider the map $\theta = \mathrm{ev}_{\hat{\alpha}} \circ \varphi$

$$F[x] \xrightarrow{\varphi} \hat{F}[x] \xrightarrow{\mathrm{ev}_{\hat{\alpha}}} \hat{K}$$

The kernel contains $p(x)$ since $\hat{\alpha}$ is a root of $\hat{p}(x)$, but it is not all of $F[x]$. By maximality of $\langle p(x)\rangle$ we must have $\ker\theta = \langle p(x)\rangle$. By the first isomorphism theorem there is an monomorphism, call it also θ from $F[x]/\langle p(x)\rangle$ to $\hat{K}$, such that

$$\theta(f(x) + \langle p(x)\rangle = \theta(f(x)) = \hat{f}(\hat{\alpha}).$$

Composing with the inverse of the isomorphism from Scholium 6.3.9

$$\begin{array}{rccc} \nu: & F[x]/\langle p(x)\rangle & \to & F(\alpha) \\ & f(x) + \langle p(x)\rangle & \mapsto & f(\alpha) \end{array}$$

yields a homomorphism $\Phi : F(\alpha) \to \hat{K}$. Note that for $a \in F$, we have

$$\Phi(a) = \theta(\nu^{-1}(a)) = \theta(a + \langle p(x) \rangle) = \varphi(a)$$

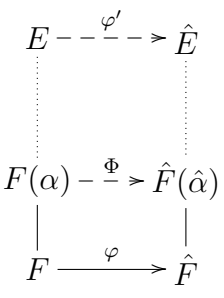
and

$$\Phi(\alpha) = \theta(\nu^{-1}(\alpha)) = \theta(x + \langle p(x) \rangle) = \hat{\alpha}.$$

So, Φ is the desired homomorphism. ■

Corollary 6.3.24 *Let F and $\hat{F}$ be fields, and $\varphi : F \to \hat{F}$ a homomorphism. Denote also by φ the homomorphism induced on the polynomial rings $\varphi : F[x] \to \hat{F}[x]$, according to Lemma* **??**. *Let $f(x) \in F[x]$ be a non-constant polynomial, and denote by $\hat{f}(x)$ its image $\varphi(f(x)) \in \hat{F}[x]$. Let E be a splitting field of $f(x)$ over F, and $\hat{E}$ an extension of $\hat{F}$ where $\hat{f}(x)$ splits. There is a homomorphism $\varphi' : E \to \hat{E}$ which agrees with φ on F. Moreover $\hat{f}(x)$ splits in $\mathrm{Im}(\varphi')$, so that if $\hat{E}$ is a splitting field of $\hat{f}(x)$ over $\mathrm{Im}(\varphi')$, then φ' is an isomorphism.*

Proof. The proof is by induction on $\deg(f(x))$. When $\deg(f(x)) = 1$ then $E = F$. Take $\varphi' = \varphi$. When $\deg(f(x)) > 1$ let $\alpha \in E$ be one of the roots of $f(x)$ and let $p(x)$ be an irreducible factor of $f(x)$ that has α as a root. Note that $\hat{p}(x) = \varphi(p(x))$ is a factor of $\hat{f}(x)$ and therefore it has a root $\hat{\alpha}$ in $\hat{E}$. By the lemma, there is a homomorphism $\Phi : F(\alpha) \to \hat{F}(\hat{\alpha})$ that agrees with φ on F and $\Phi(\alpha) = \hat{\alpha}$. In $F(\alpha)[x]$ we have $f(x) = (x - \alpha)g(x)$ with $\deg(g(x)) = \deg(f(x)) - 1$, and E is a splitting field for $g(x)$ over $F(\alpha)$. $\hat{g}(x) = \Phi(g(x)) \in \hat{F}(\hat{\alpha})[x]$ splits in $\hat{E}$, so by induction there is a homomorphism $\varphi' : E \to \hat{E}$ that agrees with Φ on $F(\alpha)$. Hence it agrees with φ on F. Moreover, by induction, $\hat{g}(x)$ splits in $\mathrm{Im}(\varphi')$, and so does $\hat{f}(x) = (x - \hat{\alpha})\hat{g}(x)$. If $\hat{E}$ is splitting field of $\hat{f}(x)$ over $\hat{F}$, by minimality of splitting field, it must equal $\mathrm{Im}(\varphi')$, so φ' is surjective. Finally, a field homomorphism is always injective. ■



By taking $\hat{F} = F$ and φ the identity map of F, we get the following corollary.

Corollary 6.3.25 *Let $f \in F[x]$ be a non-constant polynomial. If E and $\hat{E}$ are two splitting fields of f, then E and $\hat{E}$ are isomorphic as extensions of F.*

Combining Proposition 6.3.18 with this corollary we get.

Theorem 6.3.26 *Let $f \in F[x]$. There is a splitting field for f over F, which is unique up to isomorphism of extensions of F.*

04/02/2016

Example 6.3.8. We want to find the splitting field for $f = x^4+x^3+x^2+1 \in \mathbb{Z}_2[x]$. Note that 1 is a root of f, so, using synthetic division we can see that it factors as $f = (x+1)(x^3+x+1)$. The first factor is linear, hence irreducible. The second factor is cubic with no roots in $\mathbb{Z}_2$, so it is also irreducible over $\mathbb{Z}_2$. Let α be a root of $x^3 + x + 1$ in some extension of $\mathbb{Z}_2$, so that we have $\alpha^3 + \alpha + 1 = 0$, i.e. $\alpha^3 = \alpha + 1$. Once again, synthetic division yields $f = (x + 1)(x + \alpha)(x^2 + \alpha x + (1 + \alpha^2))$. A direct calculation shows that this last factor has roots α^2 and $\alpha^2 + \alpha$ in $\mathbb{Z}_2(\alpha)$. Therefore, $\mathbb{Z}(\alpha)$ is the splitting field of f. Since $\min_{\mathbb{Z}_2}(\alpha) = x^3 + x + 1$, we have $[\mathbb{Z}_2(\alpha) : \mathbb{Z}_2] = 3$, and $\{1, \alpha, \alpha^2\}$ is a basis for $[\mathbb{Z}_2(\alpha)$ as a vector space over $\mathbb{Z}_2$. Thus,

$$\mathbb{Z}_2(\alpha) = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\}.$$

The multiplication in $\mathbb{Z}_2(\alpha)$ is done using the fact that $\alpha^3 = \alpha+1$. Note that the multiplicative group $\mathbb{Z}_2(\alpha)^*$ on non-zero elements, is a group of order 7, hence cyclic, and is generated by any element different from 1. In particular, it is generated by α, so we have

$$\mathbb{Z}_2(\alpha)^* = \{\alpha, \alpha^2, \alpha^3 = \alpha+1, \alpha^4 = \alpha^2+\alpha, \alpha^5 = \alpha^2+\alpha+1, \alpha^6 = \alpha^2+1, \alpha^7 = 1\}$$

All of these elements satisfy $x^7 = 1$, i.e. are roots of $x^7 - 1$. If we multiply by $x - 0$, we get that all elements of $\mathbb{Z}_2(\alpha)$ are roots of $x^8 - x$. This polynomial has at most 8 distinct roots, so it has exactly 8 roots, i.e. the elements of $\mathbb{Z}_2(\alpha)$, and $\mathbb{Z}_2(\alpha)$ is the splitting field for this polynomial.

We will see in Section 6.4 that the above example is typical of all finite fields.

6.3.1 Algebraic Closure

The Fundamental Theorem of Algebra (FTAlg) tells us that every polynomial with complex coefficients has a root in $\mathbb{C}$. From this, it follows easily that

any polynomial in $\mathbb{C}[x]$ splits over $\mathbb{C}$. This connection holds in a more general setting, as the following proposition indicates.

algebrically closed
algebraic closure

Proposition 6.3.27 *Let F be a field. TFAE:*

1. *Every nonconstant polynomial in $F[x]$ has a root in F.*
2. *Every nonconstant polynomial in $F[x]$ splits over F.*
3. *Every irreducible polynomial in $F[x]$ is linear.*
4. *For any algebraic extension E/F one has $E = F$.*

Proof. ■

The last property in Proposition 6.3.27 tells us that F does not have any proper algebraic extension. Fields that satisfy this property, and hence all four properties in Proposition 6.3.27 are called *algebrically closed*. The FTAlg then tells us that $\mathbb{C}$ is algebraically closed. It follows from Proposition 6.3.27 that $\mathbb{C}$ has no proper algebraic extension.

04/06/2016

Corollary 6.3.28 *Let E/F be a field extension, with E algebraically closed. The set*

$$\overline{F} = \{\alpha \in E | \alpha \text{ is algebraic over } F\}$$

is an algebraic extension of F, and it is algebraically closed.

Proof. The same argument used in Corollary 6.3.21 shows that $\overline{F}$ is a subfield of E. Clearly, it contains F and is an algebraic extension of F. If $f \in \overline{F}[x]$ is a nonconstant polynomial, then it has a root $\alpha \in E$. So, α is algebraic over $\overline{F}$ and $\overline{F}$ is algebraic over F, so α is algebraic over F, and therefore $\alpha \in \overline{F}$. ■

Definition 6.3.9. Given a field extension E/F, we say that E is an *algebraic closure* of F if

- E/F is algebraic, and

- E is algebraically closed.

multiplicity
simple root
multiple root
derivative

Corollary 6.3.28 proves that if E is algebraically closed, then any subfield F of E has an algebraic closure contained in E, namely $\overline{F}$.

It can be shown, using Zorn's Lemma, that any field F has an algebraic closure, unique up to isomorphism of extensions of F. We will not prove this theorem.

6.4 Finite Fields

We have already seen in Proposition **??** that for a finite F, the number of elements of F is a prime power of p^n, where p is the characteristic of F.

In this section we will show that for any prime p and any $n \geq 1$, there is a field with p^n elements, unique up to isomorphism. This result completely characterizes all finite fields.

Let E/F be a field extension, $f \in F[x]$ and $a \in E$. Recall (from Section 4.1 in the textbook) that a is a root of f iff $(x-a)$ is a factor of f. The *multiplicity* of a as a root of f is the largest $m \in \mathbb{N}$ such that $(x-a)^m$ is a factor of f. That is, $f = (x-a)^m \cdot g$ and $(x-a) \nmid g$. A *simple root* is a root of multiplicity $m = 1$. A *multiple root* is a root of multiplicity $m \geq 2$. Proposition 6.4.2 will give us a criteria to distinguish simple roots from multiple roots. First we need the concept of derivative of a polynomial.

Definition 6.4.1. Let F be a field and $f \in F[x]$, written as

$$f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0.$$

The *derivative* of f is defined to coincide with the calculus derivative. However, there is no need for limits. We define

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

Examples 6.4.1. 1. For $f = x^4 - 3x^2 + x - 7 \in \mathbb{Q}[x]$, we have $f' = 4x^3 - 6x + 1$.

2. For $f = x^4 + x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$, we have $f' = x^2$.

fixed field

Note that the degree of f' is at least one less than the degree of f. However, when the $\mathrm{char}(F) \neq 0$, the degree can be even lower, as Example 6.4.1.2 shows. We could even have $f' = 0$ without f being a constant.

Proposition 6.4.1 *Let F be a field, $f, g \in F[x]$, $c \in F$.*

1 $(cf)' = cf'$,

2 $(f + g)' = f' + g'$,

3 $(fg)' = fg' + f'g$,

4 $(f(g))' = f'(g) \cdot g'$.

Proof. Exercise. ■

Proposition 6.4.2 *Let F be a field, $f \in F[x]$, and E an extension of F. An element $a \in E$ is a multiple root of f iff a is a root of both f and f'.*

Proof. First of all, factor f in $E[x]$ as $f = (x-a)^m g$ with the largest possible m, i.e. such that $(x - a) \nmid g$. Thus, m is the multiplicity of a as a root of f.
($\Rightarrow$) Assume $m > 1$. Then, using Proposition 6.4.1, we get $f' = m(x - a)^{m-1}g + (x - a)^m g' = (x - a)^{m-1}(mg + (x - a)g')$. Evaluating at a, we get $f(a) = 0$ and $f'(a) = 0$.
($\Leftarrow$) Assume $f(a) = 0$ and $f'(a) = 0$. From the first we get that $m \geq 1$. If we had $m = 1$, then $f'(a) = g(a) \neq 0$. Therefore, we must have $m > 1$. ■

Examples 6.4.2. 1. The polynomial $f = x^4 + x^2 + x + 1 \in \mathbb{Z}_2[x]$ has derivative $f' = 1$. 1 is a simple root, and all the roots of f are simple. Hence, f has 4 distinct roots in its splitting field.

04/07/2016

Lemma 6.4.3 *Let F be a field and $\varphi : F \to F$ an endomorphism of F. The set*

$$F_\varphi = \{a \in F | \varphi(a) = a\}$$

is a subfield of F. It contains the prime subfield of F. It is called the fixed field *of φ.*

Proof. Exercise ■ fixed field

Corollary 6.4.4 *Let F be a field and G a set of endomorphisms of F. The set* Galois field

$$F_G = \{a \in G | \varphi(a) = a, \text{ for all } \varphi \in G\}$$

is a subfield of F. It contains the prime subfield of F. It is called the ***fixed field*** *of G.*

Theorem 6.4.5 *Let p be a prime and $n \geq 1$. There is a field of order p^n, and it is unique up to isomorphism.*

Proof. Following the idea of Example 6.3.8, consider the polynomial $f = x^{p^n} - x \in \mathbb{Z}_p[x]$. Let E be a splitting field for f over $\mathbb{Z}_p$. Recall that the Frobeniüs map $\Phi : E \to E$ given by $a \mapsto a^p$ is an endomorphism of E. Composing Φ with itself n times yields an endomorphism $\Psi = \Phi^n$ of E, and the roots of f are precisely the elements of E that satisfy $\Psi(a) = a$, i.e. the fixed subfield of Ψ. Since E is minimal containing the roots of f we get that $E = E_\Psi$ is the set of all roots of f. Now, $f' = -1$ has no roots, so by Proposition 6.4.2, f has no multiple roots, i.e. it has p^n distinct roots. Therefore E is a field with p^n elements. This proves the existence part of the theorem.
For the uniqueness, we once again follow the idea of Example 6.3.8. If F is a field with p^n elements, then F^* is a multiplicative group with $p^n - 1$ elements, and all its elements satisfy $x^{p^n-1} = 1$, i.e. they are roots of the polynomial $x^{p^n-1} - 1$. Multiplying by x, we also get 0 as a root, so F is the set of roots of $f = x^{p^n} - x$. So, F is the splitting field of f. By Theorem 6.3.26, tells us that F is unique up to isomorphism. ■

Definition 6.4.2. Let p be a prime, $n \geq 1$ and $q = p^n$. The unique field with q elements is called the ***Galois field*** of order q, and it is denoted by $GF(q)$, or by $\mathbb{F}_q$. Note that $\mathbb{F}_p = \mathbb{Z}_p$.

We now want to show that any finite field $\mathbb{F}_q$ is a simple extension of $\mathbb{F}_p$ where p is the characteristic.

First, we need a lemma about finite abelian groups. Recall from Exercise **??** that if G is a group and $a, b \in G$ have finite order and commute with each other, then there is $c \in G$ whose order is l.c.m.$\{o(a), o(b)\}$. Repeated application of this result yields the following.

Lemma 6.4.6 *Let G be a finite abelian group with $\exp(G) = k$. There is $u \in G$ such that $o(u) = k$.*

Proposition 6.4.7 *If G be a finite subgroup of the multiplicative group F^* of a field F, then G is cyclic.*

Proof. Let $k = \exp(G)$. This means that all elements of G satisfy the equation $x^k = 1$, i.e. they are roots of the polynomial $x^k - 1 \in F[x]$. Since a polynomial of degree k has at most k distinct roots, it follows that $|G| \leq k$. On the other hand, we know, from Lagrange's Theorem, that for any group $\exp(G)$ is a divisor of $|G|$. It then follows that $|G| = k$. By Lemma 6.4.6, G has an element of order k, hence G is cyclic as desired. ■

Corollary 6.4.8 *The multiplicative group $\mathbb{F}_q^*$ of a finite field is cyclic.*

Corollary 6.4.9 *Let p be a prime and $q = p^n$ a power of p. The finite field $\mathbb{F}_q$ is a simple extension of its prime subfield $\mathbb{F}_p$, i.e. $\mathbb{F}_q = \mathbb{F}_p(u)$, for some $u \in \mathbb{F}_q$.*

Proof. Just take u to be a generator of the cyclic group $\mathbb{F}_a^*$. ■

Corollary 6.4.10 *Let p be prime and $n \geq 1$. There exist an irreducible polynomial of degree n in $\mathbb{Z}_p[x]$.*

Proof. Take $f = \min_{\mathbb{Z}_p}(u)$ where $u \in \mathbb{F}_{p^n}$ is such that $\mathbb{F}_{p^n} = \mathbb{F}_p(u)$. ■

Finally, we classify all the subfields of a finite field $\mathbb{F}_q$.

Theorem 6.4.11 *Let p be a prime, $n \geq 1$, and $q = p^n$.*

1. *If K is a subfield of $\mathbb{F}_q$, then $K \approx \mathbb{F}_{p^d}$ for some d divisor of n, and $[\mathbb{F}_q : K] = \frac{n}{d}$.*
2. *If d is a divisor of n, there is exactly one subfield of $\mathbb{F}_{p^n}$ of order p^d, namely the splitting field of $x^{p^d} - x$.*

Proof. (6.4.11.**??**) Since K is a finite field of characteristic p, we know that $K \approx \mathbb{F}_{p^d}$ for some $f \geq 1$. By the multiplicative property of degrees we have $[\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^d}] \cdot [\mathbb{F}_{p^d} : \mathbb{F}_p]$, i.e. $n = [\mathbb{F}_{p^n} : \mathbb{F}_{p^d}] \cdot d$, so $d|n$ and

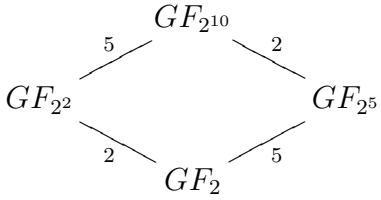
$[\mathbb{F}_{p^n} : \mathbb{F}_{p^r}] = \frac{n}{d}$.
(6.4.11.**??**) Write $n = kd$, and $r = p^d$, so that $p^n = r^k$. Note that

$$r^k - 1 = (r-1)(r^{k-1} + r^{k-2} + \cdots + r^2 + r + 1,$$

in other words,

$$p^n - 1 = (p^d - 1)(p^{d(k-1)} + p^{d(k-2)} + \cdots + p^{2d} + p^d + 1,$$

and $(p^d - 1)|(p^n - 1)$. Since $\mathbb{F}^*_{p^n}$ is a cyclic group, it has a unique subgroup H of order $p^d - 1$. All the elements of H are roots of the polynomial $x^{p^d-1} - 1$, so $H \cup \{0\}$ is the set of roots of $x^{p^d} - x$. The proof of Theorem 6.4.5 shows that $H \cup \{0\}$ is a field of order p^d. ■



Example 6.4.3. Consider the field with 1024 elements. It has four subfields: $\mathbb{F}_2$, $\mathbb{F}_{2^2}$, $\mathbb{F}_{2^5}$, and $\mathbb{F}_{2^{10}}$ itself.
The elements of $\mathbb{F}_2$ are the roots of $x^2 - x = x(x-1)$, i.e. 0 and 1.
The elements of $\mathbb{F}_4$ are the roots of $x^4 - x$. Other than 0 and 1, the other two elements of $\mathbb{F}_4$ have degree 2 over $\mathbb{F}_2$, so $x^4 - x$ must have an irreducible quadratic factor. In fact, $x^4 - x = x(x-1)(x^2 + x + 1)$ is a factorization into irreducible factors, and $x^2 + x + 1$ is the only monic irreducible quadratic polynomial in $\mathbb{F}_2[x]$.
$\mathbb{F}_{32}$ has $32 - 2 = 30$ elements of degree 5 over $\mathbb{F}_2$. Each one of them is a root of an irreducible polynomial of degree 5, and each such irreducible polynomial contributes 5 elements to $\mathbb{F}_{32}$. Since $x^{32} - x$ has no multiple roots, its factorization into irreducible factors cannot have repeated factors. It then follows that $x^{32} - x = x(x-1)f_1f_2f_3f_4f_5f_6$ where $f_1, f_2, f_3, f_4, f_5, f_6$ are distinct irreducible polynomials of degree 5. Moreover, any irreducible polynomial of degree 5 over $\mathbb{F}_2$ has a root in an extension of degree 5 over $\mathbb{F}_2$. But $\mathbb{F}_{32}$ is the only extension of degree 5 over $\mathbb{F}_2$, up to isomorphism. So, any irreducible of degree 5 over $\mathbb{F}_2$ has a root in $\mathbb{F}_{32}$, and it must be one of $f_1, f_2, f_3, f_4, f_5, f_6$. We have shown, that there are exactly 6 irreducible polynomials of degree 5 over $\mathbb{F}_2$, i.e. the factors of $\frac{x^{32}-x}{x(x-1)}$.
There are 32 monic quintic polynomials over $\mathbb{F}_2$. Half of them, have 0 constant term, so they have 0 as a root and are reducible. Of the other 16, the ones with contant term 1, half of them have an even number of non-zero

coefficients, so they have 1 as a root, and are reducible. This leaves 8 potential irreducible quintic polynomials. Those that have constant term 1, and an odd number of non-zero coefficients. But they are not all irreducible. A quintic polynomial may factor as a product of a quadratic irreducible and a cubic irreducible. There is only one monic quadratic irreducible polynomial in $\mathbb{F}_2[x]$, namely $x^2 + x + 1$, and exactly 2 monic cubic irreducible polynomials, namely $x^3 + x^2 + 1$ and $x^3 + x + 1$, there are two quintic polynomials that factor as a product of a quadratic and a cubic:

$$(x^2 + x + 1)(x^3 + x^2 + 1) = x^5 + x + 1$$
$$(x^2 + x + 1)(x^3 + x + 1) = x^5 + x^4 + 1$$

When we exclude these two polynomials from the 8 potential irreducibles we had, we are left with the 6 quintic irreducible polynomials over $\mathbb{F}_2$

$$\begin{array}{l} x^5 \qquad\quad +x^2 \quad +1 \\ x^5 \quad +x^3 \qquad +1 \\ x^5 \quad +x^3+x^2+x+1 \\ x^5+x^4 \quad +x^2+x+1 \\ x^5+x^4+x^3 \quad +x+1 \\ x^5+x^4+x^3+x^2 \quad +1 \end{array}$$

Exercise 6.4.1. How many monic irreducible polynomials of degree 10 are there over $\mathbb{F}_2$?

04/08/2016 Problem Set 8 board presentations