



UiO : Department of Mathematics
University of Oslo

MAT2200 Spring 2023

Revision on fields

Fields

Recall a **field** is a ring F which is

- commutative
- has unity
- such that every non-zero element is a unit.

Some useful facts:

- The non-zero elements of a field form an abelian group under multiplication.
- If $I \leq F$ is an ideal, then $I = \{0\}$ or $I = F$.

If F and E are fields so that F is a subfield of E, we call E an **extension field** of E, and write $F \leq E$.

Kronecker's theorem

Let F be a field and let $f(x) \in F[x]$ be a nonconstant polynomial.

Theorem

There exists a field extension $F \leq E$ such that $f(x)$ has a zero in E.
If $f(x)$ is irreducible, we can take

$$E = F[x]/\langle f(x) \rangle,$$

and $\alpha = x + \langle f(x) \rangle \in E$ will be a zero of $f(x)$.

Algebraic and transcendental elements

Let $F \leq E$ be a field extension, and let $\alpha \in E$ We say α is

- **algebraic** (over F) if there exists a polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$.
- **transcendental** (over F) otherwise.

Complex numbers which are algebraic/transcendental over $\mathbb{Q}$ are called **algebraic/transcendental numbers**

The irreducible polynomial of an element

Let $F \leq E$ be a field extension, and let $\alpha \in E$ be algebraic over F.

Definition

The **irreducible polynomial** of α over F, denoted $\mathrm{irr}(\alpha, F) \in F$, is defined as either

- The unique monic[a], irreducible polynomial with α as a 0, or
- The monic polynomial of minimal degree which has α as a 0.

[a] "Monic" means $f(x) = c_n x^n + c_{n_1} x^{n-1} + \cdots + c_0$ with $c_n = 1$.

If $f(x) \in F[x]$ has α as a zero, then $\mathrm{irr}(\alpha, F)$ divides $f(x)$.

Vector spaces

Let F be a field. A vector space over F is an abelian group V with a given operation of scalar multiplication:

$$F \times V \to V$$
$$(c, v) \mapsto cv$$

We require this operation to satisfy the following axioms, for given $c, d \in F$ and $v, w \in V$:

1. $1v = v$
2. $(c + d)v = cv + dv$
3. $c(v + w) = cv + cw$
4. $c(dv) = (cd)v$

Main example: If $F \leq E$ is a field extension, then E is a vector space over F, with the scalar multiplication given by the product in E.

Basis of a vector space

Let V be a vector space over a field F.

- A sequence of vectors $v_1, \ldots, v_n \in V$ **spans** V if every $v \in V$ can be written as
$$v = c_1 v_1 + c_2 v_2 + \cdots + c_n v_n$$
for some $c_i \in F$.
- A set $v_1, \ldots, v_n \in V$ is **linearly independent** if
$$c_1 v_1 + \cdots + c_n v_n = 0$$
with $c_i \in F$ implies that $c_i = 0$ for all i.
- A sequence $v_1, \ldots, v_n \in V$ is a **basis** for V if it spans V and is linearly independent. Equivalently: $v_1, \ldots, v_n$ is a basis if every $v \in V$ can be written *uniquely* as
$$v = c_1 v_1 + \cdots + c_n v_n.$$

Dimension of a vector space

Let V be a vector space over a field F. If there exists a basis $v_1, \ldots, v_n$ of V, we say V is **finite-dimensional**.

Theorem

If $v_1, \ldots, v_n$ and $v_1', \ldots, v_m'$ are bases of V, then $n = m$.

Definition (which makes sense because of the above theorem)

If V has a basis $v_1, \ldots, v_n$, then we say V has **dimension** n.

Theorem

Suppose V has dimension n. Then

- If $v_1, \ldots, v_k \in V$ span V, $k \geq n$
- If $v_1, \ldots, v_k \in V$ are linearly independent, then $k \leq n$.

Finite and algebraic extensions

Let $F \leq E$ be a field extension.

- If E is finite-dimensional as a vector space over F, we say that the field extension is **finite**.
- If $F \leq E$ is finite, its **degree**, denoted $[E : F]$, is the dimension of E as a vector space over F.
- If every $\alpha \in E$ is algebraic over F, we say that the field extension is **algebraic**.
- $F \leq E$ finite $\Rightarrow$ $F \leq E$ algebraic.

Example

The extension $\mathbb{R} < \mathbb{C}$ is finite (and hence algebraic) of degree 2, since $1, i$ is a basis for $\mathbb{C}$ as a vector space over $\mathbb{R}$.

Simple extensions

Let $F \leq E$, and let $\alpha \in E$. The field

$$F(\alpha) \leq E$$

is the smallest subfield of E which contains F and α. If there is an $\alpha \in E$ such that $E = F(\alpha)$, we say $F \leq E$ is a **simple** extension.

Theorem

If α is algebraic, then

$$F(\alpha) = \varphi_\alpha[F[x]] \simeq F[x]/\langle \text{irr}(\alpha, F)\rangle.$$

If the degree of $\text{irr}(\alpha, F)$ is n, we have $[F(\alpha) : F] = n$, and one basis for $F(\alpha)$ as a vector space over F is given by

$$1, \alpha, \alpha^2, \ldots, \alpha^{n-1} \in F(\alpha)$$

Adjoining elements

Let $F \leq E$ be a field extension, and let $\alpha_1, \ldots, \alpha_n \in E$. The field

$$F(\alpha_1, \ldots, \alpha_n) \leq E$$

is the smallest subfield of E containing F and $\alpha_1, \ldots, \alpha_n$. An extension $F \leq F(\alpha_1, \ldots, \alpha_n)$ can be obtained as a tower of extensions

$$F \leq F(\alpha_1) \leq F(\alpha_1, \alpha_2) \leq \cdots \leq F(\alpha_1, \ldots, \alpha_n),$$

where for each i,

$$F(\alpha_1, \ldots, \alpha_i) \leq F(\alpha_1, \ldots, \alpha_{i+1}) = F(\alpha_1, \ldots, \alpha_i)(\alpha_{i+1})$$

is a simple extension.

Theorem

$F \leq E$ is finite if and only if we can find $\alpha_1, \ldots, \alpha_n \in E$, algebraic over F such that $E = F(\alpha_1, \ldots, \alpha_n)$.

Degrees and towers of extensions

Theorem

Let $F \leq K \leq E$ be finite field extensions. Then

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

If $\alpha_1, \ldots, \alpha_{[E:K]} \in E$ is a basis for E as a vector space over K, and $\beta_1, \ldots, \beta_{[K:F]} \in K$ is a basis for K as a vector space over F, then the collection of all products $\alpha_i \beta_j$ is a basis for E as a vector space over F.

Algebraically closed fields

Definition

A field F is **algebraically closed** if every polynomial $f(x) \in F$ has a zero in F.

Theorem

If F is algebraically closed, then

- If $F \leq E$ is algebraic, then $F = E$.
- Every $0 \neq f(x) \in F[x]$ is a product of polynomials of degree ≤ 1.

Algebraic closures

Definition

Let $F \leq E$ be a field extension. We say E is an **algebraic closure** of F if

1. $F \leq E$ is algebraic, and
2. E is algebraically closed.

Theorem

Every field F has an algebraic closure $F \leq \overline{F}$. It is "unique up to isomorphism": If $\overline{F}$ and $\overline{F}'$ are algebraic closures of F, there is an isomorphism of fields $\psi\colon \overline{F} \to \overline{F}'$ fixing F.

Finite fields

Let F be a finite field, i.e. a field with finitely many elements.

Theorem

The number of elements of F equals p^n for some prime p and integer n.

Theorem

For every prime p and integer $n \geq 1$ there exists a field $GF(p^n)$ with p^n elements. If $\overline{\mathbb{Z}}_p$ is an algebraic closure of $\mathbb{Z}_p$, we have

$$GF(p^n) = \{\alpha \in \overline{\mathbb{Z}}_p \mid \alpha^{p^n} = \alpha\} < \overline{\mathbb{Z}}_p.$$

If F is some field with p^n elements, then $F \simeq GF(p^n)$.

If $F \leq E$ is an extension of finite fields, then $|E| = |F|^{[E:F]}$.

Homomorphisms fixing a field

From this point on we fix a field F, an algebraic closure $\overline{F}$, and assume that every field extension $F \leq E$ is such that $E \leq \overline{F}$.

Definition

Let $F \leq E$ and $F \leq E'$. A homomorphism of fields $\tau \colon E \to E'$ **fixes** F if for every $a \in F$ we have $\tau(a) = a$.

Conjugate elements

Let now F be a field with algebraic closure $\overline{F}$, and let $\alpha, \beta \in \overline{F}$.

Definition

We say that α and β are conjugate over F if $\operatorname{irr}(\alpha, F) = \operatorname{irr}(\beta, F)$.

Theorem

Let $F \leq E$ be an algebraic extension, and let $\tau \colon E \to \overline{F}$ be a homomorphism fixing F. Then for every $\alpha \in E$, $\tau(\alpha)$ must be a conjugate of α.

Theorem

If $\alpha, \beta \in \overline{F}$ are conjugate over F, there exists a unique isomorphism $\psi_{\alpha,\beta} \colon F(\alpha) \to F(\beta)$ which fixes F, and is such that $\psi_{\alpha,\beta}(\alpha) = \beta$.

Automorphisms

Let $F \leq E$ be a finite field extension.

Definition

An **automorphism** of E is an isomorphism $\sigma\colon E \to E$. The set of automorphisms of E which fix F forms a group with multiplication

$$\sigma\tau = \sigma \circ \tau,$$

which we denote $G(E/F)$.

Index

Let $F \leq E$ be a finite field extension.

Definition

The **index** of the field extension, denoted $\{E : F\}$, is the number of homomorphisms $\tau \colon E \to \overline{F}$ fixing F.

- If $F \leq K \leq E$ is a tower of field extensions,

$$\{E : F\} = \{E : K\}\{K : F\}$$

Splitting fields

Definition

- Let $f(x) \in F[x]$. The **splitting field** over F of $f(x)$ is $F(\alpha_1, \ldots, \alpha_m) \leq \overline{F}$, where $\alpha_1, \ldots, \alpha_m$ is the set of zeros of $f(x)$.
- A finite extension $F \leq E$ is **a splitting field** if there exists an $f(x) \in F[x]$ for which E is the splitting field.

Theorem

Let $F \leq E$ be a finite extension. The following are equivalent:

1. $F \leq E$ is a splitting field.
2. Every homomorphism $\tau \colon E \to \overline{F}$ fixing F is an automorphism of E.
3. $|G(E/F)| = \{E : F\}$.

Separable extensions

Let $F \leq E$ be a finite extension.

Theorem

The index $\{E : F\}$ divides the degree $[E : F]$, so $\{E : F\} \leq [E : F]$.

Definition

The extension is **separable** if $\{E : F\} = [E : F]$.

Definition

A field F is **perfect** if every finite extension $F \leq E$ is separable.

Theorem

If F is of characteristic 0 or if F is finite, then F is perfect.

Galois theory, I

Let $F \leq E$ be a finite extension.

Definition

If the extension is separable and E is a splitting field, we say that $F \leq E$ is **finite normal**.

In this case,

$$|G(E/F)| = \{E : F\} = [E : F].$$

Galois theory, II

Let $F \leq E$ be a finite extension. We can map subgroups of $G(E/F)$ to fields K with $F \leq K \leq E$ and vice versa.

Definition

Let $H \leq G(E/F)$ be a subgroup. The **fixed field** of H is

$$E_H = \{\alpha \in E \mid \tau(\alpha) = \alpha \ \forall \tau \in H\},$$

and we have $F \leq E_H \leq E$.

Conversely, given a field K with $F \leq K \leq E$, the group $G(E/K)$ is a subgroup of $G(E/F)$.

Galois theory, III

Theorem

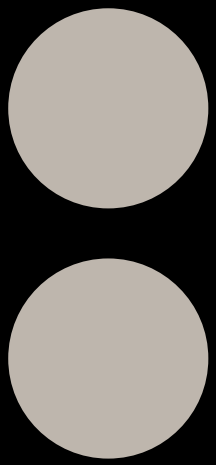
Let $F \leq E$ be a finite normal extension. There is a bijection of sets

$$\{\text{subgroups } H \leq G(E/F)\} \leftrightarrow \{\text{fields } K \mid F \leq K \leq E\}.$$
$$H \mapsto E_H$$
$$G(E/K) \hookleftarrow K$$

- For all $H \leq G(E/F)$, $|H| = [E : K]$
- The subgroup H is normal (as a subgroup) if and only if $F \leq E_H$ is normal (as a field extension). If so

$$G(E/F)/H \simeq G(E_H/F).$$

UiO : Department of Mathematics
University of Oslo



MAT2200 Spring 2023

Revision on fields

