Lecture 1, 4/3/23

Definition 0.1. A field extension $F \subseteq K$ is a field F, which is a subfield of a larger field K.
One way to keep track of how these are related is the degree, $[K : F]$. This is the dimension of K as a vector space over F.
If this degree is $< \infty$, then we refer to this as a finite extension (we of course do not mean that they are finite as sets)
If $S \subseteq K$, then $F(S)$ is the subfield of K given by $F \cup S$.
$F[S]$ is the sub-*ring* of K generated by $F \cup S$. These are different in general!
If $S = \{a_1, \ldots, a_n\}$, we use $F(a_1, \ldots, a_n)$ and $F[a_1, \ldots, a_n]$ to denote $F(S)/F[S]$.
If the extension has the form $F[a]$ for some element a, then this is called a simple extension.
Here, a is called a primitive element.
An extension $F \subseteq K$ is called algebraic if every $k \in K$ is algebraic over F, meaning is the root of some polynomial in $F[x]$

Example 0.1.

- $Q \subseteq \mathbb{R}$. This is an infinite extension. Further, it is not an algebraic extension. The hard way to show this is to demonstrate that some element of $\mathbb{R}$ is not algebraic. For example, π, e are real, but transcendental over the rationals.

  The easy way is by a simple cardinality argument: Because $\mathbb{Q}$ is countable, $\overline{\mathbb{Q}}$ is, but $\mathbb{R}$ is not

- $\mathbb{R} \subseteq \mathbb{C}$. This is a finite extension. In fact, it is a simple extension, with primitive i.

- $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{5})$. This is algebraic. Of course, $\sqrt{5}$ is a root of $x^5 - 1$, but what about the other elements of $\mathbb{Q}(\sqrt{5})$?

  Consider $\{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$. This is a subset of $\mathbb{Q}(\sqrt{5})$, a subring, and a subfield: indeed, consider $\frac{1}{a+b\sqrt{5}}$. The "typical high school trick" is to multiply by the conjugate:
  $$\frac{1}{a+b\sqrt{5}}\frac{a-b\sqrt{5}}{a-b\sqrt{5}} = \frac{a-b\sqrt{5}}{a^2-5b^2}$$
  So $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$, as this is a subfield of $Q(\sqrt{5})$ which contains $\sqrt{5}$, so must contain $\mathbb{Q}(\sqrt{5})$. That is,
  $$\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\} = \mathbb{Q}[\sqrt{5}]$$
  It is easy to see that $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$

Let $F \subseteq K$ be a field extension, and consider $F[a_1, \ldots, a_n]$.
There exists an evaluation map $\varepsilon : F[X_1, \ldots, X_n] \to K$, given by $\varepsilon(f) = f(a_1, \ldots, a_n)$.
ε is a ring homomorphism, so $\operatorname{Im}(\varepsilon)$ is a subring of K. We have $F[a_1, \ldots, a_n] = \operatorname{Im} \varepsilon$
$F(a_1, \ldots, a_n)$ is a quotient field for the ring $F[a_1, \ldots, a_n]$
Let F be a field, x, y be indeterminants which are independent over F. Let $L = F(y)[x]/\langle x^2 - y\rangle$.
We can check that $x^2 - y$ is irreducible in $F(y)[x]$ because it is quadratic, and y has no square roots.
So because this is irreducible, L is a field.
In particular, $F(y)$ embeds in L via the natural map $F(y) \hookrightarrow F(y)[x] \twoheadrightarrow L$. So $F(y) \subseteq L$. This is a degree two extension of $F(y)$.

Proposition 1. *If $[K : F] < \infty$, then $F \subseteq K$ is an algebraic extension.*

Proof. Let $n = [K : F]$, and let $a \in K$. Look at $1, a, a^2, \ldots, a^n$. This is $n + 1$ elements in K, so they must be linearly independent over F. So there exists $c_0, c_1, \ldots, c_n$, not all zero, such that $\sum_{i=0}^{n} c_i a^i = 0$. Then $f = \sum_{i=0}^{n} c_i x^i \in F[x]$ is a polynomial to which a is a solution, so a is algebraic. ∎

Theorem 0.1. *(I)*
Let $F \subseteq K$ be a field extension, $a \in K$. Then The Following Are Equivalent (TFAE):

1. *a is algebraic over F*

2. $\dim_F F[a] < \infty$

3. $[F(a) : F] < \infty$

4. $F(a) = F[a]$

Proof. Notice that $3 \Rightarrow 2$ are really saying the same thing. Further, $2 + 4 \Rightarrow 3$. So if we can connect 1, 2, 4, then 3 will come along for the ride. Therefore, it is enough to show that $1, 2, 4$ are equivalent.

$1 \Rightarrow 2$

There exists a nonzero $f \in F[x]$ such that $f(a) = 0$. $f = \sum_{i=0}^{n} c_i x^i$, where $c_n \neq 0$. So $\sum_{i=0}^{n} c_i a^i = 0$, and so $a^n = \sum_{i=0}^{n-1} d_i a^i$, with $d_i \in F$ new coefficients.

Set $V = \sum_{i=0}^{n-1} Fa^i$. Then $a^n \in V$. So

$$\begin{aligned} a^{n+1} &= \sum_{i=0}^{n-1} d_i a^{i+1} \\ &= \sum_{j=1}^{n-1} d_{j-1} a^j + d_{n-1} a^n \end{aligned}$$

But $d_{n-1}a^n = \sum_{i=0}^{n-1} d_{n-1} d_i a^i$.
Induction gets us that $a^j \in V$ for all $j \geq 0$.
So V is closed under multiplication, hence a subring of K.
So $V = F[a]$. Note $\dim_F F[a] = \dim_F V \leq n$, because we used n elements to span in the first place.

$2 \Rightarrow 4$

It will be enough to show $F[a]$ is a field.
Let $x \in F[a]$, $x \neq 0$. Define a map $\mu_x : F[a] \to F[a]$, given by $\mu_x(y) = xy$. This is F-linear, and $\ker \mu_x = 0$. We have an injective linear transformation from a finite dimensional vector space to itself, so it has to be an isomorphism onto its image. So there exists $x' \in F[a]$ so that $\mu_x(x') = 1$, so x is invertible.

Lecture 2, 4/5/23

We continue the proof.

$4 \Rightarrow 1$

If $A = 0$, we are done. If $A \neq 0$, then $\frac{1}{a} \in F(a) = F[a]$.
So $\frac{1}{a} = \sum_{i=1}^{m} c_i a^i$ where each $c_i \in F$. Note $1 = \sum_{i=0}^{m} c_i a^{i+1}$, so a is a root of $-1 + \sum_{i=0}^{m} c_i x^{i+1} = 0$
Thus a is algebraic over F.

$\blacksquare$

Theorem 0.2. *Assume a is algebraic over K.*

(i) There exists a unique monic polynomial $p \in F[x]$ such that $p(a) = 0$ with minimal degree. We call this the minimal polynomial for a over F, and write $p_{a,F}$.

(ii) p is irreducible.

(iii) If $g \in F[x]$, $g(a) = 0$, then $p \mid g$ in $F[x]$.

(iv) $[F(a) : F] = \deg p$

(v) If $n = \deg p$, then $(1, a, a^2, \ldots, a^{n+1})$ is a basis for $F(a)$ over F.

(vi) Let $\varepsilon : F[x] \to K, \varepsilon(f) = f(a)$. This induces an isomorphism of rings $\overline{\varepsilon} : \frac{F[x]}{\langle p \rangle} \to F(a), \overline{\varepsilon}(f + \langle p \rangle) = f(a)$

Proof.

(i) Since a is algebraic over F, there exists $f \in F[x]$ such that $f(a) = 0$. Note that we can divide by the leading coefficient to make f monic with a as a root. Find minimal polynomial of this form, and call it p.

Uniqueness: Suppose $p' \in F[x]$ is monic, $p'(a) = 0$ minimal. Then $(p - p')(a) = 0$. Since $\deg(p - p') < \deg p$, if $p - p' \neq 0$, we have found a monic polynomial with smaller degree than p with a as a root. Contradiction

(ii) Let $\varepsilon : F[x] \to F(a) = F[a]$ be the evaluation map. ε induces $\overline{\varepsilon} : \frac{F[x]}{\ker \varepsilon} \to F(a)$. Note $\ker \varepsilon = 0$. Since $F[x]$ is a PID, $\ker \varepsilon = \langle q \rangle$ where $0 \neq q \in F[x]$. Without loss of generality, assume q is monic. We know

- q is irreducible
- $q(a) = 0$
- When $g \in F[x], g(a) = 0$, then $q \mid g$

Thus, if $g \neq 0$, $\deg(q) \leq \deg(g)$. This implies that $q = p$.

(iii) See above

(iv) $\overline{\varepsilon}$ is also an isomorphism of vectors over F. Exercise: If $x \in X + \langle p \rangle$, then $(1, x, x^2, \ldots, x^{n+1})$ is a basis for $\frac{F[x]}{\langle p \rangle}$. Thus $(1, a, a^2, \ldots, a^{n-1})$ is a basis for $F(a)$

Furthermore, $[F(a) : F] = n = \deg p$

■

Let $F \leq K$ be a field extension, $a \in K$ algebraic over F. If $p \in F[x]$ is monic and irreducible with $p(a) = 0$, then $p = p_{a,F}$

(v) See iv

(vi) See ii

Example 0.2. Let $a = \sqrt[4]{5} \in \mathbb{R}_{>0}, p = X^4 - 5 \in \mathbb{Q}[x]$. Since p is irreducible over $\mathbb{Q}[x]$, $p = p_{a,F}$.
Note that p is reducible over $\mathbb{Q}(\sqrt{5})[x]$. In fact, $p_{a,\mathbb{Q}[\sqrt{5}]} = x^2 - \sqrt{5}$. We have the tower of fields:

$$\begin{tikzcd}
\mathbb{Q}(a) \arrow[d, dash] \arrow[dd, bend right=60, "4"'] \\
\mathbb{Q}(\sqrt{5}) \arrow[d, dash, "2"] \\
\mathbb{Q}
\end{tikzcd}$$

Let $F \subseteq K \subseteq L$ be a tower of fields. If $a \in L$ is algebraic in F, then a is also algebraic over K. Furthermore, $p_{a,K} \mid p_{a,F}$ in $K[x]$.

Proposition 2. *If $f \in F[x]$ is a nonzero polynomial of degree n, then f has at most n roots in n.*

Proof. By induction.
$n = 0$: trivial.
$n > 0$: if there are no roots, we're okay.
Otherwise, there exists $a \in F$ such that $f(a) = 0$. So $f = (x - alg$, for some $g \in F(x)$.
$g \neq 0, \deg g = n - 1$. Thus g has $\leq n - 1$ roots in F.
Since $\{\text{roots of } f\} = \{a\} \cup \{\text{roots of } g\}$, there are $\leq n$ roots of f.
Let $F \subseteq K$ be a field extension. Let $\mathcal{A} = \{a \in K, a \text{ algebraic over } F\}$.
If F is infinite, then $|\mathcal{A}| = |F|$. If F is finite, $|\mathcal{A}|$ is countable.
Let $\mathbb{A}$ denote the complex numbers which are algebraic over $\mathbb{Q}$. Note $|\mathbb{A}| = |\mathbb{Q}| = \aleph_0$

Lecture 3, 4/10/23