Fields and Galois Theory

Lectures by Uzi Vishne
Summary by Ari Feiglin (`ari.feiglin@gmail.com`)

Contents

1 Field Extensions

Suppose $F \subseteq K$ are fields, then K is certainly also an F-vector space and therefore has a dimension and we denote it $[K : F] := \dim_F K$.

1.0.1 Theorem

Suppose $F \subseteq K$ and V is a K-vector space, then V is also a vector space over F as well, and $\dim_F V = [K : F] \dim_K V$.

Proof: Let $B_1 \subseteq V$ be a basis for V over K and $B_2 \subseteq K$ be a basis for K over F, then define $B = \{\alpha v \mid \alpha \in B_2, v \in B_1\}$. This is a basis for V in F, it is linearly independent since if $\alpha_1 v_1, \ldots, \alpha_n v_n \in B$ and $\beta_1, \ldots, \beta_n \in F$ then $\sum_{i=1}^n \beta_i \alpha_i v_i = 0$ implies $\beta_i \alpha_i = 0$ for all i since B_1 is a basis, and this means that β_i or α_i is zero, but $\alpha_i v_i \in B$ so $\beta_i = 0$ as required. B spans V since for $v \in B$ there exist $v_1, \ldots, v_n \in B_1$ and $\alpha_1, \ldots, \alpha_n \in K$ such that $v = \sum_{i=1}^n \alpha_i v_i$ and α_i can be written as the linear combination of elements in B_2 by elements of F which gives a linear combination of elements in B of F. So B is indeed a basis for V over F. Finally $B \cong B_2 \times B_1$ since $(\alpha, v) \mapsto \alpha v$ is a bijection: it is obviously surjective and $\alpha_1 v_1 = \alpha_2 v_2$ implies $\alpha_1 = \alpha_2, v_1 = v_2$ since v_1, v_2 are independent. Thus we have

$$\dim_F V = |B| = |B_2 \times B_1| = [K : F] \dim_K V$$

$\blacksquare$

In particular if $F \subseteq K \subseteq E$ are fields then $[E : F] = [E : K] \cdot [K : F]$.
The following are methods of constructing fields:

(1) If R is a commutative ring and $M \triangleleft R$ is a maximal ideal then ${}^{R}\!/_{M}$ is a field. Specifically if $R = F[x]$ and p is an irreducible polynomial, $\langle p \rangle$ is maximal and ${}^{F[x]}\!/_{\langle p \rangle}$ is a field.

(2) If F is a field, then the set of rational functions is also a field:

$$F \subseteq F(x) := \left\{ \frac{f(x)}{g(x)} \,\middle|\, f, g \in F[x] \right\},\ g(x) \neq 0]$$

In general if R is an integral domain then its field of fractions/quotients $q(R) := \left\{ \frac{a}{b} \,\middle|\, a, b \in R,\ b \neq 0 \right\}$ is a field. And $F(x)$ is the quotient field of $F[x]$.

(3) If $F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots$ is a chain of fields then so is $\bigcup F_n$ (the theory of fields is inductive, this holds for arbitrary chains, not just inductive ones). So for example $F(\lambda_1, \lambda_2, \ldots)$ is a field since we can define $F_n = F(\lambda_1, \ldots, \lambda_n)$ (the quotient field of $F[\lambda_1, \ldots, \lambda_n]$) and the union of this chain is $F(\lambda_1, \lambda_2, \ldots)$.

Let F be a field and $F \subseteq K$ a ring with $a \in K$, we define a homomorphism $F[\lambda] \xrightarrow{\psi_a} K$ defined by $\alpha \mapsto \alpha$ for $\alpha \in F$ and $\lambda \mapsto a$, meaning

$$\psi_a\Big(\sum \alpha_i \lambda^i\Big) = \sum \alpha_i a^i \qquad (\psi_a(f) = f(a))$$

In particular ψ_a is a linear transformation from F to K, and is called the *evaluation homomorphism* at a. The kernel of the homomorphism is

$$\ker \psi_a = \{f \in F[\lambda] \mid f(a) = 0\} \triangleleft F[\lambda]$$

1.0.2 Definition

$a \in K$ is **algebraic** if $\ker \psi_a \neq 0$ and **transcendental** if the kernel is trivial.

If a is transcendental then $\ker \psi_a$ and so $\operatorname{Im} \psi_a = \{f(a) \mid f \in F[\lambda]\} = F[a] \cong F[\lambda]$. In fact we get

$$\begin{array}{ccccccc} F & \subseteq & F[a] & \subseteq & F(a) & \subseteq & K \\ & & \cong & & \cong & & \\ & & F[x] & & F(x) & & \end{array}$$

Now if a is algebraic, since $F[x]$ is a euclidean domain and therefore a PID, the kernel has a generator $\ker \psi_a = \langle h \rangle = h \cdot F[\lambda]$. So $h(a) = 0$ and $f(a) = 0 \implies h | f$, and h is called the *minimal polynomial* of a. And so

$${}^{F[\lambda]}\!\Big/_{\langle h \rangle} = {}^{F[\lambda]}\!\Big/_{\ker \psi_a} \cong \operatorname{Im} \psi_a = \{f(a) \mid f \in F[\lambda]\} = F[a] = \operatorname{span}\{1, a, \ldots, a^{n-1}\} \subseteq K$$

where $n = \deg h$, since $f(x) = q(x)h(x) + r(x)$ where $\deg r < \deg h = n$ and so $f(a) = r(a)$. $\{1, \dots, a^{n-1}\}$ is a basis due to h being minimal, a zeroing linear combination would give a zeroing polynomial of a of degree less than h. This means that the dimension of $F[a]$ as an F-vector space is n, ie. $\left[F[a] : F\right] = n$.

Since K is an integral domain and therefore so too is $F[a]$ and this means that $\langle h \rangle$ is a prime ideal (since $^R/_I$ is an integral domain if and only if I is prime), this means that h is a prime (irreducible) polynomial. And since $F[a]$ is a PID, prime and maximal ideals are one and the same, so $\langle h \rangle$ is maximal and therefore $^{F[\lambda]}/_{\langle h \rangle} \cong F[a]$ is a field. Let us summarize this:

1.0.3 Proposition

Let $F \subseteq K$ where K is an integral domain and $a \in K$ is algebraic in F, let h_a be its minimal polynomial. Then (1) h_a is irreducible, (2) $F[a]$ is a field, (3) $\left[F[a] : F\right] = \deg h_a$.

So for example let $a \in K \setminus F$ be algebraic then $F \subseteq F[a] \subseteq K$ and suppose $[K : F] = p$ is prime. Then $p = [K : F] = [K : F[a]] \cdot [F[a] : F]$, and since $a \in F[a] \setminus F$ this means $[F[a] : F] > 1$ so $[F[a] : F] = p$ and $[K : F[a]] = 1$ since p is prime so $F[a] = K$.

1.0.4 Corollary

Suppose F is a field and $F \subseteq K$ is an integral domain with finite dimension. Then every element of K is algebraic and K is a field.

Proof: Let $a \in K$ then $[K : F] = [K : F[a]] \cdot [F[a] : F]$ so $[F[a] : F]$ is finite. If a were transcendental then $F[a] \cong F[x]$ and $F[x]$ has infinite dimension over F. K is a field since every $a \in K$ must have a multiplicative inverse, since $F[a]$ is a field. ∎

Notice that $[F[a, b] : F[a]] \leq [F[b] : F]$ since if h_b is b's minimal polynomial in F then it is also a zeroing polynomial in $F[a]$. This means that

$$[F[a, b] : F] = [F[a, b] : F[a]] \cdot [F[a] : F] \leq [F[b] : F] \cdot [F[a] : F]$$

1.0.5 Corollary

Let F be a field and K a field extension, define

$$\mathrm{Alg}_F(K) := \{a \in K \mid a \text{ is algebraic over } F\}.$$

This is a field. Furthermore $F \subseteq \mathrm{Alg}_F(K)$ is an algebraic extension (all elements of $\mathrm{Alg}_F(K)$ are algebraic in F), and $\mathrm{Alg}_F(K) \subseteq K$ is a purely transcendental extension (all elements in $K \setminus \mathrm{Alg}_F(K)$ are transcendental in $\mathrm{Alg}_F(K)$).

Proof: Notice that $F[a \cdot b], F[a + b] \subseteq F[a, b]$ and so $[F[a, b] : F] \leq [F[b] : F] \cdot [F[a] : F] < \infty$, so $\mathrm{Alg}_F(K)$ is closed under addition and multiplication (and obviously additive inverses). For a algebraic, $F[a]$ is a field so $a^{-1} \in F[a]$ and so $F[a^{-1}] \subseteq F[a]$ and therefore $[F[a^{-1}] : F] < \infty$ so a^{-1} is algebraic as well (and so by symmetry $F[a] = F[a^{-1}]$). So $\mathrm{Alg}_F(K)$ is indeed a field.

To show that $\mathrm{Alg}_F(K) \subseteq K$ is a pure transcendental extension, notice that if $F_1 \subseteq F_2 \subseteq F_3$ where $F_1 \subseteq F_2$ is algebraic, if $a \in F_3$ is algebraic in F_2 it is also algebraic in F_1. Indeed if $f \in F_2[x]$ such that $f(a) = 0$, let its coefficients be b_i then a is algebraic in $F_1[b_0, \dots, b_n]$ and so

$$[F_1[b_0, \dots, b_n, a] : F_1[b_0, \dots, b_n]] = [F_1[b_0, \dots, b_n, a] : F_1[b_0, \dots, b_n]] \cdot [F_1[b_0, \dots, b_n] : F_1]$$

and this is finite since $b_0, \dots, b_n$ are algebraic in F_1 as they are in F_2, so both terms are finite. So if K had any algebraic numbers not in $\mathrm{Alg}_F(K)$, they would be algebraic in F and thus in $\mathrm{Alg}_F(K)$ in contradiction. ∎

1.0.6 Proposition

Let F be a field and $f \in F[\lambda]$ be irreducible, then there exists a field extension $F \subseteq K$ such that f has a root in K, and $[K : F] = \deg f$.

Proof: since f is irreducible, $\langle f \rangle$ is prime and $F[\lambda]$ is a PID so it is maximal. So $K := {}^{F[\lambda]}/_{\langle f \rangle}$ is a field, and its dimension is $\deg f$, since it can be generated by $\{1, x, \dots, x^{\deg f - 1}\}$. Now recall that by the second isomorphism theorem, ${}^{F}/_{F \cap \langle f \rangle} \cong {}^{F + \langle f \rangle}/_{\langle f \rangle} \subseteq {}^{F[\lambda]}/_{\langle f \rangle} = K$. But since elements of $\langle f \rangle$ are multiples of f, which is disjoint from F, so $F \cap \langle f \rangle = (0)$ so ${}^{F}/_{F \cap \langle f \rangle} \cong F$, and so F can be embedded into K and is thus for all intents and purposes, a subfield of K. Now define $\alpha := \lambda + \langle f \rangle$, and suppose $f(\lambda) = \sum_{i=0}^{n} a_i \lambda^i$ where $a_i \in F$ (viewing f as a polynomial over K, a_i is actually $a_i + \langle f \rangle$). Then

$$f(\alpha) = \sum_{i=0}^{n} a_i (\lambda + \langle f \rangle)^i = \sum_{i=0}^{n} a_i (\lambda^i + \langle f \rangle) = \sum_{i=0}^{n} a_i \lambda^i + \langle f \rangle = f + \langle f \rangle = \langle f \rangle = 0_K$$

so α is indeed a root of $f(\lambda)$, as required. ∎

1.0.7 Corollary

Let F be a field and $f \in F[\lambda]$ any polynomial. Then there exists a field extension $F \subseteq K$ such that f has a root in K and $[K : F] \leq \deg f$.

Proof: find f's irreducible factorization $f = f_1 \cdots f_t$, then extend F to a field K such that f_1 has a root in K, and by above $[K : F] = \deg f_1 \leq \deg f$. ∎

1.0.8 Definition

Let F be a field, and f a polynomial over F. A field $F \subseteq K$ **splits** f if there exist $\alpha_1, \dots, \alpha_n \in K$ such that $f(\lambda) = (\lambda - \alpha_1) \cdots (\lambda - \alpha_n)$.

1.0.9 Theorem

Every polynomial f over a field F has a field K which splits it, such that $[K : F] \leq (\deg f)!$.

Proof: by induction on $n = \deg f$. For $n = 1$ then f already has a root, and so take $F = K$ and $[K : F] = 1 = (\deg f)!$. Now suppose $\deg f = n + 1$, then by above there exists a field extension $F \subseteq K_0$ such that there exists an $\alpha_1 \in K_0$ such that $f(\alpha_1) = 0$ and $[K_0 : F] \leq \deg f = n + 1$. And so $(\lambda - \alpha_1) | f(\lambda)$, so $f(\lambda) = (\lambda - \alpha_1) g(\lambda)$. Then $\deg g = n$, and g is a polynomial over K_0, so there exists a field extension $F \subseteq K_0 \subseteq K$ such that $g(\lambda) = (\lambda - \alpha_2) \cdots (\lambda - \alpha_{n+1})$ for $\alpha_i \in K$ and $[K : K_0] \leq n!$. Then $f(\lambda) = (\lambda - \alpha_1) \cdots (\lambda - \alpha_{n+1})$ for $\alpha_i \in K$ and $[K : F] = [K : K_0][K_0 : F] \leq (n+1) n! = (n+1)!$. ∎

Notice the following

(1) the split of a polynomial over any field into its roots is unique,

(2) the number of roots is $\leq \deg f$.

Recall that a field F is *algebraically closed* if it splits every polynomial in $F[\lambda]$.

1.0.10 Definition

Let F be a field, then $F \subseteq \overline{F}$ is an **algebraic closure** of F if $\overline{F}$ is algebraically closed.

Note

Every field has a unique (up to isomorphism) algebraic closure.

So let $f(\lambda) \in F[\lambda]$, then $f(\lambda) \in \overline{F}[\lambda]$ and so $f = (\lambda - \alpha_1)\cdots(\lambda - \alpha_n)$ for $\alpha_i \in \overline{F}$. Then take $F \subseteq K = F[\alpha_1, \dots, \alpha_n] \subseteq \overline{F}$, it can be shown that $[K : F] \leq (\deg f)!$.
Now suppose $F \subseteq K$ are fields, and E is a field which F is embeddable into, suppose $\varphi\colon F \hookrightarrow E$ is an embedding. An embedding $\varphi'\colon K \hookrightarrow E$ is an *extension* of φ if $\varphi'\big|_F = \varphi$. Denote

$$\eta^E_{F\subseteq K} := \#\{\varphi' \text{ is an extension of } \varphi\}$$

where φ is held constant and understood. Then

1.0.11 Proposition

Suppose $K = F[\alpha]$, then $\eta^E_{F\subseteq K}$ is equal to the number of roots the minimal polynomial of α in F has in E.

Proof: since α generates K over F, every extension of φ is defined by its image on α. Let h be the minimal polynomial of α over F. Denote $\hat{b} := \varphi(b)$ for all $b \in F$, and this definition extends to polynomials, $\widehat{\sum_{i=0}^n b_i x^i} = \sum_{i=0} \hat{b}_i x^i$. Then if φ' is an extension of φ,

$$\hat{h}(\varphi'(\alpha)) = \varphi'(h(\alpha)) = \varphi'(0) = 0$$

this is since if $h(\lambda) = \sum_{i=0}^n a_i \lambda^i$, then $\hat{h}(\lambda) = \sum_{i=0}^n \hat{a}_i \lambda^i$, so

$$\hat{h}(\varphi'(\alpha)) = \sum_{i=0}^n \hat{a}_i \varphi'(\alpha)^i = \sum_{i=0}^n \varphi(a_i)\varphi'(\alpha)^i = \sum_{i=0}^n \varphi'(a_i)\varphi'(\alpha)^i = \varphi'\left(\sum_{i=0}^n a_i \alpha^i\right) = \varphi'(h(\alpha))$$

so $\varphi'(\alpha)$ must be one of $\hat{h}$'s roots, precisely as stated. ■

1.0.12 Definition

A polynomial f which splits over E is called **separable** in E if its linear factors are distinct (ie. all of its roots in E are distinct).

1.0.13 Theorem

Let $F \subseteq K$ be a finite extension (meaning $[K : F] < \infty$), and let $\varphi\colon F \hookrightarrow E$ be a given embedding. Then

(1) $\eta^E_{F\subseteq K} \leq [K : F]$,

(2) if K is generated by the roots of f, assuming that E splits f, then $1 \leq \eta^E_{F\subseteq K}$,

(3) if f is separable over E, then $\eta^E_{F\subseteq K} = [K : F]$.

Proof: suppose $K = F[\alpha_1, \dots, \alpha_n]$ (the generators of K can be taken to be the basis of K as an F-vector space). We prove this by induction on n, for $n = 1$ this is given by the previous proposition, since $\eta^E_{F\subseteq K}$ is the number of roots h has in E, and $[K : F] = \deg h$ which is at least this. Define $F_1 := F[\alpha_1]$, then

$$\begin{aligned}
\eta^E_{F\subseteq K} &= \#\{\varphi''\colon K \longrightarrow E \text{ is an extension of } \varphi\} \\
&= \#\bigcup\{\varphi''\colon F_1 \longrightarrow E \text{ is an extension of } \varphi' \mid \varphi'\colon F_1 \longrightarrow E \text{ is an extension of } \varphi\} \\
&= \sum_{\varphi'} \eta^E_{F_1\subseteq K} = \eta^E_{F\subseteq F_1} \cdot \eta^E_{F_1\subseteq K} \subseteq [F_1 : F] \cdot [K : F_1] = [K : F]
\end{aligned}$$

For (2), by the assumption there is an extension of $F \hookrightarrow E$ to $F_1 \hookrightarrow E$, and continue inductively. For (3), since f is separable, makes the bound an equality. ■

1.0.14 Definition

Let f be a polynomial over F, a field $F \subseteq K$ is a **splitting field** if it is the smallest field in which the polynomial splits.

Notice that if K is a splitting field, it is of the form $K = F[\alpha_1, \dots, \alpha_n]$ where α_i are roots of the polynomial, so they are algebraic. This means that $[K : F] \leq \prod_i [F : \alpha_i] < \infty$.

Furthermore, if K is a splitting field of f, then it is generated by the roots of f: $K = F[\alpha_1, \dots, \alpha_n]$, then if E is any field which splits f, we have $\eta^E_{F\subseteq K} \geq 1$, meaning there exists an embedding $K \hookrightarrow E$ which extends the embedding $F \hookrightarrow E$. And in particular if K, K' are two splitting fields of f, there exists two embeddings $K \hookrightarrow K'$ and $K' \hookrightarrow K$, which means $[K : F] = [K' : F]$ and so K and K' are isomorphic as F-vector spaces. And so $K \cong K'$ as fields.

Recall that there exists a unique ring homomorphism $f\colon \mathbb{Z} \longrightarrow F$, and ${}^{\mathbb{Z}}\!/_{\ker f} \cong \operatorname{Im} f \subseteq F$. Since $\operatorname{Im} f$ is a subring of F, it is an integral domain and so $\ker f$ is a prime ideal. Thus $\ker f = p\mathbb{Z}$ for p prime or 0, and this p is called *F's characteristic*. In other words F has characteristic p if and only if $1 + \cdots + 1 = 0$ (p times) since then $p \in \ker f$ and so $(p) \subseteq \ker f$, but $\mathbb{Z}$ is a PID and so (p) is maximal. And F has characteristic 0 if $1 + \cdots + 1$ is never zero.

If F has characteristic 0, then f is an embedding into F, so $\mathbb{Z} \subseteq F$ and since it is a field $\mathbb{Q} \subseteq F$, up to embedding. And for characteristic p, ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}} = \mathbb{F}_p \subseteq F$.

Notice that in characteristic p, $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ is zero for $k \neq 0, p$.

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = a^p + b^p$$

And so $e(x) = x^p$ is a field homomorphism $F \longrightarrow F^p = \{x^p \mid x \in F\}$, and it has a trivial kernel, and so $F \cong {}^{F}\!/_{\ker f} \cong F^p$.

1.0.15 Definition

We define the **derivative** over a field F to be the function $F[\lambda] \longrightarrow F[\lambda]$ defined by

$$\left(\sum_{i=0}^{n} \alpha_i \lambda^i\right)' = \sum_{i=1}^{n} \alpha_i \cdot i\lambda^{i-1}$$

It is trivial to show that $(f+g)' = f' + g'$ and $(fg)' = fg + f'g$, meaning that $(f^2g)' = f^2g' + 2ff'g$. This means that if $f^2|h$ then $f|h'$. In particular if f is not separable, then there exists some $(\lambda - \alpha)^2$ which divides f over a field which splits it, then $\lambda - \alpha$ divides f', meaning $f'(\alpha) = 0$. But this means that $f' = 0$, so $\alpha_i i = 0$ for all i, and so if p doesn't divide i this means $i \neq 0$ so $\alpha_i = 0$. Thus

$$f(\lambda) = \sum_{p|i} \alpha_i \lambda^i = \sum_j \alpha_{pj} (\lambda^p)^j$$

So we get that

1.0.16 Proposition

Let f be irreducible over a field of characteristic $p > 0$, then f is not separable if and only if $f' = 0$ if and only if $f(\lambda) = g(\lambda^p)$ for some polynomial g.

1.0.17 Example

Let $\lambda^p - a$ be a polynomial over F of characteristic p, and α a root in a field which splits it. Then

$$\lambda^p - a = \lambda^p - \alpha^p = (\lambda - \alpha)^p$$

so $\lambda^p - a$ is not separable (which we can see since it is $g(\lambda^p)$ for $g(\lambda) = \lambda - a$).

1.0.18 Definition

Let K/F be a field extension (meaning $F \subseteq K$), then an automorphism of K over F is an automorphism $\sigma\colon K \longrightarrow K$ which holds F constant: $\sigma(a) = a$ for all $a \in F$.

Notice that all field homomorphisms are either injective or trivial, since the kernel is an ideal and fields only have trivial ideals, so if σ is a field homomorphism there is no need to check injectivity. And $\sigma(ax) = \sigma(a)\sigma(x) = a\sigma(x)$ for $a \in F$ and $x \in K$ so σ is an F-linear transformation, so if $[K : F]$ is finite σ must be surjective. Thus in the case that K/F is a finite field extension, all monomorphisms of K over F are automorphisms.

1.0.19 Definition

Let K/F be a field extension, then define its **Galois group** to be

$$\mathrm{Gal}(K/F) := \{\sigma \mid \sigma \text{ is an automorphism of } K \text{ over } F\}$$

and this is indeed a group relative to composition.

Notice that if K/F is a field extension and $\alpha \in K$ algebraic. Let h be its minimal polynomial and $\sigma \in \mathrm{Gal}(K/F)$, then

$$h(\sigma(\alpha)) = \sigma(h(\alpha)) = \sigma(0) = 0$$

This is since $\sigma\left(\sum_i a_i\alpha^i\right) = \sum_i \sigma(a_i)\sigma(\alpha)^i = \sum_i a_i\sigma(\alpha)^i = h(\sigma(\alpha))$.

So for example, let $G = \mathrm{Gal}\left(\mathbb{Q}[\sqrt{3}]/\mathbb{Q}\right)$ and $\lambda^2 - 3 = (\lambda - \sqrt{3})(\lambda + \sqrt{3})$ and so σ must map $\sqrt{3}$ to $\pm\sqrt{3}$. And since all automorphisms of $\mathbb{Q}[\sqrt{3}]$ over $\mathbb{Q}$ are defined by $\sqrt{3}$'s image,

$$G = \left\{1, \sqrt{3} \overset{\sigma}{\mapsto} -\sqrt{3}\right\} \cong \mathbb{Z}_2$$

And similarly let $G = \mathrm{Gal}\left(\mathbb{Q}[\sqrt{3}, \sqrt{2}]/\mathbb{Q}\right)$, $\sqrt{3}$ must be mapped to $\pm\sqrt{3}$ (due to $\lambda^2 - 3$) and $\sqrt{2}$ must be mapped to $\pm\sqrt{3}$, so

$$G = \left\{1, \begin{matrix}\sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3}\end{matrix}, \begin{matrix}\sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3}\end{matrix}, \begin{matrix}\sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3}\end{matrix}\right\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

Notice that if K has characteristic p, every automorphism must keep elements of $\mathbb{F}_p$ constant (since $\sigma(1) = 1$). And if K has characteristic 0, every automorphism must keep elements of $\mathbb{Q}$ constant (since $\sigma(a/b) = \sigma(a)/\sigma(b) = a/b$). So let F_0 be the characteristic field of K (either $\mathbb{F}_p$ or $\mathbb{Q}$), so

$$\mathrm{Aut}(k) = \mathrm{Gal}(K/F_0)$$

1.0.20 Definition

Let K be a field, then for every subfield $G \leq \mathrm{Aut}(K)$, define the **fixed-point field**,

$$K^G := \{a \in K \mid \forall\sigma \in G\colon \sigma(a) = a\}$$

This is indeed a field.

Notice that if $F \subseteq K$ is a subfield, then $\mathrm{Gal}(K/F)$ is a subgroup of $\mathrm{Aut}(K)$. And if $G \leq \mathrm{Aut}(K)$ is a subgroup, then K^G is a subfield of K. So we have the following correspondences:

$$\{\text{Subgroups of } \mathrm{Aut}(K)\} \underset{K^{\bullet}}{\overset{\mathrm{Gal}(K,\bullet)}{\rightleftarrows}} \{\text{Subfields of } K\}$$

And if $F \subseteq K$ is a subfield, and $F \subseteq L \subseteq K$ is a field between them, $\mathrm{Gal}(K, L)$ is a subgroup of $\mathrm{Gal}(K/F)$ (since $\sigma \in \mathrm{Gal}(K/L)$ keeps elements of L, and thus F constant). And if $G \leq \mathrm{Gal}(K/F)$, then K^G is a field between F and K. So we have

$$\{\text{Subgroups of } \mathrm{Gal}(K/F)\} \underset{K^{\bullet}}{\overset{\mathrm{Gal}(K,\bullet)}{\rightleftarrows}} \{\text{Fields between } F \text{ and } K\}$$

Some properties:

(**1**) If $L_2 \subseteq L_1$ then $\mathrm{Gal}(K/L_2) \supseteq \mathrm{Gal}(K/L_1)$ since an automorphism which keeps elements of L_1 constant keeps elements of L_1 constant.

(**2**) If $H_2 \subseteq H_1$ then $K^{H_2} \supseteq K^{H_1}$ since if a is held constant by every $\sigma \in H_1$, it is held constant by every $\sigma \in H_2$.

(**3**) For every L, $L \subseteq K^{\mathrm{Gal}(K/L)}$ since $K^{\mathrm{Gal}(K/L)}$ are elements held constant by every automorphism in $\mathrm{Gal}(K/L)$, which includes all elements of L by definition.

(**4**) For every H, $H \subseteq \mathrm{Gal}\big(K/K^H\big)$ since for $\sigma \in H$ every element of K^H is held constant.