Autornorphisms of fields is a rigid situation (not many automorphisms).

Autornorphisms of 

\[ b: R \rightarrow R \text{ bijection, respects any structure} \]

Example

\[ \text{Aut}(\mathbb{R}) = \{1\} \text{ identity is only ring isomorphism} \]

\[ \mathbb{Z} \text{ is both a ring & abelian group, specify which structure you consider} \]

\[ \text{Example} \quad \text{Aut}(\mathbb{Z} \times \mathbb{Z}) = C_2 \quad \text{id, perumute terms, direct product of rings} \]

2) \[ \text{Aut}(\mathbb{Z} \times \mathbb{Q}) = \{1\} \text{ check that } b(e) = e \text{ if } e \text{ is an identity} \]

\[ \text{classify identity in } \mathbb{Z} \times \mathbb{Q} \]

\[ (1,0), (0,1), (0,0), (0,1) \]

\[ \text{prove any automorphism fixes each of them} \]

\[ \text{zero identity} \]

Consider group \( R^* \) of invertible elements of \( R \).

Suppose \( R \) is a non-commutative ring

Then each \( c \in R^* \) acts on \( R \) by conjugation

\[ a \mapsto cac^{-1}, \quad a \in R \]

Check this is a homomorphism

Get a homomorphism \( R^* \xrightarrow{\phi} \text{Aut}(R) \)

\[ \text{by } (a) \quad \phi_c(a) = cac^{-1} \]

Remark: Center of \( R \), denoted \( Z(R) \), is \{ \( a \mid a = ba \text{ for all } b \in R \} \)

\[ \text{Example} \quad Z(R) \text{ is a commutative ring } ZR, \text{ for any ring } R \text{ a subring} \]

\[ Z(R) = R \text{ if } R \text{ is commutative} \]

Check that \( \text{ker } \phi = R^* \cap Z(R) \)

\[ \phi \text{ is given by (a) } \]

\[ \text{Subgroup of } R^* \]
Exercises. Let $M_n(R)$ be the matrix algebra, $R$ commutative.

Then $\mathbb{Z}(M_n(R)) = R \cdot \text{Id}$, multiples of identity matrix.

For general, noncommutative, $R$, $\mathbb{Z}(M_n(R)) \neq \mathbb{Z}(R)$.

Often consider $F$-algebras, $F$ a field. (Assume $R \neq 0$)

Def. An $F$-algebra $R$ is any $R$ with a homomorphism $F \rightarrow R$. $\phi$ is injective, field $F$ is a subring of $R$. 
$R$ acquires a structure of $F$-vector space, can be linear algebra, convenient.

Examples. $R = F, R = F/F$ - field that contains $F$, $F[x], F[x, y], \ldots$

$F/I$, where $I$ is any ideal, $R$ an $F$-algebra.

$F[x]/I = F[x]/(f(x))$, some polynomial $f(x)$.

If $f$ is reducible, $R = F[x]/(f)$ is not a field.

Example. $R = F[x]/(x^2)$, $\text{but } (R/F) \neq 0$.
"not a field" all divisors of $x$

$b(x)$ satisfies $b(x) = b(x^2) = 0$. 
$b(x) = \lambda x^k$, $\lambda \in F^*$, $k = 0$ not an automorphism.

$\Rightarrow \text{not } (R/F) \neq F^k$ if $|F| > 0$, get $\infty$ many automorphisms.

Holds true for rigid, thus cannot happen.
$[F:F] = 2 \Rightarrow \text{Gal } (E/F) = C_2$ or $\{1\}$

Dual.

Exercise. Let $R = F[x]/(x^3)$, $b(x)$ must satisfy $b(x^3) = 0$.

$\Rightarrow b(x) = u(x) + v(x^2)$, $u, v \in F$, not an automorphism.

get a large group of automorphisms of $R$
Reminder: \( E/F \) field extension \( b \in \text{Gal}(E/F) \),

take algebraic \( Z \in E \), \( a_0 + a_1 x + \ldots + a_n x^n = 0 \), \( a_i \in F \), \( f(x) = 0 \)

\( f(x) = \text{irr}(d, F) = a_n x^n + a_0 \)

\( E \rightarrow \bar{E} \)

\( \overline{\text{Gal}(E/F)} \)

\( b(x) \) has the same irreducible polynomial \( \text{irr}(d, F) = \text{irr}(d', F) = f(x) \).

\( f \) has at most \( n \) roots \( d_1, \ldots, d_m \) in \( E \).

at most \( n \) choices for \( b(x) \in \{ d_1, \ldots, d_m \} \).

If \( E = E(d) \), look at homomorphisms into \( K/F \)

\( F(K) = E \rightarrow K \)

\( b(E) \subset K \) subfield \( b|F = \text{id} \) at most \( n \) homomorphisms

where \( m \) is the \# of roots of \( f \) in \( K \).

\( E \rightarrow K \), \( b|F = \text{id} \)

\( \text{such homomorphisms, } b, \text{ are in a bijection } \leftrightarrow \text{roots of } f(x) \text{ in } K. \)

\( \downarrow \)

got a bound on \# of homomorphisms, at most \( n = \deg f \).

\( [F(E):E] = n = \deg f \)

Can trick, if we have

\( E = F(d_1, d_2) \)

\( n_1 \)

\( \text{at most } [F(d_1):F] = n_1 \) homomorphisms (extension)

\( n_2 \)

\( \text{Fix } d_1, \text{ at most } n_2 = [F(d_1, d_2):F(d_1)] \)

\( \text{extensions to } d_2 \)

\( d_1 \in \text{irr}(d_1, F) \) \( \deg_{F(d_1)} b_1 = n_1 \)

\( d_2 \in \text{irr}(d_2, F(d_1)) \) \( \deg_{F(d_1)} b_2 = n_2 \)

\( n_1, n_2 = [F(d_1, d_2):F(d_1)] [F(d_1):F] = [F(d_1, d_2):F] = [E:F] \) if \( E = F(d_1, d_2) \). Otherwise repeat.
To make the argument rigorous, phase if or

\[ E \rightarrow F \quad \quad F \rightarrow F_1 \]

\[ E/F, K/F_1 \] field extensions

\[ \phi: F \rightarrow F_1 \] isomorphism of fields

\# of extension \( b : E \rightarrow K \) homomorphisms,

\[ b \mid F = \phi \] is at most \( [E:F] \).

\# of extensions is no more \([E:F]\) in favorable circumstances:

\( K = K_0 \) is a splitting field of \( f(x) \in F(x), f \) is separable

(always so in char 0)

**E**-field, \( b \) is but \((E)\) an automorphism

**Def** \( E^b \subset E \) is the fixed field of \( b \)

\[ E^b = \{ a \in E \mid b(a) = a \} \]

**Exercise:** \( E^b \) is a subfield of \( E \). \( E^b \) always contains no prime field, \( E \) or \( E(\mathbb{Q} \cup \mathbb{F}_p) \)

\[ X \subset \text{Aut}(E) \text{ a subset} \quad E^X := \{ a \in E \mid b(a) = a \quad \forall b \in X \} \]

\( E^X \subset E \) is a subfield, \( E^X = \cap E^b \) intersection of subfields.

\[ b \in X \]

Let \( H = \langle X \rangle \) be the subgroup of \( \text{Aut}(E) \) generated by \( X \) (smallest subgroup containing \( E \)).

\( H \) consists of arbitrary products of \( E \)'s of \( X \) and their inverses.

\( \forall b \in E^X = EH \) - subfield, \( E \)'s fixed by all automorphisms in \( H \).

**Note** As \( H \) gets bigger, \( E^H \) becomes smaller

\[ H_1 \subset H_2 \Rightarrow E^{H_2} \subset E^{H_1} \]

\[ H = \{ b \} \text{ smallest} \quad E^{\{b\}} = E \]

smaller bigger
Example 1) Subgroups of $S_3$

Index is written on edges.

2) Subgroups of $C_{12} = \{ g | g^{12} = 1 \} = \mathbb{Z}(12, +)$

$C_6 \subseteq C_{12}$ \quad \text{with} \quad C_6/C_2 \cong C_3$

$\{1, g^3, g^6\} \cong \{1, 2, 4\}$
If $H \subseteq \text{Gal}(E/F)$, get a subfield $E^H$, $F \subseteq E^H \subseteq E$.

If $F \subseteq K \subseteq E$, have a subgroup $\text{Gal}(E/K)$ - automorphisms of $E$ that fix each element of $K$.

In favorable circumstances, get a bijection:

intermediate subfields $K$ \quad \longleftrightarrow \quad subgroups $H \subseteq \text{Gal}(E/F)$

$F \subseteq K \subseteq E$ \quad $H = \text{Gal}(E/K)$, $K = E^H$.

Remark: (Friedman, Gruenberg 1.8) Notes on Galois Theory I, p. 5

Let $E$ be an extension field of $F$, $f(x) \in F[x]$. Let $d_1, \ldots, d_n$ be distinct roots of $f$ in $E$.

$\{d_1, \ldots, d_n\} = \{x \in E : f(x) = 0\}$. $d_i \neq d_j$ if $i \neq j$.

Then $\text{Gal}(E/F)$ acts on $\{d_1, \ldots, d_n\}$ & there is a homomorphism

$\varphi : \text{Gal}(E/F) \rightarrow S_n$, $S_n$ - symmetric group

If, in addition, $E = F(d_1, \ldots, d_n)$, then $\varphi$ is injective and

$\text{Gal}(E/F) \subseteq S_n$. Then also $|\text{Gal}(E/F)| \leq n!$ and

the order is a divisor of $n!$.

Proof: If $E/F$ is a finite extension, then $|\text{Gal}(E/F)|$ is finite,

$|\text{Gal}(E/F)| \leq [E:F]$.

Proof: Use our techniques on extending field homomorphisms.
$E = \mathbb{Q}$  \hspace{1cm}  $\mathbb{Q}(\sqrt{2}) = (\mathbb{Q}^2)(\sqrt{2} - 3)$

$E = \mathbb{Q}(\sqrt{2}, \sqrt{3}) / \mathbb{Q}$ splitting field

$G = \text{Gal}(E/\mathbb{Q}) = \text{Aut}(E)$
Prime field

\[ \{ \pm \sqrt{2}, \pm \sqrt{3} \} \text{ roots of } f \]

$\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}$ label roots

$G \rightarrow S_4 = \text{permutations (4 roots)}'$ is injective, since roots generate $F$. What's the image $\text{Im}(\varphi)$ in $S_4$?

$E \supset \mathbb{Q}(\sqrt{2}) \supset \mathbb{Q} \quad \sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.

\[
\begin{array}{c}
E \\
\mathbb{Q}(\sqrt{2}) \\
\mathbb{Q}
\end{array}
\xrightarrow{\varphi} 
\begin{array}{c}
E \\
\mathbb{Q}(\sqrt{2}) \\
\mathbb{Q}
\end{array}
\]

2 automorphisms: $\sqrt{2} \rightarrow \sqrt{2}$ \& $\sqrt{2} \rightarrow -\sqrt{2}$

$\varphi|_{\mathbb{Q}(\sqrt{2})}$ is an ext. of $\mathbb{Q}$

$\sqrt{3} \notin \mathbb{Q}(\sqrt{2}) \Rightarrow \text{Gal}(E/\mathbb{Q}(\sqrt{2})) \cong C_2$

$\sqrt{2} \rightarrow -\sqrt{2}$ \quad identity \&

$\sqrt{3} \rightarrow \sqrt{3}$

$\sqrt{2} \rightarrow \sqrt{2}$ independently

$\sqrt{3} \rightarrow -\sqrt{3}$

$\text{Im}(\varphi) \cap \{1, (12)\} \cap \{1, (34)\} = C_2 \times C_2$

$G = \{1, (12), (34), (1234)\}$ Klein 4 group

This is a special case

\[
\begin{array}{c}
E \\
\mathbb{Q}(\sqrt{2}) \\
\mathbb{Q}
\end{array}
\xrightarrow{\varphi} 
\begin{array}{c}
E \\
\mathbb{Q}(\sqrt{2}) \\
\mathbb{Q}
\end{array}
\]

both fields are fixed by $\varphi$'s of $G$

$\text{Gal}(E/\mathbb{Q}) \cong \text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \times \text{Gal}(\mathbb{Q}(\sqrt{3})/\mathbb{Q})$

$= C_2 \times C_2$
\[ f = x^4 - 2 \quad \text{irreducible (Eisenstein)} \]

splitting field \( E \subseteq \mathbb{Q} \), roots \( \sqrt{2}, i\sqrt{2}, -\sqrt{2}, -i\sqrt{2} \)

\[ G = \text{Gal}(E/\mathbb{Q}) \rightarrow S_4 \text{ permutations, subgroup} \]

**Proof**

\( E/F \) splitting field of irreducible \( f \in F[x] \rightarrow \)

\( \text{Gal}(E/F) \) acts transitively on \( \text{roots of } f \) in \( E \)

**Proof**

\[ f(x) = c(x - d_1) \ldots (x - d_n) \] (separable case; inseparable case)

distinct \( d_1, \ldots, d_n \), terms are \((x - d_i)^m\)

\[ b \text{ is an isomorphism. } b \text{ extends to an automorphism} \]

\[ \overline{b} : E \rightarrow E, \overline{b} \in \text{Gal}(E/F) \]

**Back to example**

\( G \rightarrow S_4 \), action on roots is transitive

Complex conjugation yields automorphism of \( E \)

\[ \begin{array}{cccc}
\sqrt{2} & \quad & i\sqrt{2} \\
-\sqrt{2} & \quad & -i\sqrt{2} \\
\end{array} \]

\[ \begin{array}{cccc}
1 & \quad & 2 & \quad & 3 \\
& \rightarrow & & \rightarrow & \\
& \text{conjugation} & & \text{conjugation} & \\
& \text{exchanging} & & \text{exchanging} & \\
\end{array} \]

execute: \( H \subseteq S_4, |H| = 8, H \not\cong C_2 \times C_2 \)

\( H \) acts transitively on \( \{1, 2, 3, 4\} \implies \)

\( H \) is the dihedral group \( D_4 \subset S_4 \)

but \( E \cong \text{Gal}(E/\mathbb{Q}) = D_4 \).
Remark. Automorphisms of $E$ do not come from automorphisms of $C$.

$C$ has "topology" and has only two symmetries that preserve its
topology: identity & complex conjugation.

Denote $C$. Forget about $C$, think of $E$ as extension of $Q$.

Degree 8: $E$ is a vec. space over $Q$ of dimenson 8, basis

$$
\left\{ 1, \sqrt{2}, \sqrt{2}, i, \sqrt{2}i, i, \sqrt{2}i, \sqrt{2}i, \sqrt{2}i \right\}
$$

basis for $E \cong \mathbb{R} = Q(\sqrt{2})$.

Most symmetries of $E$ extend to "bad" symmetries of $C$ that do not respect distance on topology on $C$ and cannot be written down explicitly.

We only use embedding in $C$ do get partial information about $E$.

Think of $E$ as an 8-dimensional $\mathbb{R}$ vec. with multiplication

$$E = \mathbb{R}^8 + \text{extra structure (multiplication $\otimes$ group of symmetries).}$$