SMSTC supplementary module
Galois Theory of Commutative Rings

Andrew Baker (University of Glasgow)

updated 02/10/2019

Recollections on undergraduate Galois theory of fields

- Studies finite field extensions $F \leqslant E$ (also denoted E/F).
- Galois extension = normal + separable.
- When the extension E/F is Galois interesting things happen:
  - Order of the Galois group $\mathrm{Gal}(E/F) = \mathrm{Aut}_F(E)$ is $|\mathrm{Gal}(E/F)| = \dim_F E$.
  - Order reversing *Galois Correspondence* between subgroups of $\mathrm{Gal}(E/F)$ and intermediate fields $F \leqslant E' \leqslant E$; normal subgroups correspond to normal extensions E'/F.

$$H \leqslant \mathrm{Gal}(E/F) \Longleftrightarrow E^H$$

    where $E^H = \{x \in E : \forall h \in H,\ hx = x\}$ is the fixed field of H.
  - *The Normal Basis Theorem*: For a Galois extension E/F with Galois group $G = \mathrm{Gal}(E/F)$, $E \cong FG$ as FG-modules where FG is the group ring of G over F. The twisted group ring of G over E satisfies $E\{G\} \cong \mathrm{End}_F E$.

Recollections on undergraduate Galois theory of fields

- Studies finite field extensions $F \leqslant E$ (also denoted E/F).
- Galois extension = normal + separable.
- When the extension E/F is Galois interesting things happen:
  - Order of the Galois group $\mathrm{Gal}(E/F) = \mathrm{Aut}_F(E)$ is $|\mathrm{Gal}(E/F)| = \dim_F E$.
  - Order reversing *Galois Correspondence* between subgroups of $\mathrm{Gal}(E/F)$ and intermediate fields $F \leqslant E' \leqslant E$; normal subgroups correspond to normal extensions E'/F.

$$H \leqslant \mathrm{Gal}(E/F) \Longleftrightarrow E^H$$

    where $E^H = \{x \in E : \forall h \in H,\ hx = x\}$ is the fixed field of H.
  - *The Normal Basis Theorem*: For a Galois extension E/F with Galois group $G = \mathrm{Gal}(E/F)$, $E \cong FG$ as FG-modules where FG is the group ring of G over F. The twisted group ring of G over E satisfies $E\{G\} \cong \mathrm{End}_F E$.

Recollections on undergraduate Galois theory of fields

- Studies finite field extensions $F \leqslant E$ (also denoted E/F).
- Galois extension = normal + separable.
- When the extension E/F is Galois interesting things happen:
  - Order of the Galois group $\mathrm{Gal}(E/F) = \mathrm{Aut}_F(E)$ is $|\mathrm{Gal}(E/F)| = \dim_F E$.
  - Order reversing *Galois Correspondence* between subgroups of $\mathrm{Gal}(E/F)$ and intermediate fields $F \leqslant E' \leqslant E$; normal subgroups correspond to normal extensions E'/F.

$$H \leqslant \mathrm{Gal}(E/F) \Longleftrightarrow E^H$$

    where $E^H = \{x \in E : \forall h \in H,\ hx = x\}$ is the fixed field of H.
  - *The Normal Basis Theorem*: For a Galois extension E/F with Galois group $G = \mathrm{Gal}(E/F)$, $E \cong FG$ as FG-modules where FG is the group ring of G over F. The twisted group ring of G over E satisfies $E\{G\} \cong \mathrm{End}_F E$.

Recollections on undergraduate Galois theory of fields

- Studies finite field extensions $F \leqslant E$ (also denoted E/F).
- Galois extension = normal + separable.
- When the extension E/F is Galois interesting things happen:
  - Order of the Galois group $\mathrm{Gal}(E/F) = \mathrm{Aut}_F(E)$ is $|\,\mathrm{Gal}(E/F)| = \dim_F E$.
  - Order reversing *Galois Correspondence* between subgroups of $\mathrm{Gal}(E/F)$ and intermediate fields $F \leqslant E' \leqslant E$; normal subgroups correspond to normal extensions E'/F.

$$H \leqslant \mathrm{Gal}(E/F) \Longleftrightarrow E^H$$

    where $E^H = \{x \in E : \forall h \in H,\ hx = x\}$ is the fixed field of H.
  - *The Normal Basis Theorem*: For a Galois extension E/F with Galois group $G = \mathrm{Gal}(E/F)$, $E \cong FG$ as FG-modules where FG is the group ring of G over F. The twisted group ring of G over E satisfies $E\{G\} \cong \mathrm{End}_F E$.

Recollections on undergraduate Galois theory of fields

- Studies finite field extensions $F \leqslant E$ (also denoted E/F).
- Galois extension = normal + separable.
- When the extension E/F is Galois interesting things happen:
  - Order of the Galois group $\mathrm{Gal}(E/F) = \mathrm{Aut}_F(E)$ is $|\,\mathrm{Gal}(E/F)| = \dim_F E$.
  - Order reversing *Galois Correspondence* between subgroups of $\mathrm{Gal}(E/F)$ and intermediate fields $F \leqslant E' \leqslant E$; normal subgroups correspond to normal extensions E'/F.

$$H \leqslant \mathrm{Gal}(E/F) \Longleftrightarrow E^H$$

where $E^H = \{x \in E : \forall h \in H,\ hx = x\}$ is the fixed field of H.
  - *The Normal Basis Theorem*: For a Galois extension E/F with Galois group $G = \mathrm{Gal}(E/F)$, $E \cong FG$ as FG-modules where FG is the group ring of G over F. The twisted group ring of G over E satisfies $E\{G\} \cong \mathrm{End}_F E$.

Recollections on undergraduate Galois theory of fields

- Studies finite field extensions $F \leqslant E$ (also denoted E/F).
- Galois extension = normal + separable.
- When the extension E/F is Galois interesting things happen:
  - Order of the Galois group $\mathrm{Gal}(E/F) = \mathrm{Aut}_F(E)$ is $|\mathrm{Gal}(E/F)| = \dim_F E$.
  - Order reversing *Galois Correspondence* between subgroups of $\mathrm{Gal}(E/F)$ and intermediate fields $F \leqslant E' \leqslant E$; normal subgroups correspond to normal extensions E'/F.

$$H \leqslant \mathrm{Gal}(E/F) \Longleftrightarrow E^H$$

    where $E^H = \{x \in E : \forall h \in H,\ hx = x\}$ is the fixed field of H.
  - *The Normal Basis Theorem*: For a Galois extension E/F with Galois group $G = \mathrm{Gal}(E/F)$, $E \cong FG$ as FG-modules where FG is the group ring of G over F. The twisted group ring of G over E satisfies $E\{G\} \cong \mathrm{End}_F E$.

Extension to commutative rings

What do normal and separable mean and can they be extended to commutative rings?

Answer: Rewrite field theory in terms of ring theory. For a Galois extension E/F with Galois group $G = \mathrm{Gal}(E/F)$, there is a ring isomorphism

$$E \otimes_F E \cong \mathrm{Map}(G, E) \qquad (*)$$

which is G-equivariant with respect to the action of G on the right hand factor of the domain and the domain in the function ring. In fact

$$\mathrm{Map}(G, E) \cong \prod_G E$$

so $E \otimes_F E$ has $|G|$ idempotents.

All of this makes sense if F and E are replaced by commutative rings $R \leqslant S$ and the Galois group by a subgroup $G \leqslant \mathrm{Aut}_R(S)$.

We take $(*)$ together with the requirement that $S^G = R$ to be the definition of S being a G-Galois extension of R.

Extension to commutative rings

What do normal and separable mean and can they be extended to commutative rings?

Answer: Rewrite field theory in terms of ring theory. For a Galois extension E/F with Galois group $G = \mathrm{Gal}(E/F)$, there is a ring isomorphism

$$E \otimes_F E \cong \mathrm{Map}(G, E) \qquad (*)$$

which is G-equivariant with respect to the action of G on the right hand factor of the domain and the domain in the function ring.

In fact

$$\mathrm{Map}(G, E) \cong \prod_G E$$

so $E \otimes_F E$ has $|G|$ idempotents.

All of this makes sense if F and E are replaced by commutative rings $R \leqslant S$ and the Galois group by a subgroup $G \leqslant \mathrm{Aut}_R(S)$.

We take $(*)$ together with the requirement that $S^G = R$ to be the definition of S being a G-Galois extension of R.

Extension to commutative rings

What do normal and separable mean and can they be extended to commutative rings?

Answer: Rewrite field theory in terms of ring theory. For a Galois extension E/F with Galois group $G = \mathrm{Gal}(E/F)$, there is a ring isomorphism

$$E \otimes_F E \cong \mathrm{Map}(G, E) \qquad (*)$$

which is G-equivariant with respect to the action of G on the right hand factor of the domain and the domain in the function ring.

In fact

$$\mathrm{Map}(G, E) \cong \prod_G E$$

so $E \otimes_F E$ has $|G|$ idempotents.

All of this makes sense if F and E are replaced by commutative rings $R \leqslant S$ and the Galois group by a subgroup $G \leqslant \mathrm{Aut}_R(S)$.

We take $(*)$ together with the requirement that $S^G = R$ to be the definition of S being a G-Galois extension of R.

Extension to commutative rings

What do normal and separable mean and can they be extended to commutative rings?

Answer: Rewrite field theory in terms of ring theory. For a Galois extension E/F with Galois group $G = \mathrm{Gal}(E/F)$, there is a ring isomorphism

$$E \otimes_F E \cong \mathrm{Map}(G, E) \qquad (*)$$

which is G-equivariant with respect to the action of G on the right hand factor of the domain and the domain in the function ring.

In fact

$$\mathrm{Map}(G, E) \cong \prod_G E$$

so $E \otimes_F E$ has $|G|$ idempotents.

All of this makes sense if F and E are replaced by commutative rings $R \leqslant S$ and the Galois group by a subgroup $G \leqslant \mathrm{Aut}_R(S)$.

We take $(*)$ together with the requirement that $S^G = R$ to be the definition of S being a G-Galois extension of R.

Extension to commutative rings

What do normal and separable mean and can they be extended to commutative rings?
Answer: Rewrite field theory in terms of ring theory. For a Galois extension E/F with Galois group $G = \mathrm{Gal}(E/F)$, there is a ring isomorphism

$$E \otimes_F E \cong \mathrm{Map}(G, E) \qquad (*)$$

which is G-equivariant with respect to the action of G on the right hand factor of the domain and the domain in the function ring.
In fact

$$\mathrm{Map}(G, E) \cong \prod_G E$$

so $E \otimes_F E$ has $|G|$ idempotents.
All of this makes sense if F and E are replaced by commutative rings $R \leqslant S$ and the Galois group by a subgroup $G \leqslant \mathrm{Aut}_R(S)$.

We take $(*)$ together with the requirement that $S^G = R$ to be the definition of S being a G-Galois extension of R.

Technicalities required

To work over a general ring R requires homological algebra and notion of separable and étale algebras.

Other topics that might be discussed:

- Cohomological aspects relating to Brauer groups and Picard groups, Hochschild and André-Quillen cohomology.
- Interpretation in algebraic geometry language (Galois and étale coverings).
- Number theoretic examples.
- Hopf Galois extensions: replace group action by (co)action of a Hopf algebra.
- Galois extensions in derived commutative algebra and algebraic topology.
- More abstract formulations of Galois Theory in symmetric monoidal categories.

Technicalities required

To work over a general ring R requires homological algebra and notion of separable and étale algebras.

Other topics that might be discussed:

- Cohomological aspects relating to Brauer groups and Picard groups, Hochschild and André-Quillen cohomology.
- Interpretation in algebraic geometry language (Galois and étale coverings).
- Number theoretic examples.
- Hopf Galois extensions: replace group action by (co)action of a Hopf algebra.
- Galois extensions in derived commutative algebra and algebraic topology.
- More abstract formulations of Galois Theory in symmetric monoidal categories.

Technicalities required

To work over a general ring R requires homological algebra and notion of separable and étale algebras.

Other topics that might be discussed:

- Cohomological aspects relating to Brauer groups and Picard groups, Hochschild and André-Quillen cohomology.
- Interpretation in algebraic geometry language (Galois and étale coverings).
- Number theoretic examples.
- Hopf Galois extensions: replace group action by (co)action of a Hopf algebra.
- Galois extensions in derived commutative algebra and algebraic topology.
- More abstract formulations of Galois Theory in symmetric monoidal categories.

Technicalities required

To work over a general ring R requires homological algebra and notion of separable and étale algebras.

Other topics that might be discussed:

- Cohomological aspects relating to Brauer groups and Picard groups, Hochschild and André-Quillen cohomology.
- Interpretation in algebraic geometry language (Galois and étale coverings).
- Number theoretic examples.
- Hopf Galois extensions: replace group action by (co)action of a Hopf algebra.
- Galois extensions in derived commutative algebra and algebraic topology.
- More abstract formulations of Galois Theory in symmetric monoidal categories.

Technicalities required

To work over a general ring R requires homological algebra and notion of separable and étale algebras.

Other topics that might be discussed:

- Cohomological aspects relating to Brauer groups and Picard groups, Hochschild and André-Quillen cohomology.
- Interpretation in algebraic geometry language (Galois and étale coverings).
- Number theoretic examples.
- Hopf Galois extensions: replace group action by (co)action of a Hopf algebra.
- Galois extensions in derived commutative algebra and algebraic topology.
- More abstract formulations of Galois Theory in symmetric monoidal categories.

Technicalities required

To work over a general ring R requires homological algebra and notion of separable and étale algebras.

Other topics that might be discussed:

- Cohomological aspects relating to Brauer groups and Picard groups, Hochschild and André-Quillen cohomology.
- Interpretation in algebraic geometry language (Galois and étale coverings).
- Number theoretic examples.
- Hopf Galois extensions: replace group action by (co)action of a Hopf algebra.
- Galois extensions in derived commutative algebra and algebraic topology.
- More abstract formulations of Galois Theory in symmetric monoidal categories.

Technicalities required

To work over a general ring R requires homological algebra and notion of separable and étale algebras.

Other topics that might be discussed:

- Cohomological aspects relating to Brauer groups and Picard groups, Hochschild and André-Quillen cohomology.
- Interpretation in algebraic geometry language (Galois and étale coverings).
- Number theoretic examples.
- Hopf Galois extensions: replace group action by (co)action of a Hopf algebra.
- Galois extensions in derived commutative algebra and algebraic topology.
- More abstract formulations of Galois Theory in symmetric monoidal categories.

Technicalities required

To work over a general ring R requires homological algebra and notion of separable and étale algebras.

Other topics that might be discussed:

- Cohomological aspects relating to Brauer groups and Picard groups, Hochschild and André-Quillen cohomology.
- Interpretation in algebraic geometry language (Galois and étale coverings).
- Number theoretic examples.
- Hopf Galois extensions: replace group action by (co)action of a Hopf algebra.
- Galois extensions in derived commutative algebra and algebraic topology.
- More abstract formulations of Galois Theory in symmetric monoidal categories.