15.1 Separable splitting fields

**Theorem 15.1**: For a finite Galois extension $E/F$, we have a natural isomorphism

$$\text{Br}(E/F) = H^2(\text{Gal}(E/F), E^\times).$$

To use this theorem, we want to say that every element splits over a finite Galois extension. In characteristic 0, every finite extension is contained in a finite Galois extension and we proved that every element splits over a finite extension. In general, a field extension is contained in a Galois extension iff it is separable.

**Proposition 15.2**: Every element in $\text{Br}(F)$ splits over a finite separable extension (and hence over a finite Galois extension).
Proof. Let $D$ be a skew field with center $F$ (so a central simple algebra over $F$). It’s enough to show that there exists a commutative subfield $E \subset D$ such that $E \supseteq F$ and $E/F$ is separable; then we can consider instead the centralizer $D' = Z_D(E)$; since $[Z_D(E)] = [E \otimes F D]$, we are done by induction on dim $D$, use Lemma 14.12. Suppose such an $E$ does not exist. Then, by field extension theory, for every $x \in D$, there exists $n$ such that $x^n \in F$.

Lemma 15.3: Let $A$ be an $F_p$-algebra. For $x \in A$, we have $\text{ad}(x)^p = \text{ad}(x^p)$, where $\text{ad}(x)(y) = y \mapsto xy -yx$.

Proof. If $a, b$ are commuting elements in an $F_p$-algebra, then $(a - b)^p = a^p - b^p$. Applying this to $a = L_x$ and $b = R_x$, where $L_x$ is left multiplication by $x$ and $R_x$ is right multiplication by $x$, we see that $(a - b)^p = \text{ad}(x)^p$ while $a^p - b^p = \text{ad}(x^p)$.

Now we have two ways to finish the argument.

The first uses Engel’s Theorem (see 18.745): if $\mathfrak{g} \subset \mathfrak{gl}_n(F)$ is a subalgebra consisting of nilpotent matrices, then $\mathfrak{g}$ is nilpotent. Equivalently, it is contained in the algebra of strictly upper triangular matrices in some basis. The lemma implies that $\text{ad}(x)$ is nilpotent for all $x$. Hence, the image of $D$ in the Lie algebra $\text{End}_F(D)$ (via the map $x \mapsto \text{ad}(x)$) is nilpotent by Engel’s Theorem. This contradicts that $D \otimes_F E \cong \text{Mat}_n(E)$ for some $E$.

The second uses Jordan normal form. Pick $x \in D$ such that $x \not\in F$ but $x^p \in F$. Let $E = F(x)$. Then $[E:F] = p$ and $\text{dim}_F(Z_D(E)) = \frac{d^2}{p}$. By the lemma, $\text{ad}(x)^p = 0$ where $\text{ad}(x) : D \rightarrow D$, and

$$\text{dim}_F(\ker(\text{ad}(x))) = \text{dim}_F(Z_D(E)) = \frac{\text{dim}_F(D)}{p}.$$ 

Therefore, the Jordan normal form of $\text{ad}(x)$ must have $d^2/p$ equal Jordan blocks of size $p > 1$. In particular, $\ker(\text{ad}(x)) \subset \text{im}(\text{ad}(x))$. So if $x \in \ker(\text{ad}(x))$, there exists $y$ such that $[x, y] = x$. Then $\text{ad}(-y)$ fixes $x$, so $\text{ad}(-y)$ cannot be nilpotent, contradiction. \qed

15.2 Group cohomology

Let $G$ be a group. Recall that a $G$-module is the same as a $\mathbb{Z}[G]$-module, and for such a $G$-module $M$, we define

$$H^i(M) := \text{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z}, M)$$

where $\mathbb{Z}$ is the trivial $\mathbb{Z}[G]$-module. In other words, $H^i$ is the $i$th derived functor of the functor of $G$-invariants. To compute this, you can also use the bar resolution, which is a resolution for any flat algebra over a commutative ring, in particular $\mathbb{Z}[G]$. This results in a complex where $C^n$ consists of maps $f : G^n \rightarrow M$ and the differential is

$$df(g_0, \ldots, g_n) = g_0f(g_1, \ldots, g_n) + \sum_{i=0}^{n-1} (-1)^i f(\ldots, g_ig_{i+1}, \ldots) + (-1)^n f(g_0, \ldots, g_{n-1}).$$

Example 15.4: In particular, a 1-cocycle is a map $c : G \rightarrow M$ such that $gc(h) - c(gh) + c(g) = 0$; these are called “cross homomorphisms” and you can produce them from an $M$-torsor $T$ over $G$ and a choice of point $x_0 \in T$. The correspondence takes a cocycle $c$ to the $G$-module structure on $M$ where $g.m = m + c(g) (T = M$ and $x_0 = 0)$. Given a torsor $T$ and a point $x_0 \in T$, for each $g \in G$ we set $c(g)$ to be the element in $M$ such that $g(x_0) = x_0 + c(g)$. Varying the choice of a point results in adding a coboundary to the cocycle. We end up with a bijection between $H^1(G, M)$ and isomorphism classes of $M$-torsors over $G$. There is also a bijection between $H^1(G, M)$ and extensions of $\mathbb{Z}$ by $M$ because of its definition as $\text{Ext}^1$.

Remark 15.5: Moreover, the definition of $H^1(G, M)$ generalizes to the case when $M$ is a nonabelian group equipped with a $G$-action, and in this case we view $M$ as acting on itself on the right, while $G$ acts on the left. This does not hold for higher cohomology.
Example 15.6: A 2-cocycle is a map \( c : G^2 \to M \) such that \( gc(h, k) - c(gh, k) + c(g, hk) - c(g, h) = 0 \).

**Definition 15.7:** A cross-product extension of \( G \) by \( M \) is a group \( \tilde{G} \) with a normal subgroup identified with \( M \) and an isomorphism \( G/M \cong G \) (i.e., an extension of \( G \) by \( M \)) such that the conjugation action of \( G \) on \( M \), which automatically factors through \( G \), coincides with the given action of \( G \) on \( M \) (the cross-product).

2-cocycles are in bijection with cross-product extensions of \( G \) by \( M \) together with a splitting of the surjection of sets \( \tilde{G} \to G \). Choosing a different splitting modifies the cocycle by a coboundary. Hence, there is a bijection between \( H^2(G, M) \) and cross-product extensions of \( G \) by \( M \) up to isomorphism.

### 15.3 Cross-product algebras

Recall that given a group \( G \) acting on a ring \( R \), we can form the smash product

\[
G \# R = \bigoplus_{g \in G} R_g, x_g y_h = (x g(y))_{gh}.
\]

Given a cocycle \( c \in H^2(G, R^\times) \), one can define a twisted version of this called the cross-product algebra,

\[
G \#_c R = \bigoplus_{g \in G} R_g, x_g y_h = (x g(y)c(g, h))_{gh}.
\]

Up to isomorphism, the cross-product algebra depends only on the class of \( c \) in \( H^2(G, R^\times) \).

This can also be described in terms of the cross-product group \( \tilde{G} \) as

\[
\tilde{G} \# R/(\lambda - [\lambda]), \lambda \in R^\times, [\lambda] \in \tilde{G} \text{ is the corresponding element.}
\]