An Example of Conjugate Subfields

This handout presents two examples from class on Monday, March 30 again. These examples illustrate the following lemma from class, which is Lemma 7.2.4 in the book:

Lemma. Let $L/K/F$ be algebraic extensions. Define $G = \mathrm{Gal}(L/F)$ and $H = \mathrm{Gal}(L/K)$. Then:

1. $H \subseteq G$ is a subgroup, and
2. For all $\sigma \in G$, we have $\mathrm{Gal}(L/\sigma K) = \sigma H \sigma^{-1}$.

Both of the examples to be presented here are in the following context.
Fix p prime and $D \in \mathbb{Q}$ not a p-th power. Let $\boxed{F = \mathbb{Q} \text{ and } L = \mathbb{Q}(\zeta_p, \sqrt[p]{D}).}$
So L/F is Galois, since it is the splitting field of $x^p - D \in \mathbb{Q}[x]$ over $\mathbb{Q}$.
(For $D = 2$, which is the value I used in class, see Section 6.4.A. For $p = 3$, see also Example 7.2.3.)

Let $G = \mathrm{Gal}(L/F)$. Recall (from Section 6.4.A, which I also did as an example in class on Friday, March 13) that $|G| = [L : F] = p(p-1)$, and in fact that

$$\boxed{G = \{\sigma_{ij} \,|\, i \in \mathbb{F}_p^\times,\, j \in \mathbb{F}_p\} \text{ where } \sigma_{ij}(\zeta_p) = \zeta_p^i \text{ and } \sigma_{ij}\big(\sqrt[p]{D}\big) = \zeta_p^j \sqrt[p]{D}}$$

This group is isomorphic to $\mathbb{F}_p^\times \ltimes \mathbb{F}_p$, with σ_{ij} written as (i, j). The group is also isomorphic to $\mathrm{AGL}(1, \mathbb{F}_p)$, with σ_{ij} written as γ_{ij}, where $\gamma_{ij} : \mathbb{F}_p \to \mathbb{F}_p$ by $\gamma_{ij}(t) = it + j$. The point here is that the group law is given by

$$\boxed{(i,j)(k,\ell) = (ik, i\ell + j), \text{ with inverses given by } (i,j)^{-1} = \big(i^{-1}, -i^{-1}j\big)}$$

for any $i, k \in \mathbb{F}_p^\times$ and $j, \ell \in \mathbb{F}_p$. That is, $\sigma_{ij}\sigma_{k\ell} = \sigma_{ik, i\ell+j}$.

Example 1. Let $\boxed{K = \mathbb{Q}(\sqrt[p]{D}), \text{ so that we have } L/K/F.}$ What are the conjugate fields σK?
Well, given any $\sigma \in G$, we have $\sigma = \sigma_{ij}$ for some $(i, j) \in \mathbb{F}_p^\times \ltimes \mathbb{F}_p$, so

$$\sigma_{ij}\big(\sqrt[p]{D}\big) = \zeta_p^j \sqrt[p]{D}, \quad \text{and hence} \quad \sigma_{ij}K = \mathbb{Q}\big(\zeta_p^j \sqrt[p]{D}\big)$$

So let's define $\boxed{K_j = \mathbb{Q}\big(\zeta_p^j \sqrt[p]{D}\big)}$ for each $j = 0, 1, \ldots, p-1$, so that $K_0 = K$, and $\boxed{\sigma_{ij}K = K_j.}$

Separately, let's define $\boxed{H = \mathrm{Gal}(L/K),}$ which is automatically a subgroup of $G = \mathrm{Gal}(L/F)$
Then since every $\sigma \in G$ already fixes every $a \in F = \mathbb{Q}$, we must have

$$\boxed{H = \big\{\sigma \in G \,\big|\, \sigma\big(\sqrt[p]{D}\big) = \sqrt[p]{D}\big\} = \{\sigma_{i,0} \,|\, i \in \mathbb{F}_p^\times\}}$$

where the second equality is, of course, because $\sigma_{ij}(\sqrt[p]{D}) = \sqrt[p]{D} \iff j = 0$.

So for any $(i, j) \in \mathbb{F}_p^\times \ltimes \mathbb{F}_p$, the lemma above says that we are supposed to have

$$\mathrm{Gal}(L/K_j) = \mathrm{Gal}(L/\sigma_{ij}K) = \sigma_{ij} H \sigma_{ij}^{-1}.$$

Let's verify that now.
First, note that since K_j depends only on j and not on i, the group $\sigma_{ij} H \sigma_{ij}^{-1}$ ought to be independent of i. So for any $(i, j) \in \mathbb{F}_p^\times \ltimes \mathbb{F}_p$, let's define

$$\boxed{H_j = \sigma_{ij} H \sigma_{ij}^{-1} = \big\{\sigma_{ij}\sigma_{k0}\sigma_{ij}^{-1} \,\big|\, k \in \mathbb{F}_p^\times\big\} = \big\{\sigma_{k, j(1-k)} \,\big|\, k \in \mathbb{F}_p^\times\big\}}$$

where the second equality is by the following computation in $\mathbb{F}_p^\times \ltimes \mathbb{F}_p$:

$$(i,j)(k,0)(i,j)^{-1} = (ik, j)\big(i^{-1}, -i^{-1}j\big) = \big(iki^{-1}, ik(-i^{-1}j) + j\big) = \big(k, j(1-k)\big).$$

Sure enough, this set H_j — which is necessarily a subgroup of G, since it is a conjugate $\sigma H \sigma^{-1}$ of the subgroup H — depends only on j, and not on i. And also, we can see that this subgroup $H_j = \sigma_{ij} H \sigma_{ij}^{-1}$ is indeed equal to $\mathrm{Gal}(L/K_j)$, as the lemma claims, because

$$\boxed{\mathrm{Gal}(L/K_j) = \big\{\sigma \in G \,\big|\, \sigma\big(\zeta_p^j \sqrt[p]{D}\big) = \zeta_p^j \sqrt[p]{D}\big\} = \big\{\sigma_{k,\ell} \in G \,\big|\, \ell = j(1-k)\big\} = H_j}$$

where the final equality is by the computation of H_j above, and the second equality is because

$$\sigma_{k,\ell}\big(\zeta_p^j \sqrt[p]{D}\big) = \sigma_{k,\ell}(\zeta_p)^j \sigma_{k,\ell}\big(\sqrt[p]{D}\big) = \big(\zeta_p^k\big)^j \cdot \zeta_p^\ell \sqrt[p]{D} = \zeta_p^{kj+\ell} \sqrt[p]{D},$$

and hence $\sigma_{k,\ell}\big(\zeta_p^j \sqrt[p]{D}\big) = \zeta_p^j \sqrt[p]{D}$ if and only if $kj + \ell = j$, i.e., if and only if $\ell = j(1-k)$ (as elements of $\mathbb{F}_p$).

Example 2. Let $\boxed{M = \mathbb{Q}(\zeta_p), \text{ so that we have } L/M/F.}$ What are the conjugate fields σM?
Well, given any $\sigma \in G$, we have $\sigma = \sigma_{ij}$ for some $(i,j) \in \mathbb{F}_p^\times \ltimes \mathbb{F}_p$, so

$$\sigma_{ij}(\zeta_p) = \zeta_p^i \quad \text{and hence} \quad \sigma_{ij} M = \mathbb{Q}\big(\zeta_p^i\big) = \mathbb{Q}(\zeta_p) = M$$

because, since $\gcd(p,i) = 1$, there exists $m \in \mathbb{Z}$ such that $mi \equiv 1 \pmod{p}$, and hence $(\zeta_p^i)^m = \zeta_p$.
So $\sigma M = M$ for all $\sigma \in G$. That is, M has only one conjugate field: itself.

Separately, let's define $\boxed{N = \mathrm{Gal}(L/M),}$ which is automatically a subgroup of $G = \mathrm{Gal}(L/F)$
Then since every $\sigma \in G$ already fixes every $a \in F = \mathbb{Q}$, we must have

$$\boxed{N = \big\{\sigma \in G \,\big|\, \sigma(\zeta_p) = \zeta_p\big\} = \{\sigma_{1,j} \,|\, j \in \mathbb{F}_p\}}$$

where the second equality is, of course, because $\sigma_{ij}(\zeta_p) = \zeta_p \iff i = 1$.

The lemma says that for any $\sigma \in G$, we have $\mathrm{Gal}(L/\sigma M) = \sigma N \sigma^{-1}$.
But since $\sigma M = M$ for all $\sigma \in G$, this means we are supposed to have

$$\sigma N \sigma^{-1} = \mathrm{Gal}(L/\sigma M) = \mathrm{Gal}(L/M) = N \quad \text{for all} \quad \sigma \in G.$$

Let's verify that now. That is, we wish to show that $N \lhd G$.
Equivalently, for any $\sigma \in G$ and any $\tau \in N$, we wish to show that $\sigma\tau\sigma^{-1} \in N$.
To see this, given such σ, τ, write $\sigma = \sigma_{ij}$ and $\tau = \sigma_{1,\ell}$ for some $(i,j) \in \mathbb{F}_p^\times \ltimes \mathbb{F}_p$ and some $\ell \in \mathbb{F}_p$.
Then

$$\sigma\tau\sigma^{-1} = \sigma_{ij}\sigma_{1,\ell}\sigma_{ij}^{-1} = \sigma_{1,i\ell} \in N$$

where the second equality is by the following computation in $\mathbb{F}_p^\times \ltimes \mathbb{F}_p$:

$$(i,j)(1,\ell)(i,j)^{-1} = (i, i\ell + j)\big(i^{-1}, -i^{-1}j\big) = \big(ii^{-1}, i(-i^{-1}j) + i\ell + j\big) = \big(1, i\ell\big).$$

This completes our verification that $N \lhd G$, and hence that yes indeed,

$$\mathrm{Gal}(L/\sigma M) = \mathrm{Gal}(L/M) = N = \sigma N \sigma^{-1},$$

once again confirming the truth of the lemma.