BOWDOIN COLLEGE MATH DEPARTMENT

MATH 3702: ALGEBRAIC NUMBER THEORY

FINAL PROJECT

WRITTEN BY ARAV AGARWAL
PROFESSOR NAOMI TANABE

Summary: This project takes up the general problem of applying techniques from Galois Theory to understanding prime decomposition in number fields. The primary reference is Chapter 4 of the lovely textbook *Number Fields* by Daniel A. Marcus. We begin by introducing the reader to necessary theorems and techniques from Galois Theory, before moving on to the second section of the paper where we actually apply these to prime decomposition.

We have attempted to keep this exposition as complete as possible, and it is mostly self-contained, with occasionally citations to references for unimportant proofs.

In the interest of brevity, we do not cover all of Chapter 4's results. It is however worth mentioning that the work displayed in this paper lays the groundwork for a short and elegant proof of the Quadratic Reciprocity Law, and serves as the necessary background to an introduction to the Frobenius Automorphism.

1. Primer on Galois Theory for Subfields of $\mathbb{C}$

We would like this exposition to be as complete as possible, so we begin by spending some time recalling the basics of Galois Theory. Given our context, we will do this specifically for subfields of $\mathbb{C}$. This will require us to fill in a few gaps, in the sense that we will provide proofs of some highly non-trivial facts we have assumed throughout the semester.

In what follows, unless otherwise stated, K and L are assumed to be subfields of $\mathbb{C}$ with $K \subset L$, such that $[L : K]$ is finite. We note that the results of this section can be generalized to arbitrary finite separable field extensions.

Theorem 1.1. *Every embedding of K in $\mathbb{C}$ extends to exactly $[L : K]$ embeddings of L in $\mathbb{C}$.*

Proof. (Induction on degree). Define $d = [L : K]$. Base case of $d = 1$ is clear. Assume $d > 1$. Let σ be an embedding of K in $\mathbb{C}$. Consider some $\alpha \in L\backslash K$. Let f be a monic irreducible for α over K. Let $g = \sigma(f)$, and so g is irreducible over σK. Note σK is also a subfield of $\mathbb{C}$, and $\deg f = \deg g = n$. Now, for any root β of g, we have an isomorphism $\phi : K(\alpha) \to \sigma K(\beta)$, s.t. ϕ restricts to σ on K. To see this note that any element of $K(\alpha)$ is uniquely written as $\sum_{i=0}^{n-1} c_i\alpha^i$, with $c_i \in K$ and multiplication carried out modulo f. Similarly, any element of $\sigma K(\beta)$ is uniquely written as $\sum_{i=0}^{n-1} d_i\beta^i$, with $d_i \in \sigma K$ and multiplication carried out modulo g. Then, ϕ acts as $\alpha \mapsto \beta$ and $c_i \mapsto \sigma(c_i)$, extended as a homomorphism.
We can now observe that σ can be extended to an embedding of $K(\alpha)$ by mapping α to β. But we have n choices for β (g has n roots), so this means σ has n extensions to $K(\alpha)$. Indeed, these are the only extensions: an extension of σ is determined completely by where it sends α and K, and α must map to a root of g.
We can now consider how each of the exactly n embeddings of $K(\alpha)$ extend to embeddings of L. Since we know $[L : K(\alpha)] < [L : K]$, we can apply our inductive hypothesis and conclude that each of these n embeddings extends to exactly $[L : K(\alpha)]$ embeddings of L in $\mathbb{C}$. But then in total we have exactly $n \cdot [L : K(\alpha)]$ extensions of σ to L. Now note that

$$n \cdot [L : K(\alpha)] = [K(\alpha) : K] \cdot [L : K(\alpha)] = [L : K].$$

We have hence shown that σ has exactly $[L : K]$ extensions to L. □

Now, if we consider the identity embedding of K in $\mathbb{C}$, we get the following corollary:

Corollary 1.2. *There are exactly $[L : K]$ embeddings of L in $\mathbb{C}$ which fix K pointwise.*

We now treat in completion the notion of a normal extension, a notion we have used throughout the semester but never formally explored.

Definition 1.3 (Normal extension)**.** L is normal over K iff L is closed under taking conjugates over K.

For this course, we have generally used an alternate definition of a normal extension. This is provided by the following theorem.

Theorem 1.4. *L is normal over K iff every embedding of L in $\mathbb{C}$ fixing K pointwise is actually an automorphism; equivalently, L has exactly $[L : K]$ automorphisms fixing K pointwise.*

Proof. ($\Longrightarrow$) Consider an embedding σ of L in $\mathbb{C}$ fixing K pointwise. Note that any $\alpha \in L$ must be mapped to a conjugate of α over K: this is seen by noting that such a σ fixes the irreducible for α over K. But L is normal, so the conjugates are contained within L itself. This means σ maps L into itself. Since $\sigma(L) \subset L$ has the same degree (choose $[L : K]$ linearly independent elements) over K, we must have $\sigma(L) = L$. This shows σ is an automorphism.
($\Longrightarrow$) Let $\alpha \in L$, and $\beta \in \mathbb{C}$ be a conjugate of α over K. We want to show $\beta \in L$. Note first that as described in the proof of Theorem 1.1, we have an isomorphism from $K(\alpha) \cong K(\beta)$. But we can

extend this to an embedding of L that fixes K and sends α to β. We know that this must actually be an automorphism, and hence $\beta \in L$. □

Recall how we have often had the need to extend a given finite extension to a normal extension; this turn out to be a very useful technique for working with conjugates in many different proof contexts. But we never showed that this was actually possible. The following theorem (technically its corollary) will fix that.

Theorem 1.5. *If $L = K(\alpha_1, \ldots, \alpha_n)$ and L contains the conjugates of all of the α_i, then L is normal over K.*

Proof. Let σ be some embedding of L that fixes K pointwise. By Theorem 1.4, it suffices to show that σ is actually an automorphism. To show this in turn, note that because σ is an embedding, it is enough to show that σ maps L into itself, and by invariance of degree over K this would imply L is mapped onto L as well. So, we work on showing that given any $\alpha \in L$, we have $\sigma(\alpha) \in L$. Note that we can write $\alpha = f(\alpha_1, \ldots, \alpha_n)$, i.e. as a polynomial in α_i with coefficients in K. But then $\sigma(\alpha) = \sigma(f(\alpha_1, \ldots, \alpha_n)) = f(\sigma(\alpha_1), \ldots, \sigma(\alpha_n))$. Since $\sigma(\alpha_i) \in L$, this shows $\sigma(\alpha) \in L$, finishing the proof. □

Corollary 1.6. *If L is any finite extension of K then there is a finite extension M of L which is normal over K. Any such M is also normal over L.*

Proof. Recall Steinitz's Primitive Element Theorem (see Theorem 21.6 in [2]); this allows us to write $L = K(\alpha)$. Now, let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ be all the conjugates of α over K. Define $M = K(\alpha, \alpha_2, \ldots, \alpha_n)$. Clearly $M \supset L$. Also M is directly seen to be normal over K by application of Theorem 1.5. This shows any finite extension can be extended to a normal extension.
Next, we show that any such M is normal over K. For this, we consider an embedding σ of M in $\mathbb{C}$ fixing L pointwise. Note σ then also fixes K pointwise, but since M is normal over K this means σ is an automorphism. We have shown that any embedding of M fixing L is an automorphism, so by Theorem 1.4 this means M is normal over L. □

Our exposition so far was necessary for two reasons. First, as earlier alluded, we hoped to justify all the assumptions we made this semester. Second, this has laid the necessary groundwork for the remainder of this paper, because this will allow us to get our hands dirty with some real Galois Theory.

Definition 1.7 (Galois group)**.** The Galois group of L over K is defined to be the group of automorphisms of L which fix K pointwise. The group operation is composition. We denote this group as $\operatorname{Gal}(L/K)$.

We now solve a problem, which allows us to rephrase normality in Galois Theoretic language.

Problem 1.1. Show L is normal over K iff $\operatorname{Gal}(L/K)$ has order $[L : K]$.

Proof. ($\implies$) Note that any element of $\operatorname{Gal}(L/K)$ is an automorphism, and hence embedding, of L fixing K. We know there are only $[L : K]$ such embeddings by Corollary 1.2, so $|\operatorname{Gal}(L/K)| \leqslant [L : K]$. Further, by normality, every embedding is an automorphism, and so $[L : K] \leqslant |\operatorname{Gal}(L/K)|$. Hence, $|\operatorname{Gal}(L/K)| = [L : K]$.
($\impliedby$) Consider embeddings of L fixing K. We know there are only $[L : K]$ of these. Since $|\operatorname{Gal}(L/K)| = [L : K]$, and any automorphism is an embedding, we see that all embeddings of L fixing K are automorphisms, and so by Theorem 1.4 this means L is normal over K. □

Definition 1.8 (Fixed Field)**.** Given a subgroup $H \leqslant \operatorname{Gal}(L/K)$, we define the fixed field of H to be the field consisting of all elements of L fixed by all elements of H. Denote this as L_H. So,

$$L_H = \{\alpha \in L \mid \sigma(\alpha) = \alpha, \forall \sigma \in H\}.$$

The verification that L_H is actually a subfield of E is seen easily to follow from the fact that σ is an automorphism. The details are left as an exercise.

We are now in a position to solve the following problem.

Problem 1.2. Show that if L is normal over K and $G = Gal(L/K)$, then K is the fixed field of G, i.e., $K = L_G$. Also, show K is not the fixed field of any proper subgroup of G.

Proof. Clearly $K \subset L_G$, because elements of G fix K. Now, suppose this containment is proper, i.e., $K \subsetneq L_G$. Note that L_G is then a non-trivial field extension of K, and a subfield of L, so that $[L : L_G] < [L : K]$. Now, by normality, Problem 1.1 tells us that $|G| = [L : K]$. In particular, since all elements of G are automorphisms of L fixing L_G, we see that we have at least $[L : K]$ such automorphisms (hence also embeddings). But we know from Theorem 1.1 that there are only $[L : L_G]$ such embeddings, and since $[L : L_G] < [L : K]$, we have found too many embeddings of L fixing L_G. This is a contradiction. So, we must have $K = L_G$.
Next, we show K is not the fixed field of any proper subgroup of G (indeed this means it is strictly smaller). ASFSOC that $H < G$ and $L_H = K$. Choose $\alpha \in L$ s.t. $L = K(\alpha)$. Now define

$$f(x) = \prod_{\sigma \in H} (x - \sigma(\alpha)).$$

We claim f is fixed by H: for any $\tau \in H$, we have

$$\tau(f(x)) = \tau\left(\prod_{\sigma \in H} (x - \sigma(\alpha))\right) = \prod_{\sigma \in H} (x - \tau(\sigma(\alpha))).$$

But this is just the left regular action by τ, so this simply permutes the linear factors $(x - \sigma(\alpha))$ amongst themselves, and hence leaves $f(x)$ invariant. That is, $\tau(f(x)) = f(x)$. So, H fixes coefficients of $f(x)$. But this means coefficients of f lie in L_H, and hence in K. Note also that $f(\alpha) = 0$ (because $x - \alpha$ is a factor). So, we have a polynomial f with coefficients in K and root α; we know such a polynomial must have $\deg f \geqslant [L : K]$ because $L = K(\alpha)$. But clearly $\deg f = |H|$, and because H is proper $|H| < |G| = [L : K]$, implying $\deg f < [L : K]$, a contradiction. So, our assumption that $L_H = K$ must be incorrect, and K cannot be the fixed field for a proper subgroup of G. □

We are now ready to prove the crown jewel of Galois Theory. Let L be normal over K, and $G = Gal(L/K)$. Define mappings

$$\left\{\begin{matrix}\text{fields F,} \\ K \subset F \subset L\end{matrix}\right\} \leftrightarrow \left\{\begin{matrix}\text{groups } H, \\ H \subset G\end{matrix}\right\}.$$

We have $F \mapsto Gal(L/F)$, i.e., a subfield of L maps to the Galois group of L over K; and $H \mapsto L_H$, i.e., a subgroup maps to its fixed field.

Theorem 1.9 (Fundamental Theorem of Galois Theory)**.** *The mappings above are inverses of each other; thus they provide a one-to-one correspondence between the two sets. Moreover if $F \leftrightarrow H$ under this correspondence then F is normal over K iff H is a normal subgroup of G. In this case there is an isomorphism*

$$G/H \to \text{Gal}(F/K)$$

obtained by restricting automorphisms to F.

Proof. We begin by showing the mappings are inverses of each other. Take a field F. It has Galois group $\text{Gal}(L/F)$. We want to show $\text{Gal}(L/F)$ maps to F, i.e., the fixed field of $\text{Gal}(L/F)$ is F. Note first that L is normal over F by Corollary 1.6. But then by Problem 1.2 we know that F is the fixed field of $\text{Gal}(L/F)$ as desired.
Next, take a subgroup H. It has fixed field L_H. We want to show L_H maps to H, i.e., the Galois group of L_H, $\text{Gal}(L/L_H)$, is H. First, notice that $H \subset \text{Gal}(L/L_H)$: any element of H must trivially fix L_H, because L_H is defined to be those elements of L fixed by all members of H. By

Corollary 1.6, L is normal over L_H, and then by Problem 1.2, L_H is not the fixed field of any proper subgroup of $\text{Gal}(L/L_H)$. But since L_H is the fixed field of H and $H \subset \text{Gal}(L/L_H)$, we must have $H = \text{Gal}(L/L_H)$.
We have hence demonstrated a one-to-one correspondence between fields F and subgroups H, as desired.

Now for the normality assertion. Let $F \leftrightarrow H$. We claim $\sigma F \leftrightarrow \sigma H \sigma^{-1}$ for any $\sigma \in G$: first, $(\sigma H \sigma^{-1})\sigma F = \sigma(HF) = \sigma F$ shows $\sigma H \sigma^{-1} \subset \text{Gal}(L/\sigma F)$, and further $\tau(\sigma F) = \sigma F \implies (\sigma^{-1}\tau\sigma)F = F \implies \sigma^{-1}\tau\sigma \in H \implies \tau \in \sigma H \sigma^{-1} \implies \text{Gal}(L/\sigma F) \subset \sigma H \sigma^{-1}$; hence $\text{Gal}(L/\sigma F) = \sigma H \sigma^{-1}$, or equivalently $\sigma F \leftrightarrow \sigma H \sigma^{-1}$, as claimed.
Now, F is normal over K iff $\sigma F = F$ for each embedding of F fixing K pointwise. Each such embedding can be extended to an embedding of L to get members of G, which then allows us to write F is normal over K iff $\sigma F = F, \forall \sigma \in G$. But since $F \leftrightarrow H$ and $\sigma F \leftrightarrow \sigma H \sigma^{-1}$, this happens iff $\sigma H \sigma^{-1} = H, \sigma \in G$, which by definition means H is normal in G.

Finally, in the normal case, we have a homomorphism $G \to \text{Gal}(F/K)$, where $\sigma \mapsto \sigma_F$, i.e. σ maps to its the restriction over F, σ_F. We know σ_F is an automorphism of G because it is an embedding of F fixing K, and F is normal over K. Further, this homomorphism is surjective because any element of $\text{Gal}(F/K)$ can be extended to an automorphism of L fixing K. Now, the kernel consists of all σ s.t. $\sigma F = F$, which is of course $H = \text{Gal}(L/F)$. So, by the first isomorphism theorem, we get an isomorphism

$$G/H \cong \text{Gal}(F/K),$$

finishing this lovely proof. □

We have now armed ourselves with enough tools from Galois Theory to apply them to the concerns of Algebraic Number Theory.

2. Galois Theory Applied to Prime Decomposition

We will apply Galois theory to the general problem of determining how a prime ideal of a number ring splits in an extension field. Some results will have to be taken for granted: we have proven them in completion in class, but for purposes of brevity we avoid reproving them in this paper, but instead provide a complete citation to the full results and proof.

Throughout what follows, we will assume K and L are number fields, and assume that L is a normal extension of K. Thus by Problem 1.1, the Galois group G, consisting of all automorphisms of L which fix K pointwise, has order $n = [L : K]$. As usual we let R and S denote the corresponding number rings. Next, fix a prime P of R, and consider all primes Q of S lying over P. The following diagram summarizes our notation:

$$\begin{array}{ccccc} L & \supset & S & \supset & Q \\ | & & | & & | \\ K & \supset & R & \supset & P \\ | & & | & & | \\ \mathbb{Q} & \supset & \mathbb{Z} & \supset & p \end{array}$$

It is a fact that in our case of L being normal over K, that all primes Q lying over P will have the same ramification index e and inertial degree f (corollary to Theorem 23 in [1]). Further, we also know that in general if there are r primes Q lying over P, then $\sum_{i=1}^{r} e_i f_i = [L : K]$ (Theorem 21 in [1]). It now follows that in our normality case this equality reduces to $ref = n$. Now, for each prime Q lying over P, we define two subgroups of G.

Definition 2.1 (Decomposition group)**.** The subgroup of G consisting of all automorphisms fixing Q as a set:

$$D = D(Q \mid P) = \{\sigma \in G : \sigma Q = Q\}.$$

Definition 2.2 (Inertia group)**.** The subgroup of G consisting of all automorphisms which leave congruence modulo Q invariant:

$$E = E(Q \mid P) = \{\sigma \in G : \sigma(\alpha) \equiv \alpha \mod Q \ \forall \alpha \in S\}.$$

Problem 2.3. *Show that $D = D(Q \mid P)$ and $E = E(Q \mid P)$ are both in fact subgroups, and further $E \subset D$.*

Proof. First note that both D, E are non-empty because the identity automorphism belongs to both. Next, if $\sigma, \tau \in D$, note $\tau Q = Q \iff Q = \tau^{-1}Q$ so that $(\sigma\tau^{-1})(D) = \sigma(\tau^{-1}(D)) = \sigma(D) = D$, which shows D is a subgroup. Similarly, $\tau(\alpha) \equiv \alpha \mod Q \iff \alpha \equiv \tau^{-1}(\alpha) \mod Q$ is easily used to show $(\sigma\tau^{-1})(\alpha) \equiv \alpha \mod Q$, which shows E is a subgroup.
Finally, let $\sigma \in E$. We will show $\sigma Q = Q$: for $\sigma(q) \in \sigma Q$, we have $\sigma(q) \equiv q \equiv 0 \mod Q \implies \sigma(q) \in Q$, which means $\sigma Q \subset Q$; similarly we can show $\sigma^{-1}Q \subset Q$, which implies $Q \subset \sigma Q$. By double containment $\sigma Q = Q$. □

We now spend some time laying the groundwork for the main result of this section.

Note now that D is almost designed to induce automorphisms of the field S/Q in a very natural way: For any $\sigma \in G$, we take its restriction as an automorphism of S, and if $\sigma \in D$ then consider the induced mapping $S \to S/Q$: this will have kernel $\sigma^{-1}Q$, which is of course Q because $\sigma \in D$. But then by the first isomorphism theorem, we obtain an automorphism $\overline{\sigma}$ of S/Q, in such a way that the following diagram commutes:

$$\begin{tikzcd} S \arrow[r, "\sigma"] \arrow[d] & S \arrow[d] \\ S/Q \arrow[r, "\overline{\sigma}"] & S/Q \end{tikzcd}$$

But note also that $\overline{\sigma}$ must fix R/P pointwise, since σ was chosen to be in G and σ fixes K pointwise. In our new Galois theoretic language, this simply means $\overline{\sigma} \in \overline{G} = \mathrm{Gal}((S/Q)/(R/P))$. We can now reformulate all of this in terms of the existence of a homomorphism from $\Theta : D \to \overline{G}$, where $\sigma \mapsto \overline{\sigma}$ (easy to check this is in fact a homomorphism: composition of automorphisms in D corresponds to composition in $\overline{G}$). Let's determine $\ker\Theta = \{\sigma \in D : \overline{\sigma} \text{ is identity on } S/Q\}$. This is true iff $\alpha + Q = \overline{\sigma}(\alpha + Q) = \sigma(\alpha) + Q$, for all $\alpha \in S$. But this means $\sigma(\alpha) \equiv \alpha \mod Q$, for all $\alpha \in S$, which is exactly the condition for $\sigma \in E$. So, $\ker\Theta = E$. Kernels are normal subgroups, so in fact $E \trianglelefteq D$, and by the first isomorphism theorem D/E is embedded in $\overline{G}$.

Now we consider the fixed fields of D and E; denote them as L_D and L_E, respectively. L_D is called the decomposition field and L_E the inertia field. In general, we adopt the following system of notation: For any subgroup H of G, L_H denotes the fixed field of H; thus $L_{\{1\}} = L$ and $L_G = K$. We extend this notation so that for any subset $X \subset L$, X_H will be $X \cap L_H$. We now claim S_H is the number ring in L_H: consider $\mathbb{A} \cap L_H = \mathbb{A} \cap (L \cap L_H) = (\mathbb{A} \cap L) \cap L_H = S \cap L_H = S_H$. Further, Q_H is the unique prime of S_H lying under Q: the fact that $Q_H = Q \cap L_H$ is an ideal of S_H follows easily from the fact that Q is a prime in S, further the fact that Q lies over Q_H follows directly from the definition of Q_H, and we know this must be unique. Since $Q_H = Q \cap L_H$, and $P \subset Q, P \subset L_H$, we see that Q_H lies over P. It should now be clear that S_H/Q_H is an intermediate field between S/Q and R/P.

Finally, we have a beautiful result which explicates some of the reason behind defining all these new structures and algebraic objects. In particular, it shows some of the underlying structure hidden behind the seemingly uninteresting statement that L is a normal extension of K with degree $n = ref$.

Theorem 2.4. *Let $K, L, R, S, P, Q, G, D, E, r, e$ and f be as above. Then we have the following:*

$$\begin{tikzcd}
\text{DEGREES} & L \arrow[d, dash, "e"'] & Q \arrow[d, dash] & \text{RAMIFICATION INDICES} & \text{INERTIAL DEGREES} \\
 & L_E \arrow[d, dash, "f"'] & Q_E \arrow[d, dash] & e & 1 \\
 & L_D \arrow[d, dash, "r"'] & Q_D \arrow[d, dash] & 1 & f \\
 & K & P & 1 & 1
\end{tikzcd}$$

Proof.

(1) We show $[L_D : K] = r$.

It follows from definitions that $\mathrm{Gal}(L/L_D) = D$. Now, as previously discussed L is normal over L_D, and this means $[L : L_D] = |D|$, which further implies $\dfrac{[L:K]}{[L:L_D]} = \dfrac{[L:K]}{|D|} = \dfrac{|G|}{|D|} \implies [L_D : K] = [G : D]$, i.e. $[L_D : K]$ is the same as the index of D in G. Now, a given left coset σD sends Q to σQ (i.e., each member of the coset does this). Next, note that $\sigma D = \tau D \iff \tau^{-1}\sigma \in D \iff (\tau^{-1}\sigma)Q = Q \iff \sigma Q = \tau Q$. This gives us a bijection between all left cosets σD and the set $\{\sigma Q : \sigma \in G\}$. But we have shown earlier in this course that elements of G permute all primes Q lying over P transitively (Theorem 23 in [1]), which means $\{\sigma Q : \sigma \in G\}$ is actually the set of all primes Q lying over P, but we said there are r such primes, and this now means there r left cosets of D. So, $[L_D : K] = r$.

(2) Next we show $e(Q_D|P) = 1$ and $f(Q_D|P) = 1$.

First, we claim Q is the only prime of S lying over Q_D. Recall again, that such primes are permuted transitively by elements of $\mathrm{Gal}(L/L_D) = D$. But $\sigma Q = Q$ for all $\sigma \in D$, so $\mathbb{Q}$ is indeed the only such prime.

We also know that the products $e_i f_i$ sum to the degree of the field extension (Theorem 21 of [1]). Since there is only one such prime (namely Q), we have the equality

$$[L : L_D] = e(Q|Q_D)f(Q|Q_D).$$

Note that $[L_D : K] = r$ and $[L : K] = ref$ imply that $[L : L_d] = ef$. Further, since e, f are also multiplicative in towers, we know that $e(Q|Q_D) \leqslant e$ and $f(Q|Q_D) \leqslant f$. But then for the equality to hold we need $e(Q|Q_D) = e$ and $f(Q|Q_D) = f$. Again because e and f are multiplicative in towers this allows us to conclude

$$e(Q_D|P) = f(Q_D|P) = 1,$$

as desired.

(3) Now we prove $f(Q, Q_E) = 1$. Notice that since f is multiplicative in towers and $f(Q|P) = f$, this will automatically imply that $f(Q_E|Q_D) = f$.

This is equivalent to showing S/Q is the trivial extension of S_E/Q_E. Since these are finite fields,

it is in fact enough to prove that the Galois group of S/Q over S_E/Q_E is trivial. There is a nice technique to showing this, and borrows a construction from the proof of Problem 1.2. Given any $\theta \in S/Q$, we demonstrate that the polynomial $(x-\theta)^m$ has coefficients in S_E/Q_E for some $m \geqslant 1$; it follows that any automorphism in the Galois group maps θ to another root of $(x-\theta)^m$, but since θ is the only root this means $\theta \mapsto \theta$. This shows any automorphism in the Galois group is actually the identity map, which means the group is trivial, as desired.
Now, given $\theta \in S/Q$, fix $\alpha \in S$ such that $\alpha + Q = \theta \in S/Q$. Construct the polynomial

$$g(x) = \sum_{\sigma \in E} \Big(x - \sigma(\alpha)\Big).$$

Consider $\tau \in \mathrm{Gal}(L/L_E) = E$, and observe that $\tau(g(x)) = g(x)$ since τ will simply permute the roots of g amongst themselves. This means the coefficients of g are fixed by any $\tau \in \mathrm{Gal}(L/L_E) = E$, so the coefficients are in L_E; but they are also in S because all the $\sigma(\alpha)$s must be in S, and hence the coefficients are in S_E. We can now reduce coefficients modulo Q to find $\overline{g} \in (S/Q)[x]$ actually has coefficients in S_E/Q_E. Note however that since $\sigma \in E$, $\sigma(\alpha) \equiv \alpha \mod Q$, so all the $\sigma(\alpha)$ reduce to θ. Hence $\overline{g}(x) = (x-\theta)^m$, where $m = |E|$. We have found the type of polynomial we wanted, and this finishes this step of the proof.

(4) Now, because $f(Q_E|Q_D) = f$, and the sum of $e_i f_i$ should give the degree $[L_E : L_D]$, we see that $[L_E : L_D] \geqslant f$. But recall also that D/E is embedded in $\overline{G} = \mathrm{Gal}((S/Q)/(R/P))$, and since the latter group has order f, we can write $[L_E : L_D] = |D/E| \leqslant |\overline{G}| = f$. Hence, $[L_E : L_D] = f$. But this also means $e(Q_E|Q_D) = 1$ because of $[L_E : L_D] = e(Q_E|Q_D)f(Q_E|Q_D)$.

(5) $[L : L_E] = e$ and $e(Q|Q_E) = e$ are now easily obtained by using multiplicativity in towers of degree and ramification index. □

References

[1] Daniel A. Marcus. *Number Fields, 2nd edition.* Springer International Publishing, 2018.

[2] J. A. Gallian. *Contemporary Abstract Algebra, 9th edition.* Cengage Learning, Boston MA, 2016.

[3] Michael Artin. *Algebra, 2nd edition.* Pearson Prentice Hall, 2011.