The notes below are for the students who attended the consultation session in Galois Theory run by Damian Rössler on W3 Thu 2-4pm in C5 (2019). They are not an extract of the model solution of the 2018 exam in Galois Theory.

Notes on the 2018 exam in B3.1 Galois Theory.

Q1 (e)

Recall that in (d) it was shown that F is Galois over K. Recall also that by assumption (in (d)) L_1 and L_2 are Galois over K. Under the further assumption that $L_1 \cap L_2 = K$, we have to show that there is a bijective homomorphism of groups

$$\phi : G \to \Gamma(L_1 : K) \times \Gamma(L_2 : K).$$

As explained during the session, we define ϕ by the formula $\phi(\gamma) = \gamma|_{L_1} \times \gamma|_{L_2}$. The kernel of ϕ is by construction $\Gamma(F : L_1) \cap \Gamma(F : L_2)$. By the Galois correspondence, the group $\Gamma(F : L_1) \cap \Gamma(F : L_2)$ corresponds to the smallest field containing L_1 and L_2, which is F by assumption. Hence $\Gamma(F : L_1) \cap \Gamma(F : L_2) = \{\mathrm{Id}_F\}$, which shows that ϕ is injective. Alternatively, one may consider that $F = L_1 L_2$ consists of products of elements of L_1 and L_2 (prove this - if you don't see why, ask me in the next consultation sessions) and therefore any element in the kernel of ϕ must fix all of $L_1 L_2$ and therefore be equal to $\{\mathrm{Id}_F\}$.

We now turn to the surjectivity of ϕ. Note that by the Galois correspondence the group generated by $\Gamma(F : L_1)$ and $\Gamma(F : L_2)$ corresponds to the biggest field contained in L_1 and L_2, ie $L_1 \cap L_2$. Now $L_1 \cap L_2 = K$ by assumption and the group corresponding to K is $\Gamma(F : K)$ so the group generated by $\Gamma(F : L_1)$ and $\Gamma(F : L_2)$ is $\Gamma(F : K)$.

Lemma 0.1 (suggested by a student). *Every element of the group generated by* $\Gamma(F : L_1)$ *and* $\Gamma(F : L_2)$ *is of the form* $\gamma_1 \cdot \gamma_2$*, where* $\gamma_1 \in \Gamma(F : L_1)$ *and* $\gamma_2 \in \Gamma(F : L_2)$.

Proof. It is sufficient to show that the set

$$H := \{\gamma_1 \cdot \gamma_2 \,|\, \gamma_1 \in \Gamma(F : L_1),\ \gamma_2 \in \Gamma(F : L_2)\}$$

is a subgroup. For any $\gamma \in \Gamma(F : K)$, denote by

$$\lambda_\gamma : \Gamma(F : K) \to \Gamma(F : K)$$

the group homomorphism st $\lambda_\gamma(\alpha) = \gamma^{-1} \cdot \alpha \cdot \gamma$ (ie λ_γ is "conjugation by γ"). Remember that

$$\lambda_\gamma(\Gamma(F : L_1)) \subseteq \Gamma(F : L_1)$$

and

$$\lambda_\gamma(\Gamma(F:L_2)) \subseteq \Gamma(F:L_2)$$

for all $\gamma \in \Gamma(F:K)$. This follows from the fact the the subgroups $\Gamma(F:L_1)$ and $\Gamma(F:L_2)$ are normal in $\Gamma(F:K)$ (recall that the extensions $L_1|K$ and $L_2|K$ are Galois). This implies in particular that $\lambda_\gamma(H) \subseteq H$ for all $\gamma \in \Gamma(F:K)$.

Note finally that we have $\lambda_\gamma \circ \lambda_{\gamma^{-1}} = \mathrm{Id}_{\Gamma(F:K)}$ for all $\gamma \in \Gamma(F:K)$.

Since $\mathrm{Id}_F \in H$, we now only have to show that if $\gamma_1, \gamma_1' \in \Gamma(F:L_1)$ and $\gamma_2, \gamma_2' \in \Gamma(F:L_2)$ then

$$(\gamma_1 \cdot \gamma_2)^{-1} \in H \quad (*)$$

and

$$\gamma_1 \cdot \gamma_2 \cdot \gamma_1' \cdot \gamma_2' \in H \quad (**)$$

We compute

$$(\gamma_1 \cdot \gamma_2)^{-1} = \lambda_{\gamma_2} \circ \lambda_{\gamma_2^{-1}}((\gamma_1 \cdot \gamma_2)^{-1}) = \lambda_{\gamma_2} \circ \lambda_{\gamma_2^{-1}}(\gamma_2^{-1} \cdot \gamma_1^{-1}) = \lambda_{\gamma_2}(\gamma_1^{-1}\gamma_2^{-1})$$

which lies in H. So $(*)$ is proven.

For $(**)$, compute

$$\gamma_1 \cdot \gamma_2 \cdot \gamma_1' \cdot \gamma_2' = \lambda_{\gamma_2^{-1}} \circ \lambda_{\gamma_2}(\gamma_1 \cdot \gamma_2 \cdot \gamma_1' \cdot \gamma_2') = \lambda_{\gamma_2^{-1}}(\lambda_{\gamma_2}(\gamma_1) \cdot \gamma_1' \cdot \gamma_2' \cdot \gamma_2)$$

which also lies in H, since $\lambda_{\gamma_2}(\gamma_1) \in \Gamma(F:L_1)$ by assumption. So the lemma is proven. □

We can now complete the proof of the surjectivity of ϕ. Let $n := \#\Gamma(F:K)$. From the lemma and the fact that $\Gamma(F:L_1)$ and $\Gamma(F:L_2)$ generate $\Gamma(F:K)$, we see that

$$n \leq \#\Gamma(F:L_1) \cdot \#\Gamma(F:L_2).$$

We know from the fundamental theorem of Galois theory that

$$\#\Gamma(L_1:K) = n/\#\Gamma(F:L_1) \text{ and } \#\Gamma(L_2:K) = n/\#\Gamma(F:L_2).$$

So the injectivity of ϕ implies that

$$n \leq (n/\#\Gamma(F:L_1)) \cdot (n/\#\Gamma(F:L_2))$$

or equivalently

$$n \geq \#\Gamma(F:L_1) \cdot \#\Gamma(F:L_2).$$

Combining the inequalities we see that

$$n = \#\Gamma(F:L_1) \cdot \#\Gamma(F:L_2).$$

In particular,

$$n = (n/\#\Gamma(F : L_1)) \cdot (n/\#\Gamma(F : L_2)) = \#\Gamma(L_1 : K) \cdot \#\Gamma(L_2 : K).$$

Thus the source and target of the map ϕ has the same number of elements. Since ϕ is injective, this implies that ϕ is a bijection.

Q3 (iii) Let $G := \mathrm{Aut}_F(F')$. According to the theorem in section 5.2 of the notes, we have $[F' : (F')^G] = \#G$. By assumption we have $\#G = [F' : F]$ so that we have $[F' : (F')^G] = [F' : F]$. Since $F \subseteq (F')^G$ by assumption, the tower law implies that $(F')^G = F$, ie $F = (F')^{\mathrm{Aut}_F(F')}$. This means that $F'|F$ is a Galois extension in the sense of the definition in section 5.1.

(iv) This was proven in the lectures, as a consequence of Artin's lemma. Here is a way to derive this from the lecture notes. According to the theorem in section 5.1, the extension $L|L^G$ is finite. It is also separable, because L has characteristic 0 by assumption (see theorem in section 4.3). Hence by the theorem in section 5.3, we only have to show that the extension $L|L^G$ is normal. Let $\alpha \in L$ and let $P(x) \in L^G[x]$ be the minimal polynomial of α. We have

$$Q(x) = \prod_{\beta \in \text{orbit of } \alpha \text{ under } \mathrm{Aut}_{L^G}(L)} (x - \beta) \mid P(x)$$

since $P(\sigma(\alpha)) = \sigma(P(\alpha)) = 0$ for all $\sigma \in \mathrm{Aut}_{L^G}(L)$. Furthermore, the coefficients of $Q(x)$ are symmetric functions in the roots of $Q(x)$ and are thus invariant under $\mathrm{Aut}_{L^G}(L)$, ie they lie in L^G. In other words, $Q(x) \in L^G[x]$. Since $P(x)$ is irreducible, we thus see that $Q(x) = P(x)$. Hence $P(x)$ splits in L. This shows that $L|L^G$ is normal and completes the proof.

The hint about the primitive element theorem can be exploited as follows. According to the theorem in section 4.2, the extension $L|L^G$ is normal and finite iff L is the splitting field of a polynomial in L^G. By the primitive element theorem and the fact that $L|L^G$ is finite and separable, there is an $\alpha \in L$ such that $L = L^G(\alpha)$. According to the preceding paragraph, the minimal polynomial $P(x)$ of α splits in L and hence L is a splitting field of $P(x)$. In particular, L is a normal extension of L^G.

The last part of (iv) follows from the first part and the fact that any finite group is a subgroup of some S_n (Cayley's theorem).