M3/4/5P11 Galois theory, Progress test 2, 12/13/2018, solutions.

Q1.(i) $K \subset L_1 \cap L_2$ is separable. We proved in class that $K \subset L$ is separable if and only if for all $a \in L$, a is separable over K. Pick any $a \in L_1 \cap L_2$. Because $a \in L_1$, a is separable over K.

(ii) $K \subset L_1 \cdot L_2$ is separable. We proved in class that if $a \in F$ is separable over K, then $K \subset K(a)$ is a separable extension. More generally, I **claim**: If $a_1, \ldots, a_m$ are separable over K, then $K \subset K(a_1, \ldots, a_m)$ is a separable extension. Indeed, by induction on m, $K \subset K_1 = K(a_1, \cdots, a_{m-1})$ is a separable extension. Since a_m is separable over K, it is also separable over K_1 (the minimal polynomial of a_m over K_1 is a factor of the minimal polynomial of a_m over K), it follows that $K_1 \subset K_1(a_m)$ is a separable extension. Since $K \subset K_1$ is separable and $K_1 \subset K_1(a_m)$ is separable, then also $K \subset K_1(a_m) = K(a_1, \ldots, a_m)$ is separable. This concludes the proof of the claim.

Now $K \subset L_1$ is finite and separable, hence for some $a_1, \ldots, a_m \in L_1$, $L_1 = K(a_1, \cdots, a_m)$. Necessarily all a_i are separable over K. Similarly, $L_2 = K(b_1, \ldots, b_r)$ and again all b_j are separable over K. By the claim, $K \subset K(a_1, \ldots, a_m, b_1, \ldots, b_r) = L_1 \cdot L_2$ is a separable extension.

Q2. (a) $\mathbb{F}_q$ is a finite dimensional vector space over $\mathbb{F}_p$ hence (by choosing a basis) $\mathbb{F}_q \cong \mathbb{F}_p^d$ as vector spaces, where $d = \dim_{\mathbb{F}_p}(\mathbb{F}_q) = [\mathbb{F}_q : \mathbb{F}_p]$. By counting elements $d = m$.

(b) The extension is separable because, as we proved in class, all finite fields are perfect. The extension is normal because, as we showed in class, $\mathbb{F}_p \subset \mathbb{F}_q$ is the splitting field of the polynomial $X^q - x$.

(c) We essentially did this in class but let me spell it out again. F is a field automorphism: It is clear that $F(0) = 0$, $F(1) = 1$ and for all $a, b \in \mathbb{F}_q$, $F(ab) = F(a)F(b)$. Now in any field K of characteristic p we have that for all $a, b \in K$:

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = a^p + b^p$$

because for all $1 \leq k \leq p-1$, p divides $\binom{p}{k}$ (elementary fact). Hence F is a field automorphism.

Finally F fixes $\mathbb{F}_p$ since for all $a \in \mathbb{F}_p$, $a^p = a$ (in `M1F` this is called "Fermat's little theorem" but it follows immediately from the fact that the multiplicative group $\mathbb{F}_p^\times$ has $p-1$ elements). That is $F \in \mathrm{Emb}_{\mathbb{F}_p}(\mathbb{F}_q, \mathbb{F}_q)$.

(d) We have just shown that $F \in G$. I claim that the order of F in G is m, that is, F generates a cyclic subgroup of order m in G. Note that if I show the claim I am done, because we know from Galois theory that $|G| = [\mathbb{F}_q : \mathbb{F}_p] = m$ hence and hence then $\langle F \rangle = G$ is a cyclic group of order m. Indeed we observed in class that for all $a \in \mathbb{F}_q$, $F^m(a) = a^q = a$, so indeed $F^m = 0$. Assume for a contradiction that the order of F is strictly smaller then m, that is, there exists a positive integer $k < m$ such that $F^k = e$ in G. But then for all $a \in \mathbb{F}_q$, a is a root of the polynomial $x^r - x$ where $r = p^k < q$, hence this polynomial of degree r has $q > r$ roots, which is absurd.

(e) By Galois theory, fields correspond to subgroups of $G = C_{12}$, that is, to divisors of 12. Now 12 has 6 divisors (they are $1, 2, 3, 4, 6, 12$) hence there are 6 intermediate fields.[1]

[1] some may only count proper divisors and state that there are 4 intermediate fields. Those people will get full marks for the question.