NAP 2019, MODULE-III, SOLUTIONS OF EXERCISE SET 2

SHIV PRAKASH PATEL & SHREEDEVI MASUTI

* Here the references referes to the Garling's book on Galois theory.

(1) Exercise 9.2 from the book.
Solution: Let $L : K$ be algebraic. Set

$$M := K(\alpha \in L : \text{the minimal polynomial of } \alpha \text{ over } K \text{ splits in } L).$$

We claim that M is the greatest intermediate field of L for which $M : K$ is normal. Let $\alpha \in M$ and m be the minimal polynomial of α over K. Let H be a splitting field of m and $\beta \in H$ be another root of m. As m splits in L, $\beta \in L$. Since the minimal polynomial of β is m itself and m splits in L, $\beta \in M$. Thus $M : K$ is normal.

Now suppose let M' be an intermediate field such that $M' : K$ is normal. Then for any $\alpha \in M'$ the minimal polynomial of α over K splits in M' and hence in L. Therefore $\alpha \in M$. Hence M is the greatest intermediate field of L for which $M : K$ is normal.

(2) Exercise 9.3 from the book.
Solution: First we prove that $K(M_1, M_2) : K$ is normal. By Theorem 9.1 $M_1 : K$ (resp. $M_2 : K$) is a splitting field extension for some $S_1 \subseteq K[X]$ (resp. $S_2 \subseteq K[X]$). Define $S := \{fg : f \in S_1, g \in S_2\}$ and let $M \subseteq L$ be the splitting field extension of S over K. (Since for every $f \in S_1$ (resp. $g \in S_2$), f splits in M_1 (resp. M_2), fg splits in L. Hence there exits a splitting field $M \subseteq L$ of S). We claim that $M = K(M_1, M_2)$. Since for every $f \in S_1$ the polynomial f splits in M, $M_1 \subseteq M$. Similarly, $M_2 \subseteq M$. Hence $K(M_1, M_2) \subseteq M$. Moreover, if $M' \subseteq L$ is any other intermediate field containing M_1 and M_2, then for every $f \in S_1$, $g \in S_2$, fg splits in M'. Hence $M \subseteq M'$. Thus M is the smallest field containing M_1 and M_2 which implies that $M = K(M_1, M_2)$.

Now we prove that $M_1 \cap M_2 : K$ is normal. Clearly, $M_1 \cap M_2 : K$ is algebraic. Let $\alpha \in M_1 \cap M_2$ and m be the minimal polynomial of α over K. As $M_1 : K$ and $M_2 : K$ are normal, m splits over M_1 and M_2. Hence all the roots of m are in $M_1 \cap M_2$ and thus $M_1 \cap M_2 : K$ is normal.

(3) Prove Exercise 9.4 of the book in the case $L : K$ is finite.
Solution: Let $L : K$ be finite and $N : L$ be a normal closure of $L : K$. First we prove that $N : K$ is finite. Let $L = K(\alpha_1, \ldots, \alpha_n)$ and m_{α_i} be the minimal polynomial of α_i over K. Set $g = m_{\alpha_1} \ldots m_{\alpha_n}$. Let M be the splitting field of g over K. Then $M : K$ is a finite normal extension. Consider a monomorphism $i : L \longrightarrow N$ defined as $i(l) = l$ for $l \in L$. Then $i(g) = g$. Since $N : K$ is normal, each m_{α_i} splits over N and so does g splits over N. Therefore by Theorem 7.5 i can be extended to a monomorphism $\sigma : M \longrightarrow N$. As $M : K$ is normal, $\sigma(M) : K$ is a normal extension. Since $N : L$ is the normal closure of $L : K$, $\sigma(M) = N$ and hence in particular, $N : K$ is a splitting field extension of $\sigma(g) = g$.

Now, let N' be another normal closure of $L : K$. Consider a monomorphism $i' : L \longrightarrow N'$ defined as $i'(l) = l$ for $l \in L$. Then $i'(g) = g$. Since $N' : K$ is normal, each m_{α_i} splits over N' and so does g splits over N'. Therefore i' can be extended to a monomorphism $j : N \longrightarrow N'$. Then $j(N) : K$ is a normal extension. As $N' : L$ is a normal closure of $L : K$, $j(N) = N'$ and hence j is an isomorphism onto N'.

(4) Let $K \subseteq M \subseteq L$ be an extension of fields such that $M : K$ and $L : M$ is normal. Is $L : K$ normal ? If so, prove this or else give a counter-example.
Solution: No, $L : K$ need not be normal. Let $L = \mathbb{Q}(\sqrt[4]{2}),\ M = \mathbb{Q}(\sqrt{2})$ and $K = \mathbb{Q}$. Then $L : M$ and $M : K$ are quadratic extensions and hence are normal. But $L : K$ is not normal because the minimal polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}$ is $X^4 - 2$ which doesn't split in L.

(5) Find the normal closure for the following field extensions: (a) $\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}$ where p is a prime; (b) $\mathbb{Z}_3(\alpha) : \mathbb{Z}_3$ where $\alpha^3 - \alpha + 1 = 0$
Solution: (a) Note that the minimal polynomial of $\alpha := \sqrt[p]{2}$ over $\mathbb{Q}$ is $X^p - 2$. Let $\omega \in \mathbb{C}$ be the p-th root of unity. Then $\alpha, \omega\alpha, \omega^2\alpha, \ldots, \omega^{p-1}\alpha$ are all the distinct roots of $X^p - 2$. Hence we need to add ω in the normal closure of $\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}$. We prove that in fact $\mathbb{Q}(\sqrt[p]{2}, \omega) : \mathbb{Q}(\sqrt[p]{2})$ is the normal closure of $\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}$. Since $\mathbb{Q}(\sqrt[p]{2}, \omega) : \mathbb{Q}$ is the splitting field of $X^p - 2$, $\mathbb{Q}(\sqrt[p]{2}, \omega) : \mathbb{Q}$ is a normal extension.

Now suppose $\mathbb{Q}(\sqrt[p]{2}) \subseteq M \subseteq \mathbb{Q}(\sqrt[p]{2}, \omega)$ is a tower and $M : \mathbb{Q}$ is normal. Then since $X^p - 2$ is irreducible over $\mathbb{Q}$ it splits over M and hence $\sqrt[p]{2},\ \omega \in M$. Thus $M = \mathbb{Q}(\sqrt[p]{2}, \omega)$.

(b) We prove that $\mathbb{Z}_3(\alpha) : \mathbb{Z}_3$ is normal and hence its normal closure is itself. Since $X^3 - X + 1$ has no roots over $\mathbb{Z}_3$, it is irreducible over $\mathbb{Z}_3$. Moreover, if α is a root of $X^3 - X + 1$, then $\alpha + 1$ and $\alpha + 2$ are also the roots of $X^3 - X + 1$. Hence $\mathbb{Z}_3(\alpha) : \mathbb{Z}_3$ is a splitting field extension of $X^3 - X + 1$ and thus $\mathbb{Z}_3(\alpha) : \mathbb{Z}_3$ is normal.

(6) Let $L : K$ be a finite normal extension. Prove that the number of automorphisms of L which fixes K is at most $[L : K]$.
Solution: Let $L = K(\alpha_1, \ldots, \alpha_n)$ and m_{α_i} be the minimal polynomial of α_i over K of degree d_i. Consider a tower of fields

$$K \subseteq K(\alpha_1) \subseteq \cdots \subseteq K(\alpha_1, \ldots \alpha_i) \subseteq \cdots \subseteq K(\alpha_1, \ldots, \alpha_n).$$

Then by Corollary 2 of Theorem 7.4 (Section 7.2) the number of monomorphisms $j : K(\alpha_1) \longrightarrow L$ which extends a monomorphism $i : K \longrightarrow L$ defined as $i(k) = k$ is equal to the number of distinct roots of m_{α_1} in L which is at most $[K(\alpha_1) : K]$. Using similar argument it follows that for each monomorphism $j : K(\alpha_1) \longrightarrow L$ there are at most $[K(\alpha_1, \alpha_2) : K(\alpha_1)]$ monomorphisms from $K(\alpha_1, \alpha_2)$ to L which extend j. Thus there are at most $[K(\alpha_1, \alpha_2) : K]$ monomorphisms from $K(\alpha_1, \alpha_2)$ to L which fixes K. Continuing this we get that there are at most $[L : K]$ automorphisms of L which fixes K.

(7) Let $L : K$ be algebraic. Suppose that $\alpha, \beta \in L$ are separable over K. Prove that $\alpha + \beta$ and $\alpha\beta$ are separable over K.
Solution: Let $M := K(\alpha, \beta)$. Since α, β are algebraic over K, $M : K$ is a finite extension. As α, β are separable over K, by Corollary 2 of Theorem 10.3 (Section 10.2), $M : K$ is separable. Since $\alpha + \beta,\ \alpha.\beta \in M$, they are separable over K.

(8) Exercise 10.1 from the book.
Solution: Suppose that $L : K$ is separable. Let $j : K \longrightarrow L'$ be a monomorphism defined as $j(k) = k$ for $k \in K$. Since $L : K$ is separable and $j(m_\alpha) = m_\alpha$ splits in L' (as $L' : K$ is normal), by Theorem 10.3 there are exactly $[L : K]$ monomorphisms from L to L'.

Conversely, if $L : K$ is not separable then there are fewer than $[L : K]$ monomorphisms which fix K by Theorem 10.3

Thus the result follows.

(9) Find the number of automorphisms of $\mathbb{Q}(\sqrt[3]{2}, \omega)$ which fixes $\mathbb{Q}$ where ω is a cube root of unity.
Solution: Since $\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}$ is Galois, by Theorem 10.4 the number of automorphisms of $\mathbb{Q}(\sqrt[3]{2}, \omega)$ which fixes $\mathbb{Q}$ is $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = 6$.

(10) Consider an extension $\mathbb{Z}_p(t^{1/p}) : \mathbb{Z}_p(t)$ where p is a prime and t an indeterminate over $\mathbb{Z}_p$. Prove that the number of automorphisms of $\mathbb{Z}_p(t^{1/p})$ which fixes $\mathbb{Z}_p(t)$ is less than p.
Solution: Notice that $\mathbb{Z}_p(t^{1/p}) : \mathbb{Z}_p(t)$ is not separable because the minimal polynomial of $t^{1/p}$ over $\mathbb{Z}_p(t)$ is $X^p - t = (X - t^{1/p})^p$ which is not separable. Hence by Theorem 10.4 the number of automorphisms of $\mathbb{Z}_p(t^{1/p})$ which fixes $\mathbb{Z}_p(t)$ is less than $[\mathbb{Z}_p(t^{1/p}) : \mathbb{Z}_p(t)] = p$.