PartII Galois Theory 2

zc231

1. Consider the map $f : F \to F$ by $f(x) = x^2 - x$. $f(0) = f(1) = 0$ so f is not injective and hence not surjective because F is finite. Therefore there exists $a \in F$ such that $f(x) \neq a$ for all $x \in F$. Thus $x^2 - x - a$ is irreducible.

2. L/K is finite and so algebraic and let $L = K(a_1, \ldots, a_n)$. Since $\bar{K}$ contains every algebraic element over K so it contains a subfield which is isomorphic to $K(a_i)$ for each i. Then take the smallest field which contains $K(a_i)$ for all i, which is K-isomorphic to L.

3. (Possibly an answer) Let $K = \mathbb{Q}$ if the characteristic is zero and $K = \mathbb{F}_p$ if the characteristic is $p > 0$. Let S be the set of subsets of K_1 which are algebraically independent over K. Then $(S, \subset)$ is a partially ordered set and for each chain $A_1 \subset A_2 \cdots$ the union $\cup A_n$ is an upper bound so we have an maximal element A in S by Zorn's Lemma. Let $K(A)$ be the field by adjoining the set of elements in A. Now for each element $x \in K_1$, x satisfies a polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ where $a_i \in K(A)$, because $\{x, A\}$ is algebraically dependent. Since K_1 is algebraically closed, so $K_1 = \bar{K(A)}$. Similarly we have a maximal algebraically independent subset B of K_2 and $K_2 = \bar{K(B)}$. Therefore K_1 is isomorphic to a subfield of K_2 if the cardinality of A is smaller than the cardinality of B and vice versa and the embedding from K_1 to K_2 can be constructed by matching up the elements in A with the elements in B (since A, B are both algebraically independent so this extends to a well-defined homomorphism).

4. Let K be a field of characteristic 2 and $t \in K$ which is not a square then $L = K(\alpha)$ where α is a root of $X^2 - t$, is normal but not separable.

5. Use Question 13 on sheet 1.

6. Let $K = \mathbb{Q}$, $F = \mathbb{Q}(\sqrt{2})$ and $L = \mathbb{Q}(\sqrt[4]{2})$.

7. $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ and the Galois group is S_3 generated by σ, τ where

$$\sigma(\sqrt[3]{2}) = \zeta_3\sqrt[3]{2}, \sigma(\zeta_3) = \zeta_3, \quad \tau(\sqrt[3]{2}) = \sqrt[3]{2}, \tau(\zeta_3) = \zeta_3^2$$

   and so the subgroup generated by τ is not normal.

8. The Galois group of $\mathrm{Gal}(L/F \cap M)$ is the composite group of $\mathrm{Gal}(L/F)$ and $\mathrm{Gal}(L/M)$, i.e. the smallest group containing $\mathrm{Gal}(L/F)$ and $\mathrm{Gal}(L/M)$. x is fixed by the composite group of $\mathrm{Gal}(L/F)$ and $\mathrm{Gal}(L/M)$ if and only if x is fixed by $\mathrm{Gal}(L/F)$ and $\mathrm{Gal}(L/M)$, if and only if x is in $F \cap M$ so indeed the fixed field is $L \cap M$.

For the second part, let $\sigma : F \to M$ be a K-isomorphism of fields. We extends σ to a K-automorphism of L. Since L/F is finite and separable, we can write $L = F(\alpha)$ for some $\alpha \in L$. Let f be the minimal polynomial of α over F, say

$$f = X^n + f_{n-1}X^{n-1} + \cdots + f_0, f_i \in F.$$

Define $\sigma(f)$ to be $X^n + \sigma(f_{n-1})X^{n-1} + \cdots + \sigma(f_0)$ and we claim that every root of $\sigma(f)$ is inside L.

Let g be the minimal polynomial of α over K. Then $f|g$ and $\sigma(f)|\sigma(g) = g$. Therefore, every root of $\sigma(f)$ is some root of g. But L/K is Galois so every root of g is contained in L. Now pick any root β of $\sigma(f)$. If $\sigma(f)$ is reducible, so is $f = \sigma^{-1}\sigma(f)$, which is a contradiction. So $\sigma(f)$ is the minimal polynomial of β over M. Therefore, sending α to β gives an automorphism τ of L which sends F to M. Explicitly, if $\{1, \alpha, \ldots, \alpha^n\}$ where $n = [L : F]$ is an F-basis for L and $\{1, \beta, \ldots, \beta^n\}$ is an M-basis for L then we takes every element $\sum f_i\alpha^i$ to $\sum \sigma(f_i)\beta^i$. This extends the isomorphism σ. Then we see the group $\tau^{-1}\operatorname{Gal}(L/M)\tau$ fixes F and has the same size as $\operatorname{Gal}(L/F)$ and so it is the same as $\operatorname{Gal}(L/F)$ by using Galois correspondence.

9. $L = \mathbb{Q}(\sqrt{2}+\sqrt{-1})$ by considering the degree of the minimal polynomial of $\sqrt{2}+\sqrt{-1}$. The other conjugates are $-\sqrt{2}-\sqrt{-1}, -\sqrt{2}+\sqrt{-1}, \sqrt{2}-\sqrt{-1}$ are in L (for example, $\sqrt{2}-\sqrt{-1} = \frac{3}{\sqrt{2}+\sqrt{-1}}$). The Galois group is $C_2 \times C_2$, generated by two elements σ, τ where

$$\sigma(\sqrt{-1}) = -\sqrt{-1}, \sigma(\sqrt{2}) = \sqrt{2}, \quad \tau(\sqrt{-1}) = \sqrt{-1}, \tau(\sqrt{2}) = -\sqrt{2}.$$

The subfield corresponding to $\langle\sigma\rangle$ is the one which is fixed by σ, and so it is $\mathbb{Q}(\sqrt{2})$. Similarly the subfield corresponding to τ is $\mathbb{Q}(\sqrt{-1})$ and the subfield corresponding to $\sigma\tau$ is $\mathbb{Q}(\sqrt{-2})$.

10. Let $L = K(X_1, \ldots, X_n)$ then $G = S_n$ acts on $\{X_1, \ldots, X_n\}$ by permutation and let $F := L^G$ be the fixed field. Note that the elementary polynomials in $X_1, \ldots, X_n$ are contained in K. Write $L = K(X_1, \ldots, X_n) = F(X_1, \ldots, X_n)$ Now $X_1, \ldots, X_n$ are roots of $f = \prod_i (X - X_i)$ and the coefficients of f are elementary symmetric polynomials in $X_1, \ldots, X_n$ and so f is a polynomial over F. Therefore $[L : F] \leq n$ and so L/F is Galois with Galois group G.

For the second part, by Cayley's theorem every finite group G is isomorphic to a subgroup of S_n for some n and take L/K Galois with $\operatorname{Gal}(L/K) \cong S_n$ as in the previous part and then embed G as a subgroup of S_n. Then $\operatorname{Gal}(L/L^G) = G$.

11. $f = t^5 - 4t + 2$ is 2-Eisenstein and hence irreducible. Therefore the Galois group G acts transitively on the roots. f is irreducible mod 3 so G contains a 5-cycle, or indeed by considering the action of G on the roots and use orbit-stabiliser theorem we see $|G|$ is divisible by 5 and so it contains an element of order 5 by Sylow's theorem. Similarly, $f \equiv (t+1)(t^2+2t+3)(t^2+2t+4)$ mod 5 so it contains an element of cycle type $2-2-1$. $f \equiv (t^2+4t+6)(t^3+3t^2+3t+5)$ mod 7 so G contains an element of cycle type $2-3$. This shows G is not contained in A_5 and the size of G is at least 30. Since G is transitive so $G = S_5$. Alternatively note that f has exactly two non-real roots so there is an element of cycle type $2-1-1-1$ which corresponds to complex conjugation and this element together with the 5-cycle generate S_5.

12. Note that the Galois group of finite extension is always cyclic. When $K = \mathbb{F}_2$ the polynomial is irreducible so $\operatorname{Gal}(L/K) = C_4$. When $K = \mathbb{F}_2$ then $t^4 + t^3 + 1 = (t+2)(t^3+2t^2+2t+2)$ and so $\operatorname{Gal}(L/K) = C_3$. When $K = \mathbb{F}_4$ then $t^4 + t^3 + 1$ factorises into a product of two quadratic polynomials and so the Galois group is C_2 because if once we adjoin a root of an irreducible quadratic polynomial then we obtain every element in $\mathbb{F}_{16}$ and then any quadratic polynomial

over $\mathbb{F}_4$ splits in $\mathbb{F}_{16}[X]$.

13. Let k be the order of a mod p, so $k|p-1$. We have $\psi(X^k) = a^k X^k = X^k$ so $X^k \in L^G$. Also $\psi^k(X) = a^k X = X$ so $G \cong C_k$. Since $[L : L^G] = |G| = k$, so

$$[L : \mathbb{F}_p(X^k)] = [L : L^G][L^G : \mathbb{F}_p(X^k)] = k[L^G : \mathbb{F}_p(X^k)]$$

But $[L : \mathbb{F}_p(X^k)] = k$ because X satisfies the polynomial $T^k - X^k$ in $\mathbb{F}_p(X^k)[T]$ and it is irreducible (otherwise the minimal polynomial is a proper factor of it which then implies, by looking at the constant term, that $X^t \in \mathbb{F}_p(X^k)$). Therefore $[L^G : \mathbb{F}_p(X^k)] = 1$ and so $L^G = \mathbb{F}_p(X^k)$.

14. $\mathbb{F}_{5^{17}}$ exists, and it is an extension of $\mathbb{F}_5$ of degree 17. Since 17 is a prime so there is no intermediate extensions between $\mathbb{F}_{5^{17}}$ and $\mathbb{F}_5$ so there exists an irreducible polynomial of degree 17.

15. Use $\prod_{d|n} \Phi_d = X^n - 1$ and $\Phi_1 = X - 1$, $\Phi_2 = X + 1$, $\Phi_3 = X^2 + X + 1$, $\Phi_4 = X^2 + 1$. Using Φ_2, Φ_3 we compute $\Phi_6 = X^2 - X + 1$. Therefore $\Phi_{12} = X^4 - X^2 + 1$.

16. Let $K = \mathbb{F}_q$ and if $[L : K] = n$ then $L = \mathbb{F}_{q^n}$ and the multiplicative elements of L are roots of $X^{q^n-1} - 1$ so $L = K(\mu_{q^n-1})$.

17. $\mathrm{Gal}(L/\mathbb{Q}) = C_6$ so by fundamental theorem of Galois there are two intermediate fields F_1, F_2 where $[F_1 : \mathbb{Q}] = 3$ and $[F_2 : \mathbb{Q}] = 2$. Let ζ be a non-trivial root of $X^7 - 1 = 0$ then we see $\zeta + \zeta^{-1}$ is an element fixed by $\zeta \mapsto \zeta^6$ so $F_1 = \mathbb{Q}(\zeta + \zeta^{-1})$. Also $\zeta + \zeta^2 + \zeta^4$ is fixed by $\zeta \mapsto \zeta^2$ so $F_2 = \mathbb{Q}(\zeta + \zeta^2 + \zeta^4)$. Since $L/\mathbb{Q}$ is ablelian so every subgroup is normal and hence every subextension is Galois.

18. (i) Since n is odd (and $n > 1$) if α is a nth primitive root of unity then $-\alpha$ is a $2n$th primitive root of unity and $[\mathbb{Q}(-\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \phi(n)$. Moreover, the $2n$th primitive roots are of the form $-\alpha^k$ where $(k, n) = 1$. Therefore

$$\Phi_{2n}(X) = \prod_{(k,n)=1} (X - (-\alpha^k)) = \prod_{(k,n)=1} (X + \alpha^k) = (-1)^{\phi(n)} \prod_{(k,n)=1} (-X - \alpha^k) = \Phi(-X)$$

because $\phi(n)$ is always even.

(ii) Since $p|n$ so $\phi(pn) = p\phi(n)$. Suppose α is not a primitive nth root of unity, then clearly $\sqrt[p]{\alpha}$ is not a primitive pnth root of unity. Therefore, we have at most $p\phi(n)$ primitive pnth root of unity. But we see $\phi(pn) = p\phi(n)$ so this shows that $\sqrt[p]{\alpha}$ is a primitive pnth root of unity whenever α is a primitive nth root of unity, and if $\beta_1, \ldots, \beta_p$ are pth roots of α then $\prod_i (X - \beta_i) = X^p - \alpha$. This shows that in $\Phi_{np}(X)$ we can collect these factors and so $\Phi_{np}(X)$ is the product of $X^p - \alpha$ where α is a primitive nth root of unity and so $\Phi_{np}(X) = \Phi_n(X^p)$.

(iii) We have

$$\frac{1}{(1 - X^p)(1 - X^q)} = (1 + X^p + X^{2p} + \cdots)(1 + X^q + X^{2q} + \cdots) = \sum_j a_j X^j$$

where $a_j = 1$ if $j = mp + nq$ and 0 otherwise. Suppose $m_1 p + n_1 q = m_2 p + n_2 q$ then $q|m_1 - m_2$ and $p|n_1 - n_2$ since p, q are distinct primes. So $mp + nq$ are distinct for $0 \leq mp + nq < pq$.

$$\Phi_{pq}(X) = \frac{X^{pq}-1}{(1-X^p)(1-X^q)}(X-1)$$

and so by the above observation we expand the right hand side in power series then the terms with degree less than or equal to pq are $\sum_j a_j X^{j+1} - a_j X^j$ but a_j is either 0 or 1 so the coefficients are 0 or ± 1.

(iv) Write $n = 2^a p^b q^c$ for distinct odd primes p, q and by (i) we see $\Phi_{2^a p^b q^c}(X) = \Phi_{p^b q^c}((-1)^a X)$ and so it suffices to consider the polynomial $\Phi_{p^b q^c}(X)$. If $b, c = 0$ then $\Phi_1(X) = X - 1$. If $b = 0, c \geq 1$ then $\Phi_{q^c}(X) = \Phi_q(X^{q^{c-1}})$ by (ii) and $\Phi_q(X)$ has coefficients 1. If $b \geq 1, c \geq 1$ we have $\Phi_{p^b q^c}(X) = \Phi_{pq}(X^{p^{b-1}q^{c-1}})$ and then the result follows from (iii).

(v) Compute Φ_{105} and the coefficient of X^{41} is -2.

19. The element in the Galois group corresponding to -1 is $\zeta_n \mapsto \zeta_n^{-1}$ which is the same as complex conjugation. Now $n \geq 3$ then K is not real so $K \cap \mathbb{R}$ is strictly contained in K and it is the fixed field by complex conjugation and so by FTGT we have $[K : K \cap \mathbb{R}] = 2$.

We see that $\mathbb{Q}(\zeta + \zeta^{-1})$ is strictly contained in K because it is real and $[K : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 2$ as ζ is a root of $T^2 - a\zeta_n + 1$ and it is fixed by complex conjuation so by tower law we conclude that $[K \cap \mathbb{R} : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 1$.