PartII Galois Theory 1

zc231

1. $x^4 - 10x^2 + 1 = 0$.

2. $[L : F][F : K] = [L : K]$ and since $[L : K]$ is a prime so either $[L : F] = 1$ or $[F : K] = 1$ so $L = F$ or $F = K$.

3. If Char(K)$\neq$ 2 then one can complete the square for any quadratic polynomial and so $L = K(x)$ for some $x \in L$ with $x^2 \in K$. Suppose Char(K)= 2 then take $x \notin K$ with $x \in L$. Then we have $x^2 = ax + b$ for some $a, b \in K$. Either $a = 0$ in which case we have $x^2 = b \in K$ or $a \neq 0$ in which case a^{-1} exists in K. Then

$$a^{-2}x^2 = a^{-1}x + a^{-2}b$$

and since Char(K)= 2 so $a^{-1}x = -a^{-1}x$ so $a^{-2}x^2 + a^{-1}x = a^{-2}b \in K$. Take $y = a^{-1}x$ so $y^2 + y = a^{-2}b \in K$.

4. It is clear that $K(x^2) \subset K(x)$ and by tower law we have

$$[K(x) : K] = [K(x) : K(x^2)][K(x^2) : K]$$

and $[K(x) : K(x^2)] = 1$ or 2. But if it is 2 then $[K(x) : K]$ is even which is a contradiction so $K(x) = K(x^2)$.

5. If α, β are algebraic then

$$[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\alpha)][K(\alpha) : K] \leq [K(\beta) : K][K(\beta) : K] < \infty$$

and so

$$[K(\alpha + \beta) : K], [K(\alpha\beta) : K] \leq [K(\alpha, \beta) : K] < \infty$$

and so they are algebraic because every finite extension is algebraic. Conversely, suppose $a = \alpha + \beta, b = \alpha\beta$ are both algebraic then $L = K(a, b)$ is finite over K and note that α, β are roots of $X^2 - aX + b$ over L. So

$$[K(\alpha) : K] = [K(\alpha) : L][L : K] \leq 2[L : K] < \infty, [K(\beta) : K] = [K(\beta) : L][L : K] \leq 2[L : K] < \infty$$

and so they are algebraic over K.

6. Note that $K[s]$ is a Euclidean domain. Suppose $f = \frac{p}{q}$ is algebraic over K where $p, q \in K[s]$ and we may assume p, q are coprime. Then we have

$$f^n + a_{n-1}f^{n-1} + \cdots + a_0 = 0, a_i \in K, n \geq 1, a_0 \neq 0$$

and so $p^n + a_{n-1}p^{n-1}q + \cdots + a_0q^n = 0$ and we can rearrange this

$$p(p^{n-1} + \cdots + a_1) = -a_0q^n.$$

This implies $p|a_0q^n$ and if p is not a constant function this would then imply p, q have a common factor, which is a contradiction. So p is constant. Similarly, since $a_0 \neq 0$ we have

$$q(a_0q^{n-1} + \cdots + a_{n-1}p^{n-1}) = -p^n$$

so $q|p^n$ and so q is constant. Therefore f is a constant.

7. To show L is a subfield of $\mathbb{C}$, we check that if α, β are algebraic over $\mathbb{Q}$, so is $\alpha + \beta, \alpha\beta$ We have shown this in Question 5. Also if α is algebraic then since $K(\alpha) = K(-\alpha) = K(\frac{1}{\alpha})$ so $-\alpha$ and $\frac{1}{\alpha}$ are algebraic. Suppose $[L : \mathbb{Q}]$ is finite then this implies every irreducible polynomial over $\mathbb{Q}$ has bounded degree which is not true (it is easy to construct an irreducible polynomial of degree n using Eisenstein's criteria).

8. For each $0 \neq \alpha \in L$, it satisfies a minimal polynomial

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0, a_i \in K, a_0 \neq 0$$

and apply ψ we have

$$(\psi(\alpha))^n + a_{n-1}(\psi(\alpha^{n-1})) + \cdots + a_0 = 0.$$

Suppose $\psi(\alpha) = 0$ then we must have $a_0 = 0$ which is a contradiction. Therefore the kernel is trivial. Let $\beta \in L$ so it is algebraic over K and let f be its minimal polynomial and $\beta_1 = \beta, \beta_2, \ldots$ be its conjugates in L. Then for each i, $\psi(\beta_i) = \beta_j$ for some j. But ψ is injective so $\psi : \{\beta_1, \beta_2, \ldots\} \to \{\beta_1, \beta_2, \ldots\}$ is injective and hence surjective. In particular $\psi(\beta_i) = \beta$ for some i. Therefore, ψ is bijective.

9. $[L : \mathbb{Q}] = 4$ as $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a $\mathbb{Q}$-basis for L. The three non-trivial automorphisms are

$$\sigma : \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto \sqrt{3}, \gamma : \sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}, \theta : \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}.$$

It is Galois because the number of automorphism is equal to the degree of the extension.

10. $g = (t-1)f = t^n - 1$ and so $g(\mu) = 0$. Since $\mu - 1 \neq 0$ so $f(\mu) = 0$ and since f is irreducible so it is the minimal polynomial of μ. If α is another root then α has to satisfy $\alpha^n - 1 = 0$ and $\alpha \neq 1$ so α is some power of μ and since g is separable so f must be separable. Therefore the extension is Galois.

11. Define $\phi : \mathrm{Gal}(\mathbb{Q}(\mu)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ by $\phi(\sigma_i) = i$ where σ_i sends μ to μ^i where $(i, n) = 1$ (Note that each element in the Galois group is determined by the image of μ). So it is injective. If $(j, n) = d > 1$ then μ^j is a root of $X^{\frac{n}{d}} - 1$ and so

$$[\mathbb{Q}(\mu^j) : \mathbb{Q}] \leq \frac{n}{d} < n - 1 = [\mathbb{Q}(\mu) : \mathbb{Q}] = \deg f$$

so μ^j cannot be a root of f. Therefore, the roots of f are exactly the ones which are coprime to n and so the map ϕ is bijective and it is clear that ϕ is a homomorphism as $\sigma_i\sigma_j(\mu) = \mu^{ij}$.

12. (i) $(t^2-2)(t^2-3) = 0$ so $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $[L : \mathbb{Q}] = 4$. (ii) $t^8-1 = (t-1)(t+1)(t^2+1)(t^4+1)$. So we need a root of $t^4+1 = 0$, say $\alpha = \frac{1+i}{\sqrt{2}}$ and so $L = \mathbb{Q}(\alpha)$ and $[L : \mathbb{Q}] = 4$. (iii) $L = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$ so $[L : \mathbb{Q}] = 6$.

13. Let $f = X^2 + aX + b$ and suppose $f(x) = 0$ with $x \in L$. If f is separable then the other root of f is $-a - x \in L$. If f is inseparable then $x \in L$ is the only root of f so in both cases L contains the splitting field of L.

14. Induction on n: This is clear for $n = 1$. Suppose this holds for n. If now we have f of degree $n+1$. Let x be a root of f and write $f = (X-x)g(X)$ where g has degree n. Let L be the splitting field of g and M be the splitting field of f then $M = L(x)$. It is clear that $[M : L] = [L(x) : L] \leq [K(x) : K] = n+1$, using the result of Question 1 and by induction $[L : K] \leq n!$. Therefore by tower law $[M : K] = [M : L][L : K] \leq (n+1)n! = (n+1)!$.

15. Take any irreducible polynomial f. Suppose f is not separable then $f(X) = g(X^p)$ for some g and write

$$g(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0, a_i \in K, a_0 \neq 0$$

and by assumption for each i we have some b_i such that $b_i^p = a_i$. Then

$$f(X) = g(X^p) = X^{np} + a_{n-1}X^{(n-1)p} + \cdots + a_0 = (X^n + b_{n-1}X^{n-1} + \cdots + b_0)^p$$

which is reducible and this gives a contradiction.

16. This is a special case of the previous question. Let F be a finite field of size p^s (to see this it is clear that F contains a copy of $\mathbb{F}_p$ where p is the characteristic of F, $p \neq 0$ as F is finite and then F is a finite dimensional $\mathbb{F}_p$ vector space so $|F| = p^s$ for some s). In particular the multiplicative group is cyclic (from partIB GRM) and has size $p^s - 1$ which is prime to p, and so each element is a pth power.

17. Let f be the minimal polynomial of α. Suppose α is inseparable then $D(f) = 0$ so we must have

$$f = a_0 + a_1X^p + \cdots + a_mX^{mp}$$

for some $m \geq 1$ so $[K(\alpha) : K] = mp > m$. On the other hand x^p satisfies the polynomial $a_0 + a_1X + \cdots + a_mX^m$ so $[K(\alpha^p) : K] \leq m$ so $K(\alpha) \neq K(\alpha^p)$. Conversely, if $K(\alpha) \neq K(\alpha^p)$. Let g be the minimal polynomial of α over $K(\alpha^p)$. Since $X^p - \alpha^p$ has α as a root so $g \big| X^p - \alpha^p = (X-\alpha)^p$ and so $g = (X-\alpha)^t$ for some $t \geq 1$ and $\alpha^t \in K(\alpha^p)$. If $t < p$ then there exists s such that $ts \equiv 1 \bmod p$ and hence $x \in K(\alpha^p)$ which is a contradiction. So $t = p$ and $g = X^p - \alpha^p$, which is irreducible and inseparable. As $g \big| f$ so f is inseparable. In this case, we see that $[K(x) : K(\alpha^p)] = \deg g = p$ so $p \big| [K(x) : K]$ by tower law.

18. L/K is finite and hence algebraic. L/K is not separable so take an element α which is not separable. Then by the previous question $p|[K(\alpha) : K]$ and hence $p|[L : K]$ by tower law.

19. Let F be a subfield of L which consists of all separable elements of K. We check F is a field and it suffices to check that if x, y are both separable, then so is $x+y$ and xy, but this follows immediately from the fact that $K(x+y), K(xy)$ are subfields of $K(x,y)$.

    Let $x \in L \backslash F$ and f be the minimal polynomial of x over K. Since f is inseparable if p is the characteristic of K ($p > 0$) then we have $f = f_1(X^p)$ for some polynomial f_1 and $\deg f_1 < \deg f$. If f_1 is inseparable we conclude $f_1(X) = f_2(X^p)$ for some f_2 and so on. We do this inductively and since $\deg f_i < \deg f_{i-1}$ so eventually there exists j such that f_j is separable and so the roots of f_j are in F. But $f_j(X^{p^j}) = f(X)$ and so x^{p^j} is a root of $f_j(X)$ so $x^{p^j} \in F$. But x is a root of $X^{p^j} - x^{p^j} = (X-p)^{p^j}$ and so f divides $X^{p^j} - x^{p^j}$ and so $f = (X-p)^t$ for some t. Since $x \notin F$ we conclude $t \geq 2$ and so f is inseparable.

    If g is the minimal polynomial of x over F then $g|f$ and so g is inseparable and this also shows that the minimal polynomial of x over F only has one root and therefore the number of F-homomorphism from L to any extension E is at most 1.

The extension is unique because if $x \in L$ is separable but $x \notin F$ then L/F cannot be purely inseparable as x is separable over K and hence over F. So F consists of exactly the separable elements over K.

20. L/K is finite and L/K is separable as they are subfields of $\mathbb{C}$ which has characteristic zero. Then by primitive element theorem $L = K(x)$ and if $L \neq K$ then the minimal polynomial of x over K has at least two roots and so the number of homomorphism is at least 2.