# PartII Galois Theory 3

zc231

1. (i) True for $n = 1$. Suppose it holds for $n$ then write $(1+p)^{p^{n-1}} = 1 + p^{n-1} + p^n c$ for some $c$. We have
$$(1+p)^{p^{n-1}} = \left((1+p)^{p^{n-2}}\right)^p \equiv (1 + p^{n-1} + p^n c)^p = 1 + p^n + p^{n+1}d$$
for some $d$ so it also holds for $n+1$. Hence $(1+p)^{p^{n-1}} \equiv 1 \bmod p^n$ and by the previous congruence relation we see the order is exactly $p^{n-1}$.

(ii) It is clear that $\left(b^{p^{n-1}}\right)^{p-1} \equiv 1 \bmod p^n$ because the size of the group is $p^{n-1}(p-1)$ and suppose the order is $d$. Then
$$\left(b^{p^{n-1}}\right)^d = \equiv 1 \bmod p^n, \equiv 1 \bmod p$$
and since $b^p \equiv b \bmod p$ so then we have $b^d \equiv 1 \bmod p$ and so $d = p-1$. By (i) and (ii), the element $(1+p)b^{p^{n-1}}$ has order $(p-1)p^{n-1}$ so the group is cyclic.

(iii) This is true for $n = 3$. Suppose $5^{2^{n-3}} \equiv 1 + 2^{n-1} \bmod 2^n$ then
$$5^{2^{n-2}} = \left(5^{2^{n-3}}\right)^2 \equiv \left(1 + 2^{n-1}\right)^2 \equiv 1 + 2^n \bmod 2^n.$$
$-1$ has order 2 and by above we see $-1 \notin \langle 5 \rangle$ and so $\langle -1, 5 \rangle$ has size $2^{n-1}$ so $5, -1$ generate the group and the group is isomorphic to $\mathbb{Z}/2^{n-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(iv) Use (ii) and (iii).

(v) Let $G$ be a finite abelian group then $G \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n^{\alpha_n}\mathbb{Z}$ and for each $p_i$ take a prime $q_i$ with $q_i \equiv 1 \bmod p_i^{\alpha_i}$, using Dirichlet's theorem. Let $N = \prod_{i=1}^n q_i$ and $F = \mathbb{Q}(\zeta_N)$. Let
$$H = \mathrm{Gal}(F/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times \cong \mathbb{Z}/(q_1 - 1)\mathbb{Z} \times \cdots \times \mathbb{Z}/(q_k - 1)\mathbb{Z}.$$
Now pick integers $h_i$ with $h_i = \frac{q_i - 1}{p_i^{\alpha_i}}$ and so $C_{h_i}$ is a subgroup of $\mathbb{Z}/(q_i - 1)\mathbb{Z}$ and let $H_i = (\mathbb{Z}/(q_i - 1)\mathbb{Z})/C_{h_i}$. Since $F/\mathbb{Q}$ is abelian extension so each subextension is again abelian and let $L$ be the fixed field of $F$ by $H_1 \times H_2 \times \cdots H_n$ then the Galois group of $L/\mathbb{Q}$ is isomorphic to $G$.

(vi) Use (v) we take $q = 47$ which is 1 mod 23 and let $F = \mathbb{Q}(\zeta_{47})$ and let $H$ be a subgroup of order 2 inside $G = \mathrm{Gal}(F/\mathbb{Q}) \cong \mathbb{Z}/46\mathbb{Z}$ then $G/H \cong \mathbb{Z}\mathbb{Z}/23\mathbb{Z}$. Let $L = F^H$ and in fact we take $H$ to be group generated by complex conjugation so $L = \mathbb{Q}(\cos\left(\frac{2\pi}{47}\right))$.

2. Since $\mu_n \subset K$ so the splitting field of $f$ is $K(\sqrt[n]{a})$ and if $b = c^n a^r$ then the splitting field of $g$ is $K(c\sqrt[n]{a^r}) = K(\sqrt[n]{a}$ as $(r, n) = 1$. Conversely, if the splitting field of $f$ is the same as the splitting field of $g$, say $L$. Then $L/K$ is Galois and is cyclic. Let $\sigma$ be an element in the Galois group such that $\sigma(\sqrt[n]{b}) = \zeta_n \sqrt[n]{b}$. So $\sigma$ generates the Galois group. Then $\sigma(\sqrt[n]{a}) = \zeta_n^s \sqrt[n]{a}$ for some $s$ coprime to $n$. Then take $r$ with $rs \equiv 1 \bmod n$ and so
$$\sigma\left(\sqrt[n]{\frac{a^r}{b}}\right) = \frac{\zeta_n^{rs}\sqrt[n]{a}}{\zeta_n \sqrt[n]{b}} = \sqrt[n]{\frac{a^r}{b}}.$$

Therefore $\sqrt[n]{\frac{a^r}{b}}$ is fixed by the Galois group and so $\frac{a^r}{b} = \frac{1}{c^n}$ for some $c \in K$, which then gives $b = c^n a^r$.

3. One direction is clear: if it is irreducible over $L$ then it is irreducible over $K$ because $K$ is a subfield of $L$. Conversely, if $t^p - a$ is reducible over $L$. Let $\beta$ be a root of $t^p - a$ so $s := [L(\beta) : L] < p$ because $t^p - a$ is reducible. Suppose $t^p - a$ is irreducible over $K$ and $\alpha$ a root of $t^p - a$. Then $[K(\beta) : K] = p$. But on the other hand, $K(\alpha) \subset L$ and $L = K(\mu_p)$ so $[L : K] = p - 1$ because the characteristic of $K$ is not equal to $p$. Then by tower law, we have

$$p[L(\beta) : K(\beta)] = [L(\beta) : K(\beta)][K(\beta) : K] = [L(\beta) : K] = [L(\beta) : L][L : K] = s(p-1)$$

which is impossible because $s, p-1 \nmid p$. Therefore $t^p - a$ is also reducible over $K$.

If $p$ is not a prime, then consider $K = \mathbb{Q}$, $p = 4$ and $t^4+1$. So $L = \mathbb{Q}(i)$ and $t^4+1 = (t^2+i)(t^2-i)$. But $t^4 + 1$ is irreducible over $\mathbb{Q}$ because $(t+1)^4 + 1$ is 2-Eisenstein.

4. If $a = c^d$ for some $d|n$ with $d > 1$ then $t^{\frac{n}{d}} - a$ is a factor of $t^n - a$ and so it is reducible. Conversely, assume $t^n - a$ is reducible. Let $\alpha$ be a root of $t^n - a$ and then $t^n - a$ factors as $(t-\alpha)(t-\zeta_n\alpha)\cdots(t-\zeta^{n-1}\alpha)$ over the splitting field. Since $t^n - a$ is reducible over $K$ so the minimal polynomial of $\alpha$ is a proper factor of the above and by considering the constant term we conclude that $\alpha^q \in K$ for some $q < n$ because $\zeta_n \in K$. Let $q$ be the smallest positive integer such that $\alpha^q \in K$. Then we conclude that $q|n$. Write $d = \frac{n}{q}$ so $d > 1$ and $d|n$. Then $a = (\alpha^q)^d$ is a $d$th power.

Consider $K = \mathbb{Q}$ and $a = -4$. Then $t^4+4 = (t^2+2+2t)(t^2+2-2t)$. But $-4$ is not a power in $\mathbb{Q}$.

5. If the characteristic is not equal to 2 then $L/K$ is separable and $L = K(\sqrt{\alpha})$ for some $\alpha \in K$ and so it is Kummer extension.

6. For each $i \geq 1$ let $F_i$ be the splitting field of $(t^i-1)(t^{i-1}-1)\cdots(t-1)$. We check that $F_i/F_{i-1}$ is a Kummer extension for each $i$. It is clear that $F_i/F_{i-1}$ is Galois with Galois group a subgroup of $(\mathbb{Z}/i\mathbb{Z})^*$. So the exponent of the group is a factor of $(n-1)!$. By construction $\mu_{(n-1)!} \subset F_{i-1}$. Since the Galois group is Abelian so the extension is a Kummer extension. Thus we have $K \subset F_1 \subset \cdots \subset F_n$ and $L \subset F_n$.

Note that if you use your definition of Kummer extension then this still works because then $F_i/F_{i-1}$ is a sequence of Kummer extensions because you can decompose the Abelian group into product of cyclic groups and each of them has size dividing $(n-1)!$ so each subextension is Kummer.

7. Soluble extensions are radical extensions. So $F/K, E/K$ are both radical. We have extensions $K = F_0 \subset F_1 \subset \cdots F_n$ and $K = E_0 \subset E_1 \subset \cdots E_m$ where $F_n/F, E_m/E$ are both finite extensions, $F_i = F_{i-1}(a_i), E_i = E_{i-1}(b_i)$ are either cyclotomic of Kummer extension. Now define $R_0 = F_n$ and inductively define $R_i = R_{i-1}(b_i)$ for each $i \leq m$. Then $R_i/R_{i-1}$ is either cyclotomic or Kummer extension and $R_m = F_n(b_1, \ldots, b_m) = F_nE_m$ which contains $FE$ and $F_nE_m/FE$ is finite because $F_n/F, E_m/E$ are both finite. Therefore we have a sequence of cyclotomic or Kummer extensions

$$K = F_0 \subset F_1 \subset \cdots F_n = R_0 \subset R_1 \subset R_2 \cdots R_m = F_nE_m$$

and so $FE/K$ is radical. Note that $R_1/R_0$ is Kummer or cyclotomic because $E_1/E_0$ is Kummer or cyclotomic (if $E_1/E_0$ is Kummer extension of degree $k$ then that means $\mu_k \subset K \subset F_n$).

8. Let $F = \mathbb{Q}(\mu_{17})$ and $L = \mathbb{Q}(\cos\frac{2\pi}{17})$. $[F : L] = 2$ and $\mathrm{Gal}(F/\mathbb{Q}) \cong (\mathbb{Z}/17\mathbb{Z})^\times$ so
$$\mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/17\mathbb{Z})^\times/\{\pm 1\} \cong \mathbb{Z}/8\mathbb{Z}.$$
Let $\alpha = e^{\frac{2\pi i}{17}}$ so $2\cos\frac{2\pi}{17} = \alpha + \alpha^{-1}$. The other conjugates of $\alpha+\alpha^{-1}$ are $\alpha^2+\alpha^{-2}, \cdots, \alpha^8+\alpha^{-8}$. Then we find an element in the Galois group has order 2 in $(\mathbb{Z}/17\mathbb{Z})^\times/\{\pm 1\}$. For example we can take $\alpha \mapsto \alpha^4$. Note that $\alpha^4 + \alpha^{-4} = \beta^4 - 4\beta^2 - 2$. So we take $\gamma = \alpha + \alpha^{-1} + \alpha^4 + \alpha^{-4} = \beta^4 - 4\beta^2 + \beta - 2$. The other conjugate of $\beta$ over $\mathbb{Q}(\gamma)$ is $\alpha^4 + \alpha^{-4}$. So the minimal polynomial of $\beta$ over $\gamma$ is
$$X^2 - \gamma X + \frac{1}{2}(-\gamma^3 + 6\gamma - 3).$$
Finally we take an element in the Galois group which has order 2 in $(\mathbb{Z}/16\mathbb{Z})^\times/\{\pm 1, \pm 4\}$. For example we can take $\alpha \mapsto \alpha^2$ so we take
$$\delta = \alpha + \alpha^{-1} + \alpha^2 + \alpha^{-2} + \alpha^4 + \alpha^{-4} + \alpha^8 + \alpha^{-8}$$
The minimal polynomial of $\gamma$ over $\mathbb{Q}(\delta)$ is
$$X^2 - \delta X - 1.$$
Also the minimal polynomial of $\delta$ should have degree 2 and indeed it is
$$X^2 + X - 4.$$
Then $\delta = \frac{-1+\sqrt{17}}{2}$. Now use the minimal polynomial of $\gamma$ over $\mathbb{Q}(\delta)$ to work out $\delta$ and so on. Note that at each stage we will have 2 roots. We always take the larger one because of our choices for $\beta, \gamma, \delta$ we pick. For example, the other conjugate of $\beta$ is $\alpha^4 + \alpha^{-4}$ but $\alpha + \alpha^{-1} > \alpha^4 + \alpha^{-4}$ by properties of cos.

9. If $f$ is not irreducible, say $f = f_1 f_2$ then the Galois group cannot send roots of $f_1$ to $f_2$ so it does not act transitively. Conversely, if $f$ is irreducible then for any roots $\alpha_1, \alpha_2$, the map sending $\alpha_1$ to $\alpha_2$ extends to a $K$-isomorphism from $K(\alpha_1)$ to $K(\alpha_2)$. By using argument for question 8 on the second example sheet, we see this $K$-isomorphism extends to a $K$-automorphism of $L$, which gives an element of the Galois group. Therefore $\mathrm{Gal}(L/K)$ acts transitively on the roots.

10. If the discriminant is a square then the statement is obvious so we assume the discriminant is not a square in $K$. Then $[K(\alpha) : K] = 2$. Suppose $f$ is reducible over $K(\alpha)$ then $f$ has a root in $K(\alpha)$, say $\beta$. But $f$ is irreducible over $K$ so $[K(\beta) : K] = 3$. Since $\beta \in K(\alpha)$ so $[K(\beta) : K] \leq [K(\alpha) : K] = 2$ which is a contradiction.

11. $V_4 \cong C_2 \times C_2$ is a normal subgroup of $A_4$ and let $F$ be the field corresponding to $V_4$. Then $F/\mathbb{Q}$ is a cubic Galois extension and $\mathrm{Gal}(L/F) \cong V_4$. We have 3 subgroups of $V_4$ with index 2, which correspond to 3 intermediate fields of degree 2 between $F$ and $L$. Since the characteristic is not equal to 2, so each of them is generated by a square root of some element in $F$, say $F_1 = F(\sqrt{a}), F_2 = F(\sqrt{b}), F_3 = F(\sqrt{c})$. Then $F(\sqrt{a}, \sqrt{b}) \subset L$ has degree 4 over $F$ because if not then $a$ is a square in $F(\sqrt{b})$ which means $F(\sqrt{a}) = F(\sqrt{b})$ or $F(\sqrt{a}) = F$. Then by tower law we conclude $L = F(\sqrt{a}, \sqrt{b})$.

12. We firstly consider the Galois group of $f$ over $\mathbb{Q}$. $f$ is 2-Eisenstein so it is irreducible and so the Galois group acts transitively. Then either by considering $f$ mod 3 or computing the resolvent cubic, which is $X^3 - 8X + 16$, we conclude the Galois group over $\mathbb{Q}$ has a 3-cycle (Note that if we replace $X$ by $2X$ in the resolvent cubic then it is 2-Eisenstein and hence irreducible). Then the only transitive subgroups of $S_4$ which contains a 3-cycle are $A_4$ or $S_4$. But discriminant of $f$ is $-4864$ which is not a square so the Galois group is not contained in $A_4$ and so the Galois group of $f$ over $\mathbb{Q}$ is $S_4$. Now the Galois group of $f$ over $\mathbb{Q}(i)$ is a subgroup of the Galois group of $f$ over $\mathbb{Q}$, of index at most 2 by using tower law. So it is either $S_4$ or $A_4$. But again the discriminant $-4864$ is not a square in $\mathbb{Q}(i)$ so the Galois group is $S_4$.

13. (i) If we obtain $R$ by intersection of two lines, say $A_1A_2$ and $B_1B_2$. The the equations for $A_1A_2$ are degree 1 polynomials in $x$ and $y$ with coefficients in $S$. So the intersection is again contained in $S$. Suppose $R$ is intersection of a line $AB$ and a circle centered at $PQQ'$ with $Q, Q' \in S$ (and hence $P \in S$). Then the equation of $PQQ'$ is a quadratic polynomial in $x, y$ which has the form $x^2 + y^2 + ax + by + c$ where $a, b, c \in \mathbb{Q}(S)$ and so the point $R$ is contained in a quadratic extension of $S$.

    Finally if we have intersection of two circles then we have intersections of

    $$x^2 + y^2 + a_1x + b_1y + c_1 = 0, x^2 + y^2 + a_2x + b_2y + c_2 = 0.$$

    Then by direct computation we conclude that the intersection is contained in a quadratic extension of $\mathbb{Q}(S)$.

    (ii) This follows direct from (i) and tower law.

    (iii) This follows from (ii), using $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.