1 Solvable groups

Definition. Let G be a group. A *finite filtration* of G is a finite sequence $G_\bullet$ of subgroups

$$\{1\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

such that G_i is normal in G_{i+1} for all $i \in \{0, \ldots, n-1\}$.

The number n is called the *length* of the finite filtration.

The finite filtration $G_\bullet$ is said to *have no redundancies* if $G_i \neq G_{i+1}$ for all i.

The finite filtration $G_\bullet$ is said to *have abelian quotients* if G_{i+1}/G_i is always abelian.

Finally, the finite filtration $G_\bullet$ is said to be *trivial* if $n = 1$

Definition. A group is *solvable* if there exists a finite filtration of G with abelian quotients.

A group G is *simple* if it has no nontrivial normal subgroups.

Lemma. Let G be a solvable group and let H be a subgroup.

Then H is solvable. If H is normal in G, then the quotient group G/H is also solvable.

Proof. Given a finite filtration $G_\bullet$ of G with abelian quotients, we can produce one for H or G/H (when $H \lhd G$) by replacing G_i with $G_i \cap H$ or $\pi(G_i)$, where $\pi : G \to G/H$ is the quotient homomorphism. □

Lemma. Let G be a group and let $H \subseteq G$ be a normal subgroup.

Suppose that H is solvable and that G/H is solvable. Then G is solvable.

Proof. To get a finite filtration of G with abelian quotients, start with one for G/H.

Then replace all the terms by their preimages under the quotient homomorphism $G \to G/H$.

This will give an ascending sequence of subgroups containing H.

Now add this sequence to the end of a finite filtration of H with abelian quotients. □

Write $Z(G) = \{x \in G : xh = hx \text{ for all } h \in G\}$ for the center of G.

Proposition. Let G be a finite group and let p be a prime number.

Suppose that there is an $n \geq 0$ such that $|G| = p^n$. Then $|Z(G)| \geq p^{\min\{1,n\}}$ and G is solvable.

A finite group whose order is a power of a prime number p is called a *p-group*.

Proof. The proposition clearly holds if $n = 0$. Assume $n > 0$.

The subgroup $Z(G)$ is abelian, hence solvable. Also, $Z(G) \lhd G$ and $G/Z(G)$ is a p-group.

If we can show that $|Z(G)| \geq p$ then the previous lemma will imply that G is solvable by induction.

Notice that $|Z(G)|$ is the number of conjugacy classes of G of size one.

There is at least one of these, given by $\{1\}$.

All other conjugacy classes of G have size divisible by p as they are G-orbits under the conjugation action of elements whose centralizers are proper subgroups, and thus whose sizes are proper divisors of p^n.

Therefore $|Z(G)| \equiv |G| \equiv p^n \equiv 0 \pmod{p}$. Thus as $|Z(G)| \geq 1$ we must have $|Z(G)| \in \{p, p^2, p^3, \dots\}$. □

Definition. The *length* of a finite group G is the quantity

$$\ell(G) = \sup\{n \in \mathbb{N} : n \text{ is the length of a finite filtration with no redundancies of } G\}.$$

Note that the length of a finite group is necessarily finite, because the length cannot be larger than $|G|$.

Lemma. Suppose that G is a finite group.

Let $G_\bullet$ be finite filtration of G with no redundancies of length $\ell(G)$.

Then G_{i+1}/G_i is simple for all i, and if G is solvable then each quotient is a cyclic group of prime order.

Proof. If G_{i+1}/G_i is not simple then we could extend $G_\bullet$ to a longer filtration by replacing $G_i \subseteq G_{i+1}$ by the preimage in G_{i+1} of a filtration of G_{i+1}/G_i with no redundancies.

Assume G is solvable. Then each subgroup G_i and each quotient G_i/G_{i+1} is solvable.

Hence each G_i/G_{i+1} must be abelian as otherwise we could similarly extend $G_\bullet$ to a larger filtration.

Any finitely generated abelian group is a finite direct sum of cyclic groups of prime order.

So if G_{i+1}/G_i is not cyclic of prime order then we could extend $G_\bullet$ to a longer filtration by replacing $G_i \subseteq G_{i+1}$ by the preimage in G_{i+1} of a filtration of G_{i+1}/G_i with cyclic quotients of prime order. □

Examples.

- All abelian groups are solvable.
- The *alternating group* $A_n = \{w \in S_n : \operatorname{sgn}(w) = 1\}$ is simple for $n = 3$ and $n \geq 5$.

  The groups A_n for $n \geq 5$ are not abelian and hence not solvable.
- The groups $A_1 = A_2 = \{1\}$ and $A_3 = \{1,\ (1,2,3),\ (1,3,2)\}$ are cyclic and therefore solvable.

  The group A_4 is solvable since we have subgroups

  $$G_0 = \{1\} \lhd G_1 = \{1,\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3)\} \lhd G_2 = A_4.$$

  The quotients G_1/G_0 and G_2/G_1 have sizes 4 and 3 so are abelian.
- As $A_n \lhd S_n$ and $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$, the symmetric group S_n is solvable if and only if $n \in \{1, 2, 3, 4\}$.

2 Solvability by radicals

Let $L \mid K$ be a finite field extension.

Definition. The extension $L \mid K$ is *radical* if $L = K(\alpha_1, \dots, \alpha_k)$ for some elements $\alpha_i \in L$ such that

$$\alpha_1^{n_1} \in K, \qquad \alpha_2^{n_2} \in K(\alpha_1), \qquad \alpha_3^{n_3} \in K(\alpha_1, \alpha_2), \qquad \dots, \qquad \alpha_k^{n_k} \in K(\alpha_1, \dots, \alpha_{k-1})$$

for some positive integers $n_1, \dots, n_k > 0$.

If $L \mid K$ and $M \mid L$ are radical extensions, then $M \mid K$ is also radical extension.

Recall that a *Kummer extension* is a splitting extension for $x^n - a$ when $a \in K$ and $\gcd(n, \mathrm{char}(K)) = 1$.

Kummer extensions are radical. This fact will play an essential role below.

Lemma. Let $L \mid K$ be a radical extension and let $J \mid L$ be a finite extension.

Assume the composed extension $J \mid K$ is a Galois extension.

Then there is an intermediate field L' between J and L such that $L' \mid K$ is Galois and radical.

Proof. Suppose that $L = K(\alpha_1, \ldots, \alpha_k)$ and that there are natural numbers $n_1, \ldots, n_k$ such that

$$\alpha^{n_1} \in K, \qquad \alpha^{n_2} \in K(\alpha_1), \qquad \alpha^{n_3} \in K(\alpha_1, \alpha_2), \qquad \ldots, \qquad \alpha^{n} \in K(\alpha_1, \ldots, \alpha_{k-1}).$$

Write $G = \mathrm{Gal}(J \mid K) = \{\sigma_1, \ldots, \sigma_t\}$ for the finite Galois group.

Note that for any $i \in \{1, \ldots, k\}$ and any $\sigma \in G$, we have

$$\sigma(\alpha_i^{n_i}) = \sigma(\alpha_i)^{n_i} \in \sigma(K(\alpha_1, \ldots, \alpha_{i-1})) = K(\sigma(\alpha_1), \ldots, \sigma(\alpha_{i-1})).$$

Let $\mathrm{Orb}(\alpha_i) = \mathrm{Orb}(G, \alpha_i)$. We conclude that the extension

$$K(\alpha_1, \ldots, \alpha_k, \sigma_1(\alpha_1), \ldots, \sigma_1(\alpha_k), \sigma_2(\alpha_1), \ldots, \sigma_2(\alpha_k), \ldots, \sigma_t(\alpha_1), \ldots, \sigma_t(\alpha_k))$$

coincides with

$$K(\mathrm{Orb}(\alpha_1), \ldots, \mathrm{Orb}(\alpha_k))$$

which is also a radical extension of K. Since

$$\sigma(K(\mathrm{Orb}(\alpha_1), \ldots, \mathrm{Orb}(\alpha_k)) = K(\sigma(\mathrm{Orb}(\alpha_1)), \ldots, \sigma(\mathrm{Orb}(\alpha_k))) = K(\mathrm{Orb}(\alpha_1), \ldots, \mathrm{Orb}(\alpha_k))$$

for any $\sigma \in G$, we see that $L' = K(\mathrm{Orb}(\alpha_1), \ldots, \mathrm{Orb}(\alpha_k)) \mid K$ is a Galois extension. □

Theorem. Suppose that $\mathrm{char}(K) = 0$. Let $L \mid K$ be a finite Galois extension.

Let $d = |\mathrm{Gal}(L \mid K)| = [L : K]$ and choose a splitting field $K(\mu_d)$ for the polynomial $x^d - 1$.

(a) If $\mathrm{Gal}(L \mid K)$ is solvable then there exists a finite extension $M \mid L$ with the following properties:

(1) The extension $M \mid K$ is Galois.

(2) There is a homomorphism of K-extensions $K(\mu_d) \hookrightarrow M$

(3) M is generated by the images of L and $K(\mu_d)$ in M

(4) The extension $M \mid K(\mu_d)$ is a composition of Kummer extensions, so $M \mid K$ is radical.

(b) Conversely, if there is a finite extension $M \mid L$ with $M \mid K$ radical, then $\mathrm{Gal}(L \mid K)$ is solvable.

Proof. By past results on splitting fields, there exists a Galois extension $J \mid K(\mu_d)$ and a homomorphism

$$J \mid K(\mu_d) \to J \mid L.$$

By construction, we then have the following diagram of field extensions:

$$\begin{array}{ccc} L & \hookrightarrow & J \\ \uparrow & & \uparrow \\ K & \hookrightarrow & K(\mu_d) \end{array}$$

Let P be the field generated by L and $K(\mu_d)$ in J. This leads to the following diagram of field extensions:

$$\begin{array}{ccccc} L & \hookrightarrow & P & \hookrightarrow & J \\ \uparrow & & \uparrow & & \\ K & \hookrightarrow & K(\mu_d) & & \end{array}$$

Let $G = \mathrm{Gal}(J \mid K)$ and note the following:

(F1) $P \mid K$ is a Galois extension as if $\sigma \in G$ then $\sigma(L) = L$ and $\sigma(K(\mu_d)) = K(\mu_d)$ and thus $\sigma(P) = P$.

(F2) $P \mid K(\mu_d)$ is a Galois extension. This follows from the fact that $P \mid K$ is a Galois extension.

(F3) The restriction map $\mathrm{Gal}(P \mid K(\mu_d)) \to \mathrm{Gal}(L \mid K)$ is injective.

Indeed if $\sigma \in \mathrm{Gal}(P \mid K(\mu_d))$ restricts to the identity on L, then σ fixes $K(\mu_d)$ and L.

Thus σ must fix all of P, since P is generated by L and $K(\mu_d)$ over K.

We now prove (a). Suppose that $\mathrm{Gal}(L \mid K)$ is solvable.

Then by (F3), we see that $\mathrm{Gal}(P \mid K(\mu_d))$ is solvable, so is a finite filtration

$$0 = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = \mathrm{Gal}(P \mid K(\mu_d))$$

whose quotients are cyclic. The subgroups H_i correspond to a decreasing sequence of subfields

$$P = P_0 \supseteq P_1 \supseteq \cdots \supseteq P_{n-1} \supseteq P_n = K(\mu_d)$$

such that $P_i \mid P_{i+1}$ is a Galois extension for any $i \in \{0, \ldots, n-1\}$. Furthermore, we then have

$$\mathrm{Gal}(P_i \mid P_{i+1}) \cong H_{i+1}/H_i$$

so $\mathrm{Gal}(P_i \mid P_{i+1})$ is cyclic.

Now $|H_{i+1}/H_i|$ is a divisor of $|\mathrm{Gal}(P \mid K(\mu_d))|$ and thus of $|\mathrm{Gal}(L \mid K)| = d$ by (F3).

Thus the polynomial $x^{\#\mathrm{Gal}(P_i|P_{i+1})} - 1$ splits in $K(\mu_d)$.

By our main theorem on Kummer extensions last time, this implies that $P_i \mid P_{i+1}$ is a Kummer extension.

Thus $P_i \mid P_{i+1}$ is a radical extension so we conclude that $P \mid K(\mu_d)$ is a radical extension.

Now note that $K(\mu_d) \mid K$ is a radical extension, because $K(\mu_d)$ is generated over K by a generator ω of the group of dth roots of unit in $K(\mu_d)$, which satisfies the equation $\omega^d - 1 = 0$.

Thus $P \mid K$ is a radical extension.

Now set $M := P$. We have just seen that M satisfies (1), (2), (3) and (4), which proves (a).

To prove (b) suppose that there is a finite extension $M \mid L$ such that $M \mid K$ is radical.

Then we may assume that $M = K(\alpha_1, \ldots, \alpha_k)$ and thre are natural numbers $n_1, \ldots, n_k$ such that

$$\alpha_1^{n_1} \in K, \qquad \alpha_2^{n_2} \in K(\alpha_1), \qquad \alpha_3^{n_3} \in K(\alpha_1, \alpha_2), \qquad \ldots, \qquad \alpha_k^{n_k} \in K(\alpha_1, \ldots, \alpha_{k-1}).$$

Let $t = n_1 n_2 n_3 \cdots n_k$. As before, choose a Galois extension $J \mid K$ with homomorphisms

$$M \mid K \hookrightarrow J \mid K \qquad \text{and} \qquad K(\mu_t) \mid K \hookrightarrow J \mid K.$$

Let E be the field generated by M and $K(\mu_t)$ in J. We then have a diagram of extensions

$$\begin{array}{ccccc} & & J & & \\ & & \uparrow & & \\ M & \hookrightarrow & E & \hookleftarrow & K(\mu_t) \\ \uparrow & & & & \uparrow \\ L & & \hookrightarrow & & K \end{array}$$

Now we see from the definitions that $E = K(\mu_t)(\alpha_1, \ldots, \alpha_k)$ and that

$$\alpha_1^{n_1} \in K(\mu_t), \qquad \alpha_2^{n_2} \in K(\mu_t)(\alpha_1), \qquad \alpha_3^{n_3} \in K(\mu_t)(\alpha_1, \alpha_2), \qquad \ldots, \qquad \alpha_k^{n_k} \in K(\mu_t)(\alpha_1, \ldots, \alpha_{k-1}).$$

Thus each of the extensions $K(\mu_t)(\alpha_1, \ldots, \alpha_{i+1}) \mid K(\mu_t)(\alpha_1, \ldots, \alpha_i)$ is a Kummer extension, since $n_i \mid t$.

We proved last time that the Galois group of a Kummer extension embeds into an abelian group.
Hence $\mathrm{Gal}(K(\mu_t)(\alpha_1, \ldots, \alpha_{i+1}) \mid K(\mu_t)(\alpha_1, \ldots, \alpha_i))$ is an abelian group.
The group $\mathrm{Gal}(K(\mu_t) \mid K)$ is also abelian, by results last time on cyclotomic extensions.
Invoking the fundamental theorem of Galois extensions, we conclude that $\mathrm{Gal}(E \mid K)$ is solvable.

Finally, the group $\mathrm{Gal}(L \mid K)$ is a quotient of the group $\mathrm{Gal}(E \mid K)$ so is also solvable. □

The previous theorem motivates the following definition.

Definition. Let $P(x) \in K[x]$ and let $L \mid K$ be a splitting extension for $P(x)$.
The polynomial $P(x)$ is *solvable by radicals* if there is an extension $M \mid L$ such that $M \mid K$ is radical.

This does not depend on the choice of splitting field of $P(x)$ as these are all isomorphic as K-extensions.
By the previous theorem, $P(x)$ is solvable by radicals if and only if the group $\mathrm{Gal}(L \mid K)$ is solvable.

The group S_n acts on $K(x_1 \ldots, x_n)$ by permuting the variables.
This action is K-linear field automorphism, and we may consider the subfield $K(x_1 \ldots, x_n)^{S_n}$.

Corollary. Let $n \geq 5$. Choose a field K.
Then the extension $K(x_1 \ldots, x_n) \mid K(x_1 \ldots, x_n)^{S_n}$ is not radical.

Proof. Note that the extension $K(x_1 \ldots, x_n) \mid K(x_1 \ldots, x_n)^{S_n}$ is a Galois extension by Artin's lemma.
On the other hand, we have seen that the group S_n is not solvable for $n \geq 5$.
By theorem, the extension $K(x_1 \ldots, x_n) \mid K(x_1 \ldots, x_n)^{S_n}$ cannot be radical. □