1 Solvable Groups

Recall that a subgroup $H$ of a group $G$ is called normal if $ghg^{-1} = h$ for all $h \in H$ and all $g \in G$. We write $H \triangleleft G$ when $H$ is a normal subgroup of $G$.

**Definition 1** A group $G$ is called solvable (or soluble) if there exist subgroups

$$\{e\} \triangleleft G_1 \triangleleft G_2 \triangleleft \ldots \triangleleft G_n \triangleleft G$$

such that the quotients $G/G_{n-1}$, $G_{n-1}/G_{n-2}$, ..., $G_2/G_1$, and $G_1/\{e\}$ are all abelian. (Usually, the trivial group is denoted $G_0$ and $G$ itself is denoted $G_n$.)

**Problem 1**

- Show that every abelian group is solvable.

  *Solution:* If $G$ is abelian, then every subgroup (in particular the trivial one) is normal, so we have $\{e\} \triangleleft G$.

- Show that the permutation group $S_3$ is solvable.

  *Solution:* $\{e\} \triangleleft \{e, (123), (132)\} \triangleleft S_3$. (The group in the middle is $\mathbb{Z}/3$, which is abelian.)

- (Challenge) Show that $S_4$ is solvable.

  *Solution:* $\{e\} \triangleleft \{e, (12)(34), (13)(24), (14)(23)\} \triangleleft A_4 \triangleleft S_4$ (see below for definition of $A_4$).

- Show that any subgroup of a solvable group is solvable.

  *Solution:* Let $H$ be a subgroup of $G$, and suppose $G$ is solvable, and take $\{e\} = G_0 \triangleleft \ldots \triangleleft G_n = G$ as in the definition. Then $\{e\} = G_0 \cap H \triangleleft \ldots \triangleleft G_n \cap H = H$, and all the quotients $(G_j \cap H)/(G_{j-1} \cap H)$ are still abelian.
As Problem 1 shows, most groups that we could possibly think of are solvable. The most important example of a non-solvable group, and also the smallest, is the following group with 60 elements (think about why it has 60 elements!)

**Definition 2** To every permutation $\sigma \in S_n$, written in cycle notation, associate with it a number as follows:
- To a $k$-cycle, associate the number $k - 1$.
- To the product of two permutations, associate the sum of their numbers.

$\sigma$ is called **even** if this number is even, and **odd** if this number is odd.

Let $A_n$ be the subset of $S_n$ containing all the even permutations.

**Problem 2** Show that $A_n$ is a subgroup of $S_n$.

**Solution:** Since $A_n$ is a subset of $S_n$, we need to check that it is closed under composition of permutations. But this is by definition: since the sum of two even numbers is even, the composition of two even permutations is still even.

$A_n$ is called the alternating group on $n$ elements (recall that $S_n$ is called the symmetric group).

**Theorem 1** For $n \geq 5$, $A_n$ is simple - that is, it has no normal subgroups besides the trivial subgroup and itself.

**Problem 3** Show that $A_5$ is not solvable. Then show that $S_5$ is not solvable.

**Solution:** Suppose $A_5$ were solvable. Then there is a sequence $\{e\} = G_0 \triangleleft \ldots \triangleleft G_n = A_5$. But $A_5$ is simple, so $G_{n-1}$ is either trivial or $A_5$, and so on - there is some $j$ such that $G_j$ is trivial and $G_{j+1}$ is $A_5$. But then $G_{j+1}/G_j = A_5$ which is not abelian, which is a contradiction. Therefore $A_5$ is not solvable, and since subgroups of solvable groups are solvable, $S_5$ cannot be solvable either.
2 The Abel-Ruffini Theorem

Last week we showed how to extend \( \mathbb{Q} \) to larger number systems. The same process can be used to extend an extension of \( \mathbb{Q} \), and so on.

**Problem 4** Suppose that \( L \) is an extension of \( K \) and \( M \) is an extension of \( L \) (and therefore also an extension of \( K \)). Show that \( \text{Gal}(M/L) \triangleleft \text{Gal}(M/K) \).

**Solution:** Let \( h \in \text{Gal}(M/L) \), and \( g \in \text{Gal}(M/K) \). Then \( h(y) = y \) for all \( y \in L \), so for all \( x \in L \), \( g^{-1}(x) \in L \), so that \( g(h(g^{-1}(x)))) = g(g^{-1}(x)) = x \), so that \( (g \circ h \circ g^{-1})(x) = x \) for all \( x \in L \), or in other words, \( ghg^{-1} \in \text{Gal}(M/L) \), and therefore this forms a normal subgroup.

**Problem 5** Let \( K, L, M \) be as in the previous problem. Show that \( \text{Gal}(M/K) / \text{Gal}(M/L) = \text{Gal}(L/K) \).

**Solution:** \( f, g \in \text{Gal}(M/K) \) are equivalent under \( \text{Gal}(M/L) \) if they are the same function on \( L \), as their behavior outside can be modified by the normal subgroup. Therefore equivalence classes in the left-hand side are represented by automorphisms of \( L \) over \( K \), which is exactly the right-hand side.

**Problem 6** Show that for any number system \( K \), \( \text{Gal}(K/K) \) is the trivial group.

**Solution:** By definition, if \( f \in \text{Gal}(K/K) \), then \( f(x) = x \) for all \( x \in K \), or in other words, \( f \) is the identity function, so this is the only element of \( \text{Gal}(K/K) \).

We also state the following useful theorem (try to think about how you would prove this!)

**Theorem 2** If \( L = K(\sqrt[n]{\alpha}) \), where \( \alpha \in K \) and this is any \( n^{th} \) root of \( \alpha \) (i.e. using any \( n^{th} \) root of unity), then \( \text{Gal}(L/K) \) is cyclic.
Definition 3 A polynomial is said to be **solvable in radicals** if there is a formula for each of its roots in terms of rational numbers and addition, subtraction, multiplication, division, and taking $n^{th}$ roots.

**Problem 7** Suppose that $p$ is a polynomial which is irreducible over $\mathbb{Q}$ and solvable in radicals. Let $x$ be a root of $p$.

- Let $K$ be a splitting field for $p$. Show that there is a sequence
  $$\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_{n-1} \subseteq K_n = K$$
  where each $K_j$ is an extension of $K_{j-1}$ by the $n^{th}$ root of an element of $K_{j-1}$. (Hint: Since $p$ is solvable in radicals, $x$ can be written in radicals, so construct $K_1, K_2, \ldots$ in a way that undoes all the radicals in the formula for $x$.)

  **Solution:** Let $K_0 = \mathbb{Q}$, and let $K_1 = \mathbb{Q}(\alpha)$, where $\alpha$ is the innermost radical in the expression for $x$. Then let $K_2 = \mathbb{Q}(\beta)$ for the next outermost radical $\beta$, and so on, until all the radical expressions are adjoined in this way - by definition the final term $K_n \ni x$ so $K_n = K$ is a splitting field.

  For example, the cubic formula gives
  $$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

  We would have, in this case
  $$K_0 = \mathbb{Q}$$
  $$K_1 = \mathbb{Q} \left( \sqrt[3]{\frac{q^2}{4} + \frac{p^3}{27}} \right)$$
  $$K_2 = K_1 \left( \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \right)$$

  Note that, in this case, only one of the cube roots $(u, v)$ is needed, because we have $v = -q - w^3$.

- Use this sequence and Problem 4 to obtain a sequence of normal subgroups of $\text{Gal}(K/\mathbb{Q})$.

  **Solution:** $\{e\} = \text{Gal}(\mathbb{Q}/\mathbb{Q}) \triangleleft \text{Gal}(K_1/\mathbb{Q}) \triangleleft \ldots \triangleleft \text{Gal}(K_n/\mathbb{Q}) = \text{Gal}(K/\mathbb{Q})$

- Conclude that $\text{Gal}(K/\mathbb{Q})$ is solvable.

  **Solution:** By Problem 5, each quotient above is $\text{Gal}(K_{j+1}/\mathbb{Q})/\text{Gal}(K_j/\mathbb{Q}) = \text{Gal}(K_{j+1}/K_j)$. By Theorem 2, each of these is cyclic, so since all cyclic groups are abelian, each quotient in the above sequence is abelian, so that $\text{Gal}(K/\mathbb{Q})$ is solvable.

Problem 7 proves one direction of the famous Abel-Ruffini Theorem. The converse is also true, but is much trickier to prove so we shall not do so this week. To summarize, we have

**Theorem 3 (Abel-Ruffini)** A polynomial $p$ is solvable in radicals if and only if its Galois group is solvable.
Problem 8  
• Using the fact that the cubic formula exists, prove that $S_3$ is solvable.

Solution: By the existence of the cubic formula and the fact that the cubic $x^3 - 2$ (for instance, this is the example from last week) has Galois group $S_3$, $S_3$ is solvable.

• Using the fact that $S_4$ is solvable (see Problem 1), prove that there exists a quartic formula.

Solution: Let $p$ be any quartic. If $p$ is reducible, then it clearly has a formula by the existence of quadratic and cubic formulas. If $p$ is irreducible, then its Galois group $G$ is a subgroup of $S_4$, which is solvable, so by Problem 1 $G$ is solvable, so $p$ is solvable in radicals.

• Can we immediately rule out the existence of a quintic formula? Why or why not?

Solution: No. It might be the case that no irreducible quintic has Galois group $S_5$ or $A_5$.

3 Transitive Subgroups and Quintics

So far we have restricted attention to irreducible polynomials, and it wasn’t entirely clear why. There are a few proofs on this and the previous worksheet which require irreducibility (go back and see how), but the most important application is that it forces a certain property on the Galois group - the Galois group can’t just be any subgroup of $S_n$.

Definition 4 A subgroup $G$ of $S_n$ is transitive if any for two different numbers $1 \leq j, k \leq n$ there exists a permutation $\sigma \in G$ such that $\sigma(j) = k$.

Problem 9 Let $p$ be an irreducible degree $n$ polynomial. Prove that its Galois group is a transitive subgroup of $S_n$. (Hint: If it weren’t transitive, there would be roots $r_j$ and $r_k$ which cannot be mapped to each other by the Galois group. Consider the set of roots which are mapped to from $r_j$, which is now missing some $r_k$, and use this set of roots to create a nontrivial factor of $p$.)

Solution: Suppose it were not transitive, so there exist roots $r_j$ and $r_k$ which are not mapped to each other. Let $r_{j_1}, ..., r_{j_l}$ be the roots which are mapped to from $r_j$, so that this set does not include $r_k$. It is nonempty, since $r_j$ is in the set (it is mapped from $r_j$ by the identity permutation), and it does not contain all the roots, so taking the product $f(x) = (x - r_{j_1})...(x - r_{j_l})$ gives a nonconstant polynomial with a smaller degree than $p$. But since all of the roots of $f$ are roots of $p$, $p$ is divisible by $f$, which contradicts the fact that $p$ is irreducible.
Problem 10  Consider the polynomial \( p(x) = x^5 - 13x - 13 \), and let \( G \) be its Galois group.

- Using Eisenstein’s Criterion (recall from last quarter), show that \( p \) is irreducible over \( \mathbb{Q} \).
  Solution: \( p = 13 \).

- Show that \( G \) contains a transposition (a 2-cycle). (Hint: You may use the fact that \( p \) has exactly three real roots - this can be seen by graphing it.)
  Solution: The transposition is given by complex conjugation, which switches the two non-real roots and fixes the three real roots.

- Show that \( G \) contains all ten transpositions in \( S_5 \). (Hint: Say you have the transposition \( g = (12) \). By transitivity there exists some \( h \) such that \( h(2) = 3 \), so what can \( hgh^{-1} \) possibly be? Repeat this process until you’ve shown that \( (13) \in G \). Then do this again for \( (14), (15) \in G \). Now can you get the other six transpositions in \( G \)?)
  Solution: Without loss of generality, complex conjugation represents the permutation \( g = (12) \). Let \( h \) be some permutation such that \( h(2) = 3 \). When finding \( hgh^{-1} \), \( g \) will only affect \( h(1) \) and \( h(2) \), the latter which is given to be 3 - any other numbers are unaffected by \( g \) and therefore unaffected by \( hgh^{-1} \). So \( hgh^{-1} \) is the transposition which switches 3 with 5 - any other numbers are unaffected by \( g \) and therefore unaffected by \( hgh^{-1} \). If \( h(1) = 1 \), then \( (13) \in G \). If \( h(1) = 2 \), then \( (23)(12)(23) = (13) \in G \). If \( h(1) = 4 \), then we find another permutation \( i \) such that \( i(2) = 5 \), and repeat this argument, eventually finding that \( (13) \in G \) in this case as well (and similarly, also when \( h(1) = 5 \)). Therefore \( (13) \in G \), and a similar argument now shows \( (14) \in G \) and \( (15) \in G \), and a similar argument also shows that since \( (12) \in G \), \( (23), (24), (25) \in G \), and so on for the others.

- Show that the transpositions generate \( S_5 \); that is, every permutation in \( S_5 \) can be written as a product of transpositions. (Hint: Every permutation can be written in cycle notation. Can you write a cycle as a product of transpositions?)
  Solution: Any cycle \((a_1...a_n)\) can be written as \((a_2a_3)...(a_{n-1}a_n)(a_1a_n)\), so any permutation can be written as transpositions by writing each of its cycles this way.

- Conclude that \( p \) is not solvable in radicals, and therefore that there is no quintic formula.
  Solution: The above shows that \( G \) contains every permutation on 5 elements, so \( G \) is \( S_5 \), which is not solvable, so \( p \) is not solvable in radicals by Abel’s Theorem.