Last time

- Cycle type and conjugacy
- Signs and A_n
- A_n is simple for $n \geq 5$

Lemma $S_n = \langle (12), (12\cdots n) \rangle$.

Proof $(i, i+1) = (1\cdots n)^{i+1}(12)(1\cdots n)^{-(i+1)}$, and S_n is generated by the transpositions $(i, i+1)$.

□

Exercise The only elements of order p in S_p are the p-cycles.

Lemma If $\sigma \in S_p$ is any p-cycle and $\tau \in S_p$ any transposition, then $\langle \sigma, \tau \rangle = S_p$

Proof WLOG, $\tau = (1k)$ and $\sigma = (1 \cdots k \cdots)$.

For some $1 \le i \le p-1$, $\sigma^i(1) = k$, and $|\sigma^i| = p$, since $|\sigma^i| \mid |\sigma| = p$. It follows (exercise) that σ^i is a p-cycle, of the form $(1k \cdots)$. Relabeling, we may have $\tau = (12)$, $\sigma^i = (12 \cdots p)$, and

$$\langle \sigma, \tau \rangle = \langle \sigma^i, \tau \rangle = S_p.$$

□

Thm The polynomial $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$ cannot be solved in radicals.

Proof By Eisenstein at $p = 3$, f is irreducible. Thus, if K denotes the splitting field of f, we have $5 \mid [K : \mathbb{Q}] = |G|$, where $G = \mathrm{Gal}(K/\mathbb{Q})$, so G contains an element of order 5 by Cauchy. Numbering the roots of f, we may identify G with a subgroup of S_5. Since the only elements of order 5 in S_5 are the 5-cycles, it follows that G contains a 5-cycle S.

From the table

x	$f(x)$
-2	-17
0	3
1	-2
2	23

and the intermediate value theorem, f has a real root in $(-2,0)$, $(0,1)$, and $(1,2)$. By the mean value theorem, f' has a root between any two roots

of f:

$$f'(c) = \frac{f(b) - f(a)}{b - a} = 0.$$

Therefore, if f had 4 real roots, then $f' = 5x^4 - 6$ would have 3 real roots, hence 4 real roots, but $\sqrt[4]{6/5}\, i \notin \mathbb{R}$. Thus, f has precisely 2 roots in $\mathbb{C} \setminus \mathbb{R}$. Since f has real coefficients, complex conjugation restricts to an automorphism of K, which

necessarily fixes the three real roots and interchanges the two complex roots. Thus, G contains a transposition τ, hence $S_5 = \langle \rho, \tau \rangle \subseteq G$, so $G = S_5$. Since S_5 is not solvable, the claim follows. $\square$

Rmk The argument shows that f is not solvable in radicals if $\deg(f)$ is prime, f has exactly two non-real roots, and f is irreducible.

with more work, one can produce infinitely many examples for every $n \geq 5$. Instead of pursuing this direction, we show that there is no general solution in radicals.

Def The general polynomial of degree n is

$$(x - x_1) \cdots (x - x_n),$$

where the x_i are formal parameters.

By foiling, we have

$$(x-x_1)\cdots(x-x_n) = x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n,$$

where s_i is the ith elementary symmetric function:

$$s_i = \sum_{S \subseteq \{1,\ldots,n\},\ |S|=i} \prod_{s \in S} x_s$$

Ex $s_0 = 1$, $s_1 = x_1 + \cdots + x_n$, $s_n = x_1 \cdots x_n$

Ex For $n=3$, $s_2 = x_1x_2 + x_1x_3 + x_2x_3$.

Def The field of rational functions in n variables $t_1, \dots, t_n$ is the set $F(t_1, \dots, t_n)$ of equivalence classes of expressions of the form P/Q, where P and Q are polynomials in $t_1, \dots, t_n$ with $Q \neq 0$, under the equivalence relation

$$P/Q \sim P'/Q' \iff QP' = Q'P.$$

Exercise $F(t_1, \dots, t_n)$ is a field.

The general polynomial has roots in $F(x_1, \ldots, x_n)$ and coefficients in the subfield $F(s_1, \ldots, s_n)$. The general polynomial being obviously separable, it follows that $F(x_1, \ldots, x_n)$ is a Galois extension of $F(s_1, \ldots, s_n)$.

Prop The degree of this extension is $n!$.

Proof As the splitting field of a degree n polynomial, the degree is at most $n!$.

As the degree is the order of the Galois group, it suffices to show that the Galois group contains a subgroup of order $n!$. But S_n clearly acts on $F(x_1, \dots, x_n)$ by permuting the indices, and this action evidently fixes each s_i. □

Cor $F(x_1, \dots, x_n)^{S_n} = F(s_1, \dots, s_n)$.

Cor The Galois group of the general polynomial of degree n is S_n.

Cor If $\mathrm{char}(F) = 0$, then the general polynomial of degree n is solvable in radicals iff $n \leq 5$.

Loosely speaking, we mean these results as applying to a "generic" polynomial of degree n, i.e., one whose coefficients/roots satisfy no algebraic relations. Thus, it should be viewed as an accident or

a coincidence if a degree ≥ 5 polynomial is solvable in radicals.

We end this course with a very brief look at an important related problem.

Inverse Galois problem Given a finite group G, is G the Galois group of a Galois extension of $\mathbb{Q}$?

This problem is open and considered very difficult.

We will treat the Abelian case of the problem.

Thm Every finite Abelian group is the Galois group of a Galois extension of $\mathbb{Q}$.

Q Which finite Abelian groups are there?

Given an Abelian group A, it is convenient to write A additively:

- group law $a+b$
- unit 0
- inverses $-a$

If A and B are both Abelian, we write their direct product as $A \oplus B := A \times B$, and we refer to this group as their direct sum.
As a reminder, $A \oplus B$ consists of pairs (a,b) with $a \in A$ and $b \in B$, and the group law is

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2).$$

Observation If A is Abelian, any Sylow subgroup is unique.

Prop Let A be finite and Abelian and $\{p_i\}_{i=1}^r$ the distinct primes dividing $|A|$. There is a canonical isomorphism

$$A \cong \bigoplus_{i=1}^{r} P_i,$$

where $P_i \trianglelefteq A$ is the p_i-Sylow subgroup.

Proof For any i, we have

$$P_{i+1} \cap P_1 \cdots P_i = \{1\}$$

by Lagrange. Thus, by induction,

$$P_1 \cdots P_r \cong \bigoplus_{i=1}^{r} P_i,$$

since all subgroups involved are normal.

In particular,

$$|P_1 \cdots P_r| = \left|\bigoplus_{i=1}^{r} P_i\right| = \prod_{i=1}^{r} |P_i| = |A|,$$

and the claim follows. □

Rmk The argument applies to any finite group with unique Sylow subgroups.

Thus, it remains to classify finite Abelian p-groups for each p.

Thm Every finite Abelian p-group is isomorphic to one of the form $\bigoplus_{i=1}^{m} C_{p^{r_i}}$.

Ex Up to isomorphism, C_{p^2} and $C_p \times C_p$ are the only groups of order p^2.

Corollary Any finite Abelian group is isomorphic to a direct sum of cyclic groups of prime power order.

Rk The cyclic factors appearing in such a decomposition are uniquely determined, but the isomorphism is not, nor even are the corresponding subgroups.

Ex $A = C_p \times C_p$, $A = \langle a \rangle \oplus \langle b \rangle$ for any nonzero a and b that are not multiples of each other.

Lemma 1 Let A be a finite Abelian p-group. Then A is cyclic iff A has a unique subgroup of order p.

Proof ($\Longrightarrow$) Exercise.

($\Longleftarrow$) We proceed by induction on $|A|$, the case $|A|=p$ being obvious. For the induction step, consider the function

$$\varphi : A \longrightarrow A$$

$$\varphi(a) = pa.$$

Then φ is a homomorphism whose kernel is the unique subgroup of order p; indeed, any

$a \notin \ker(\varphi)$ generates a subgroup of order p, which must be the unique one. Without loss of generality, $\ker(\varphi) \neq A$, so $\mathrm{im}(\varphi)$ is a nontrivial Abelian p-group of strictly smaller order. By Cauchy's theorem, $\mathrm{im}(\varphi)$ contains a subgroup of order p, which is also a subgroup of A and so must be $\ker(\varphi)$ be uniqueness. By induction, $\mathrm{im}(\varphi) \cong A/\ker(\varphi) = \langle a + \ker(\varphi) \rangle$ for some $a \in A$. We claim that $\langle a \rangle = A$; indeed, $\ker(\varphi) \subseteq \langle a \rangle$ by Cauchy and uniqueness, and any element of A is a multiple of a times an element of $\ker(\varphi)$ by exactly. $\square$