Last Time

**Theorem 45.2:** Let $D$ be a UFD and $F$ its field of quotients.

If $f(x) \in D[x]$ with $\deg f > 0$, and $f(x)$ is irreducible in $D[x]$ then it is irreducible in $F[x]$.

**Corollary 45.28:** If $f(x)$ factors in $D[x]$ then it factors in $F[x]$.

**Proof:** Obvious because $D \subset F$.

(Contrapositive of Theorem Q.E.D.)
Thm 45.29. If $D$ is a UFD, then $D[X]$ is.

Let $D[X]f(x) = g_1(x)g_2(x) \cdots g_m(x)$

where $\deg g_i(x) > 0$ and $m$ maximal.

We know that for $F = \text{field of quotients of } D$

$F[X]$ is UFD.

Each $g_i(x)$ has the form $C_i h_i(x)$

where $C_i \in D$ is the content of $g_i(x)$

and $h_i(x)$ is primitive. Each

$h_i(x)$ is irreducible since $m$ is maximal.
We know that a factorization in \( D[x] \) is equivalent to one in \( F[x] \).

\[ D[x] \text{ is a UFD because } F[x] \text{ is a UFD.} \]

By \( D[\{x_1, x_2, x_3, \ldots, x_n\}] \text{ is a UFD if } \]

\[ D[x_1, x_2] \text{ is a UFD.} \]

Proof by induction on \( n \):

\[ D[\{x_1, \ldots, x_n\}] = D[\{x_1, \ldots, x_{n-1}\}, x_n] \]

- UFD by induction
- UFD by Thm 45.29
Preview of 237

Basic problem: How to solve a polynomial equation \( f(x) = 0 \).

1. High School formula for \( f(x) \) quadratic formulas known for degrees 3 and 4. Galois proved a formula for degree \( \geq 5 \).

2. Suppose \( f(x) \in F[x] \) is irreducible over \( F = \text{field} \).
Then $F[x]/(f(x)) = E$ is called a field.

E.g., $\mathbb{Q}[x]/(x^2+5) = \{ a + b\sqrt{5} : a, b \in \mathbb{Q} \}$ is a field $E$ in called a field extension of $F$.

Consider the set of field automorphisms of $E$ that fix $F$. This is a group of the form $\{ a + b\sqrt{5} \mapsto a - b\sqrt{5} \}$ is a field automorphism.
$(	ext{cos}a)^2 = \text{identity}

We have a gap of order 2.

There are more complicated examples.

In $\mathbb{C}$ we have 3 cube roots of 2:

1. $\sqrt[3]{2} = \text{Re} + \text{Im}

2. $w = -\frac{1}{2} + \frac{\sqrt{3}}{2}

3. $w^3 = 1

Let $E$ be the field obtained from $\mathbb{Q}$ by adjoining $\sqrt[3]{2}$ and $w$.
$E$ has an action of $S_3$, that permutes the 3 cube roots of 2.

Facts about this:

$E^G = \{ x \in E : g(x) = x \text{ for all } g \in S_3 \}$

$= \mathbb{Q}$

For each subgroup $H$ of $G$, we get a subfield $E^H$ of $E$.

There are 4 intermediate subfields:

$H_1, H_2, H_3, H_4$
Under certain hypotheses, there is a 1-1 correspondence between subfields and subgroups. 

FUNDAMENTAL THEOREM OF GALOIS THEORY.
Knowing how to solve \( f(x) = 0 \) [where \( f(x) \in F[x] \) is irreducible] is equivalent to finding the field \( E = F(x_1/x_2) \) associated to \( f(x) \) is a group \( G \), its Galois group.

One way to make field extensions is to adjoin \( \sqrt[n]{a} \) for \( a \in F \), iterate this:

\[ \sqrt{2 + \sqrt{2}} \quad \text{or} \quad \sqrt[3]{\sqrt[3]{5} + \sqrt[3]{5}} \]
Galois proved: 

If $E$ is obtained from $F$ by a sequence of such steps, then $Gal(E/F)$ is solvable.

If $E = F[x]/(f(x))$, then $f(x)$ is solvable by radicals (i.e., you can write a formula for $x$).

Hence Galois group is solvable.

As is simple (not normal, e.g., $\mathbb{Z}/2\mathbb{Z}$)
$\sqrt[5]{5}$ is not solvable.

There are irreducible 5th degree polynomials with Galois group isomorphic to $S_5$. Such a polynomial cannot be solved by radicals.

Other gems

Finite fields. For each prime $p$ and integers $n > 0$, $\mathbb{F}_p^n$ field with $p^n$ elements.
For each $n$ consider
\[ K = \mathbb{Q} \left[ e^{2\pi i / n} \right]. \]
If $n$ is even, $K$ is a $n$th cyclotomic extension of $\mathbb{Q}$.

If $n$ is odd, $K$ is a vector space over $\mathbb{Q}$ of dimension $\phi(n)$ [Euler totient].

The Galois group is \( (\mathbb{Z}/n)^x \).

\[ \prod_{k \mid n, \gcd(k, n) = 1} k \]

Ruler + compass constructions

A number $x \in \mathbb{R}$ can be
constructed with $\mathbb{R} + \mathbb{C}$

$x \in \mathbb{R}$ field obtained from $\mathbb{C}$ by adjoining square roots repeatedly.

e.g. $\cos(\frac{2\pi}{17})$ is such a $x$.

$\cos(\frac{2\pi}{17})$ is not such a $x$.

It is possible to construct a regular 17-gon by $\mathbb{R} + \mathbb{C}$

but not a regular 7-gon.
If \( p \) is a prime of the form \( 2^k \cdot 3^b + 1 \), then there is an origami \( p \)-gon.