Abstract Algebra II: Urbana, Spring 2010.

- Handout survey / introduce self.

Course Overview:

(1) "Nice" rings and factorization.

Ring: Set R with $+, \times$. [$(R,+)$ is a gp, $\times$ is assoc & dist]

Suppose R is commutative, has 1, no zero divisors.

Ex: $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Z}[x]$... [Query for more]

$\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\} \subseteq \mathbb{C}$

$\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b \in \mathbb{Z}\} \subseteq \mathbb{R}$

Any $n \in \mathbb{Z}$ can be written $n = (\pm 1)\overbrace{p_1 \cdots p_k}^{\text{primes}}$

Units in R: those elts with mult. inverses.

Irreducible: if $r = a \cdot b$ then one of a, b is a unit.

Unique factorization: Any $r \in R$ is $= r_1 \cdot r_2 \cdots r_n$, where r_i irreducible, in an essentially unique way.

Ex: $6 = 2 \cdot 3 = 3 \cdot 2 = (-3)(-2) = (-2)(-3)$.

Facts: $\mathbb{Z}[i]$ has unique factorization,

but $\mathbb{Z}[\sqrt{5}i] = \mathbb{Z}[\sqrt{-5}]$ doesn't!

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}) = 1+5 = 6.$$

(2, 3, $1+\sqrt{-5}$, $1-\sqrt{-5}$ all irred (HW))

Motivation: Many elem. facts about number theory can be understood in terms of factoring in certain rings. Eg.

Thm: An odd prime p in $\mathbb{Z}$ is $= a^2+b^2$ (for $a, b \in \mathbb{Z}$) iff $p \equiv 1 \bmod 4$.

[Goes back to the ancient Greeks; "best" understood in terms factorization in $\mathbb{Z}[i]$.]

Euclidean Domain $\Rightarrow$ Principle ideal Domain $\Rightarrow$ Unique Factorization

Aside: Restoring unique factorization leads to ideals = "ideal numbers" introduced to study

Fermat's Last Thm: $a^n + b^n = c^n$

has no solutions for $a, b, c \in \mathbb{Z}$ nonzero + $n \geq 3$.

Proved by Wiles in early 1990s.

(2) Galois Theory.

both fields
↙ ↘
$F \subseteq K$

Broadly, the study of <u>field extensions</u>

<u>Ex</u>: $\mathbb{R} \subseteq \mathbb{C}$, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{C}$

↑ alg. extension, adding roots of a poly.

$\mathbb{Q} \subseteq \mathbb{Q}(\pi)$ focus of Galois theory.

↑ transcendental extension

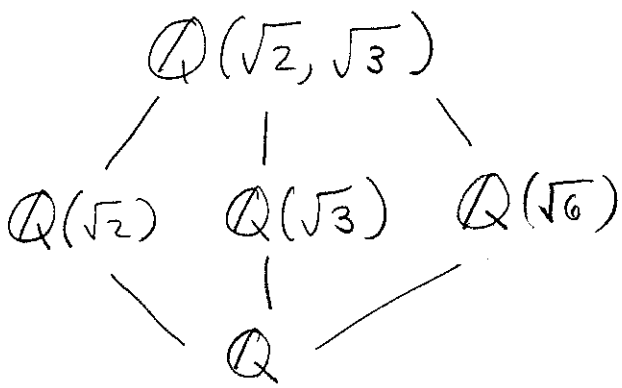
Given $F \subseteq K$ an alg. extension, get associated finite group $Gal(K/F)$.

<u>Ex</u>: $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

When K/F is Galois (whatever that means...)

then <u>subfields</u> $F \subseteq L \subseteq K$ correspond to

<u>subgroups</u> to $Gal(K/F)$.



<u>Query</u>: How many subgroups of $(\mathbb{Z}/2\mathbb{Z})^2$ are there? <u>A.</u> 5

Much of finite group theory was developed to study Galois groups.

Applications: ① Unsolvability of the general quintic.

② Can't trisect an angle $\angle$

Other topics: ⓐ Algebraic geometry?

ⓑ Error correcting codes?

ⓒ Representation theory of finite groups?

Go over syllabus.