Recall

$|G| = p^3$, p odd

G nonab

* $\mathbb{Z}_{p^2} \rtimes \mathbb{Z}_p = \langle x,y \mid x^{p^2} = y^p = 1,\ yxy^{-1} = x^{p+1} \rangle$

* $(\mathbb{Z}_p \times \mathbb{Z}_p) \rtimes \mathbb{Z}_p$ ←

Defn $\|S$ $\mathrm{Heis}(\mathbb{F}_p) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| a,b,c \in \mathbb{F}_p \right\} \leq GL_3(\mathbb{F}_p)$

Rmk nonabelian and (p odd) every elt has order $\leq p$.

What if $p=2$??

Groups $|G| = 8$

Abel: $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

Nonab: D_8, Q_8.

These are all

Pf/ $|G| = 8$ nonab.

① $\exists\, x \in G$ w/ $|x| = 4$.

(rmk $\forall x\ |x| \leq 2 \Rightarrow G$ abel ⇓)

Pick $y \in G \setminus \langle x \rangle$.

$\langle x \rangle \lneq \langle x,y \rangle \leq G$

$4 \qquad 4\,| \qquad = \qquad 8$

i.e. $G = \langle x,y \rangle$.

$yxy^{-1} \in \langle x \rangle = \{\cancel{1}, \cancel{x}, \cancel{x^2}, x^3\}$

① $\langle x \rangle \trianglelefteq G$

② $|yxy^{-1}| = |x| = 4$

③ G non ab $\Rightarrow xy \neq yx$

* $yxy^{-1} = x^3 = x^{-1}$.

Claim $y^2 \in \langle x \rangle = \{1, \cancel{x}, x^2, \cancel{x^3}\}$

Pf/ $\bar{y} \in G/\langle x \rangle \cong \mathbb{Z}_2$

$\Rightarrow \bar{y}^2 = 1 \Rightarrow$ ✓

① $|y| \neq 8$ (b/c else $G \cong \mathbb{Z}_8$)

$\Rightarrow |y^2| \neq 4$

$y^2 = 1$ or x^2

$\langle x,y \mid x^4 = 1 = y^2,\ yxy^{-1} = x^{-1} \rangle = D_8$

$\langle x,y \mid x^4 = 1,\ \underbrace{x^2 = y^2}_{-1},\ yxy^{-1} = x^{-1} \rangle = Q_8$.

Glimpse of shiny new toy: RINGS

Defn A ring is $(R,+,\times)$ a set R w/ $+,\times : R \times R \to R$ s.t. ① $(R,+)$ abelian gp. ② $\times$ assoc. ③ $a \times (b+c) = a \times b + a \times c$.

R is commutative if $\times$ commutes.

Give us nice things

* 0 = identity $(R,+)$

$\Rightarrow 0 \times a = a \times 0 = 0$.

Examples

① $\mathbb{Z}$ a ring.

② $\mathbb{Z}/n\mathbb{Z}$.

③ $\mathbb{R}[x] = \{a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n \mid a_i \in \mathbb{R}\}$

polynomial ring.

$(x+2)(x^2+1) = x^3 + 2x^2 + x + 2$

④ Any field ($\mathbb{Q}$)

⑤ $M_n(\mathbb{R})$

+: Matrix add

×: matrix mult

⑥ X any set.

$C(X) = \{f : X \to \mathbb{R}\}$

$f+g\,(x) = f(x) + g(x)$

(Ring of functions)

Ideals: (like subgroups)

Analogy $M \leq G$ | (if $M \trianglelefteq G$) G/M

Defn R ring $I \subseteq R$ subgroup $(I,+) \leq (R,+)$

I is an ideal if $\forall\, f \in R,\ g \in I,\ fg \in I$

Turns out (R comm)

R/I new ring ($\bar{f}\bar{g} = \overline{fg}$)

& All 4 isom thms hold (w/ necessary mods).

4 avenues of Ring study

① Numbers

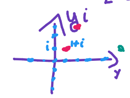
* $\mathbb{Z}$ a ring.

Ideals: $n\mathbb{Z} = \{$mult. ples of $n\}$

$a \in \mathbb{Z}$, $b \in n\mathbb{Z}$ $\Rightarrow ab \in n\mathbb{Z}$. ($n=5$, $a=2$, $b=15$, $ab=30$)

$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}$.

* $\mathbb{Z}[i] \subseteq \mathbb{C}$



"Complex ints"

"Gaussian Integers"

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

$(2+3i)(1-i) = 2 + 3i - 2i - \underbrace{3i^2}_{-3} = 5 + i$

Do we still have prime #s & prime factors? yes

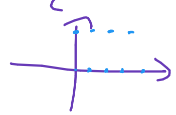
Fun Fact 2 not prime in $\mathbb{Z}[i]$.

$2 = (1+i)(1-i)$

New primes

Prime factorization of 2!!

* $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a,b \in \mathbb{Z}\}$



Lose prime factoriz

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

All "prime" in $\mathbb{Z}[\sqrt{-5}]$.

What happened to prime factorization?

Hint

(prime) numbs ⟷ (prime) ideals

$6 \longleftrightarrow (6)$

$p \cdot q$

$p = (2, 1-\sqrt{-5})$

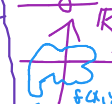
$q = (3, 1+\sqrt{-5})$

↑All this is algebraic number theory.

② Polynomial rings (& their quotients)

Polynomial fn on $\mathbb{R}$ ⟷ $\mathbb{R}[x]$ polys in 1 variable

Magic (geom / ring thry)

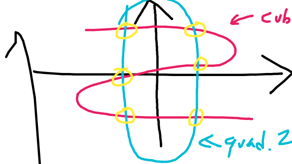


$\mathbb{R}^2 \rightsquigarrow \mathbb{R}[x,y]$ $f \in$

$f(x,y) = 0$

$C \rightsquigarrow$ Fns on C $\mathbb{R}[x,y]/(f)$.

Slogan Curves in $\mathbb{R}^2$ ⟷ Ideals in $\mathbb{R}[x,y]$.



Ring Theory & Alg Geom make this easy (Bezout's Thm).

X space ⟷ $C(X)$ $\{f : X \to \mathbb{R}\}$

$x \in X \rightsquigarrow I_x = \{f \mid f(x) = 0\}$ ↑check ideal

$f,g \in I_x$

$f(x) + g(x) = 0 \Rightarrow f+g \in I_x$

$h \in C(X)$

$hf\,(x) = h(x)f(x) = 0$

$hf \in I_x$.

Slogan Ideals of $C(X)$ recover points of X.

Algebraic Geometry (What I do!!)

③ Fields & Field Extns

Sketch

$\mathbb{Q} \to \mathbb{Q}(\sqrt{2})$ extension

What kind of symmetries does this have.

$G = \mathrm{Gal}(\mathbb{Q}\sqrt{2}/\mathbb{Q}) = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}\sqrt{2})$.

Question Why is there no analog of quadratic formula for deg 5 polys?

A/ $K = \mathbb{Q}$(roots deg 5 pol).

Comput $\mathrm{Gal}(K/\mathbb{Q}) = S_5$ too complicated.