Review.

$$(a, b) \quad = \quad (a) + (b) \text{ in a PID}$$

Why? $(a, b) = (z_1 a + z_2 b)$ is all finite linear combinations of a and b, which is just the same as the thing on the right. Commutivity we sweep under the rug by using that we're in a domain.

Example naming.

Infinite ring w/ zero-divisors: $M_n(F)$
Infinite domain: $\mathbb{Z}$
Irreducible polynomial: $x + 2 \in \mathbb{Z}[x]$.

Definitions.

Faithful: $\sigma_g = \sigma_{g'}$ (also, kernel of homomorphism of group action is identity).
Transitive: Only one orbit.

Examples.

Problem. Count the number of conjugates $(123)(45)$ in S_5.

$\binom{5}{3} 2! = 20$

$$\begin{aligned} \left|\mathcal{O}_{(123)(45)}\right| &= [S_5 : C_{S_5}((123)(45))] \\ 20 &= 120 / \left|C_{S_5}((123)(45))\right| \end{aligned}$$

Problem. Given $G = Z_{450} = \langle x \rangle$:

(1) Count all generators.
(2) Find all elements of order 25.

Part 1: $\phi(450) = 1 \cdot 3 \cdot 2 \cdot 4 \cdot 5 = 120$.
Part 2:

$$|x^a| = \frac{450}{(450, a)} = 25$$

Thus, $(450, a) = 18$. Find one element, then note that G has a unique subgroup of order 25. Thus, there are $\phi(25) = 20$ elements which generate that unique subgroup. We can use this to find all 20 elements of order 18.

Chinese Remainder Theorem. If you want to solve

$$\begin{aligned} x &\equiv a_1 \bmod I \\ x &\equiv a_2 \bmod J \end{aligned}$$

you want $x = a_1 i + a_2 j$. Use Euclidian algorithm.

Manipulating ideals. $I \cap J = IJ$ if and only if I and J are comaximal ($I + J = R$, where R is the ring we're considering).

In a domain, $(a) = (b)$ implies $a = rb$ and $b = sa$ so $a = arb$, and thus that r is a unit.