Definitions you should know:

**Group**

- Abelian gp: structure thin abelian gp
- Finitely generated ab gp
- Normal subgp + quotient gp
- $A_n$ = alternating
- $S_n$ = symmetric gp
- $D_{2n}$ = dihedral gp of order $2n$

(Also known as $D_m$)

Simple gp e.g. $\mathbb{Z}/p\mathbb{Z}$ for $p$ prime

$A_n$ for $n \geq 5$
Center of a group \( Z(G) \)

Commutator subgroup \( [G,G] \)

Lagrange Theorem: If \( H \) is a subgroup of a finite group \( G \), then \( |H| \) (order of \( H \)) divides \( |G| \).

A G-set \( X \) is a set on which the group \( G \) acts, for each \( g \in G \) we get a map \( a(g) : X \to X \) such that \( a(gh) = a(g) \circ a(h) \), \( a(e) = \text{identity map on } X \). Each map \( a(g) \) is 1-1 and onto.
For \( g \in G \), \( X_g = \{ x \in X : a(g)(x) = x \} \)

= elements of \( X \) fixed by \( g \).

For \( H \subset G \), \( X_H = \{ x \in X : a(h)(x) = x \ \forall h \in H \} \)

= \( \bigcap_{h \in H} X_h \)

(also known as \( X^H \)).

For \( x \in X \)

\( C_x = \{ g \in G : a(g)(x) \} \subset G \)

= isotropy group of \( x \).
Stabilizers

To elements of $X$ are in the same orbit if $a(g)(x) = x'$ for some $g \in G$.

When $X$ is finite we can count orbits using Burnside's formula for $G$ finite:

$$\# \text{ of orbits} = \frac{1}{|G|} \sum_{g \in G} |X_g|$$

Symmetry groups for geometric objects:

- Cube or octahedron $S_4 \times A_4$
- Tetrahedron $A_4$
Triangular prism
Dodecahedron or icosahedron
Know about conjugacy classes in $A_n$ and $S_n$. This involves cycle decompositions of permutations.

Sylow Theorems

1) $G$ is a finite group, $p$ is a prime dividing $|G|$
2) $|G| = s p^n$ where $p \nmid s$. 
3) $G$ has a subgroup of order $p^n$
2) Any 2 such subgroups are congruent and hence isomorphic.

3) The # of such subgroups divides $n$ and is $\equiv 1 \mod p$.

Thm 37.7 Let $|G| = pq$ where $p$ and $q$ are distinct primes with $p < q$.

$\Rightarrow$ there is 1 subgroup of order q (hence it is normal).

$\Rightarrow$ if $q \equiv 1 \mod p$ then there are either 1 or $q$ subgroups of order $q$.

$\Rightarrow$ if $q \not\equiv 1 \mod p$ then there is one.
The group of order $p$. 

Con $q \neq 1$ mod $p$, $G \cong C_p$.

More definitions you should know:

- Ring
- Field
- Integral domain (every finite ID is a field)
- Ring of polynomials

Fermat's Little Theorem: For a prime $p$, $n^p \equiv n \mod p$ for any $n \in \mathbb{Z}$.
Reducible and irreducible polynomials.

Example: \[ f(x) = x^4 + ax^3 + bx^2 + 1 \in \mathbb{Z}[x] \]

For which \( a \) and \( b \) is \( f(x) \) irreducible? If \( f(x) = \text{cubic} \circ \text{linear} \), then it has a zero \( n \). \( n \) must divide 1

\( m \) must be \( \pm 1 \)

\[ f(1) = a + b + 2 \]

\[ f(x) = (x-1)g(x) \quad \text{if} \; a + b = -2 \]

\[ f(-1) = 2 - a + b \]

\[ f(-1) = (x+1)g(x) \quad \text{if} \; a - b = 2 \]

If neither condition holds, then
$f(x)$ is either irreducible or a product of two quadratics

If $f(x) = (x^2 + (x+d))(x^2 + (x+f))$

$$= x^4 + (2x + d + f)x^3 + (d+f)(x^2 + (d+f)x + df)$$

$$= x^4 + (2x + d + f)x^3 + (d+f)x^2 + (d+f)x + df$$

$$= x^4 + ax^3 + bx^2 + cx + 1$$

Hence $df = 1$ so $a = b = \pm 1$

$0 = de + cf = \pm (e+c)$ so $e = -c$

$b = d+f + ec = \pm 2 - c^2$

$a = e+c = 0$

CONCLUSION
$b(x)$ is irreducible unless

\[ a + b = -2 \]

or \[ a - b = 2 \]

or \[ a = 0 \] and \[ b = \pm 2 - c^2 \]

Other definitions:

- ideal
- maximal
- prime
- principal

uniquer factorization domain
ring / maximal ideal = field
ring / prime ideal = integral domain

A domain $D$ has a field of quotients $F$

$F = \text{set fractions with numerators } + \text{denominators}$
in \( \mathbb{D} \)

\[
\mathbb{D} = \mathbb{Z} \quad \mathbb{F} = \mathbb{Q}
\]

\[
\mathbb{D} = \mathbb{Z}[x] \quad \mathbb{F} = \text{rational functions}
\]

where \( p(x), q(x) \in \mathbb{Z}[x] \)
g(x) ≠ 0