FINAL EXAM : BASIC DEFINITIONS AND THEOREMS

1. A map $f : X \to Y$ is injective, if it satisfies $f(x) = f(x') \Rightarrow x = x'$ for all $x.x' \in X$.
2. A map $f : X \to Y$ is surjective, if for all $y \in Y$ there exists $x \in X$ such that $f(x) = y$.
3. A map $f : X \to Y$ is bijective if it is both injective and surjective.
4. Bijective maps have inverses.
5. An equivalence relation on a set X is a binary relation which is reflexive, symmetric and transitive.
6. The equivalence classes of an equivalence relation on a set X give a partition of X into disjoint subsets.
7. The Well-ordering property says: Every non-empty subset of $\mathbb{N}$ has a least element.
8. A positive integer p is a prime number, if $p > 1$, and the only divisors of p are 1 and p.
9. Every positive integer n is a product of primes, and this decomposition is unique up to reordering.
10. If $a, b \in \mathbb{Z}$ and not both 0, then the $\gcd(a, b)$ is a positive integer d, such that every common divisor of a and b also divides d.
11. If $d = \gcd(a, b)$, then there exists $x, y \in \mathbb{Z}$ such that $d = ax + by$ (Bezout identity).
12. Two integers a, b are said to be co-prime if $\gcd(a, b) = 1$.
13. Groups: A group G is a set with a binary operation which is associative, has an identity and such that every element has an inverse.
14. The order of a group G is the cardinality of its underlying set. The order of an element $a \in G$ is the least positive number m such that $a^m = e$.
15. A subset $H \subset G$ is a subgroup if $e \in H$, and H is closed under the group operation and taking inverses.
16. A left (right) coset of a subgroup $H \subset G$, is a subset of the form gH (resp. Hg).
17. (Lagrange Theorem). If G is a finite group and H a subgroup, then $|H|$ divides $|G|$.
18. (Corollaries to Lagrange Theorem) Suppose G is a finite group.
    (a) If $g \in G$, then $o(g)$ divides $|G|$.
    (b) $g^{o(g)} = e$ for every $g \in G$
19. If G is a group and $g \in G$, the cyclic subgroup generated by g is the subgroup $\{g^i \mid i \in \mathbb{Z}\}$ and is denoted by $\langle g \rangle$.

20. The cylic group of order n is denoted Z_n and is the additive group of congruence classes mod n.
21. The group Z_n^* is the multiplicative group of congruences classes modulo n of numbers which are co-prime to n.
22. The group $\mathrm{GL}(n, \mathbb{R})$ is the multiplicative group of $n \times n$ invertible matrices with entries in $\mathbb{R}$.
23. The group $\mathrm{SL}(n, \mathbb{R})$ is the multiplicative group of $n \times n$ invertible matrices with entries in $\mathbb{R}$ having determinant equal to 1.
24. A map $f : G \to H$ between two groups, is a group homomorphism if it satisfies $f(gg') = f(g)f(g')$ and $f(g^{-1}) = (f(g)^{-1}$ for all $g, g' \in G$. A group homomorphism is an isomorphism if it is bijective.
25. Two groups G, G' are said to be isomorphic if there exists an isomorphism between them.
26. A subgroup N of a group G is a *normal* subgroup if $gNg^{-1} \subset N$ for all $g \in G$.
27. (First isomorphism theorem) If $f : G \to H$ is a group homomorphism, then $\mathrm{Im}(f)$ is isomorphic to $G/\mathrm{ker}(f)$.
28. (Group acting on a set). An action of a group G on a set X is a group homomorphism $G \to S_X$ (where S_X is the group of bijections of X to itself).
29. For a group G acting on a set X, the *orbit* of an element $x \in X$ is defined as $\mathrm{orbit}(x) = G \cdot x$. The *stabilizer* G_x of x is the subgroup of G defined by $G_x = \{g \in G \mid g \cdot x = x\}$.
30. (Orbit stabilizer formula). $|\mathrm{orbit}(x)| = [G : G_x]$.
31. (Burnside)
$$\text{The number of orbits } = \frac{1}{|G|} \sum_{g \in G} |X^g|,$$
where $X^g = \{x \in X \mid g \cdot x = x\}$.
32. (The class equation)
$$|G| = |Z(G)| + \sum_{x \in C \setminus Z(G)} [G : G_x],$$
where C is a subset of G containing exactly one element from each conjugacy class.
33. An ideal I of a commutative ring R is an additive subgroup satisfying the property that for each $r \in R, x \in I$, $rx \in I$.
34. An ideal is principal if it is generated by one element.
35. An ideal P is prime if it satisfies the property that $ab \in P$ implies either $a \in P$ or $b \in P$.
36. A maximal ideal M in a commutative ring R is a non-zero ideal such that $M \neq R$, and for any ideal I, $M \subset I$ implies either $I = M$ or $I = R$.

37. An integral domain is a commutative ring with no zero divisors.
38. An integral domain in which every non-zero element has a multiplicative inverse is a field.
39. An integral domain in which every ideal is principal is called a principal ideal domain (PID).