CS21001 Discrete Structures

Tutorial 10

---

1. Solve the congruence $x^2 \equiv 1 \pmod{385}$.

2. Let $n_1, n_2, \ldots, n_t$ be t moduli, not necessarily mutually coprime. Prove the t congruences $x \equiv a_i \pmod{n_i}$ for $i = 1, 2, \ldots, t$ are simultaneously solvable if and only if $\gcd(n_i, n_j)$ divides $a_i - a_j$ for all i, j with $i \neq j$.

3. Let $f : R \to S$ be an isomorphism of rings. Prove that $f^{-1} : S \to R$ is again an isomorphism of rings.

4. Let F, K be fields, and $\phi : F \to K$ a non-zero homomorphism. Prove that ϕ is injective.

5. [*Quotient rings*] Let R be a ring, and let I be an ideal of R. Define a relation $\equiv$ on R as $a \equiv b$ if and only if $a - b \in I$.

(a) Prove that $\equiv$ is an equivalence relation.
(b) Let R/I denote the set of equivalence classes of $\equiv$. Define two operations on R/I as $[a] + [b] = [a+b]$ and $[a][b] = [ab]$. Prove that these operations are well-defined.
(c) Show that R/I is a ring under these two operations.
(d) What are R/I in the two special cases $I = \{0\}$ and $I = R$?
(e) Argue that $\mathbb{Z}/n\mathbb{Z}$ is essentially the same as $\mathbb{Z}_n$.

6. [*First isomorphism theorem*] Let $f : R \to S$ be a ring homomorphism. Prove that $R/\ker(f) \cong f(R)$.

7. Let R be a commutative ring with identity, and I an ideal of R. Prove that:

(a) R/I is an integral domain if and only if I is a prime ideal.
(b) R/I is a field if and only if I is a maximal ideal.

8. Let F be a field, and $f(x)$ a non-constant polynomial of $F[x]$. Consider the ideal $I = \{f(x)g(x) \mid g(x) \in F[x]\}$. Prove that the quotient ring $F[x]/I$ is a field if and only if $f(x)$ is irreducible (over F).

9. Let $(G, \circ)$ be a group with identity e. An element $e_L \in G$ is called a *left identity* of G if $e_L \circ a = a$ for all $a \in G$. Likewise, an element $e_R \in G$ is called a *right identity* of G if $a \circ e_R = a$ for all $a \in G$. Prove that any left identity e_L and any right identity e_R of G satisfy $e_L = e_R = e$.

10. Define an operation $\circ$ on $G = \mathbb{R}^* \times \mathbb{R}$ as $(a, b) \circ (c, d) = (ac, bc + d)$. Prove that $(G, \circ)$ is a non-abelian group.

11. Let G be a multiplicative group. Prove that:

(a) $(a^{-1})^{-1} = a$.
(b) $(ab)^{-1} = b^{-1}a^{-1}$ for all $a, b \in G$.

12. Let G be a multiplicative group. Prove that the following conditions are equivalent.

(1) G is abelian.
(2) $(ab)^2 = a^2b^2$ for all $a, b \in G$.
(3) $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$.
(4) The function $f : G \to G$ taking $a \mapsto a^{-1}$ is an isomorphism.

13. Let G be a (multiplicative) group, and H, K subgroups of G. Prove that:

(a) $H \cap K$ is a subgroup of G.
(b) $H \cup K$ need not be a subgroup of G.
(c) $H \cup K$ is a subgroup of G if and only if $H \subseteq K$ or $K \subseteq H$.
(d) Define $HK = \{hk \mid h \in H,\ k \in K\}$. Define KH analogously. Prove that HK is a subgroup of G if and only if $HK = KH$.

14. Let $f : G \to H$ be a surjective group homomorphism. Prove that if G is abelian, then H is abelian too.

15. Let $n \in \mathbb{N}$. Show that the only group homomorphism $\mathbb{Z}_n \to \mathbb{Z}$ is the zero map.

16. If $f : G \to H$ is a group isomorphism, prove that $f^{-1} : H \to G$ is again a group isomorphism.

17. Let G be a group. Let $\operatorname{Aut} G$ denote the set of all automorphisms of G. Prove that $\operatorname{Aut} G$ is a group under function composition.

18. Prove that $\operatorname{Aut} \mathbb{Z}_n \cong \mathbb{Z}_n^*$.

19. Let p be a prime. Prove that $\operatorname{Aut} \mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}^*$.

20. Let G be a multiplicative abelian group with identity e, and let H, K be subgroups of G satisfying $H \cap K = \{e\}$. The *internal direct product* of H and K is defined as $HK = \{hk \mid h \in H,\ k \in K\}$. For additive groups, we talk about the *internal direct sums* of subgroups.

(a) Show that $\mathbb{Z}_{15}$ is the internal direct sum of $\{0, 3, 6, 9, 12\}$ and $\{0, 5, 10\}$.
(b) Show that $\mathbb{Z}_{15}^*$ is the internal direct product of $\{1, 11\}$ and $\{1, 4, 7, 13\}$.
(c) Prove that $HK = G$ if and only if $G \cong H \times K$. (That is, internal and external direct products are essentially the same.)

21. Let G be a multiplicative group, and $a \in G$.

(a) Define the *centralizer* of a as $C(a) = \{b \in G \mid ab = ba\}$. Prove that $C(a)$ is a subgroup of G. What is $C(a)$ if G is Abelian?
(b) Two elements $a, b \in G$ are said to be *conjugate* (to one another), denoted $a \sim b$, if $b = xax^{-1}$ for some $x \in G$. Prove that conjugacy is an equivalence relation on G.
(c) Prove that if $a \sim b$, then $\operatorname{ord}(a) = \operatorname{ord}(b)$.
(d) For any fixed $x \in G$, define the map $f : G \to G$ as $a \mapsto xax^{-1}$. Prove that f is an automorphism pf G.

22. Let G be a multiplicative group. The *center* of G is defined as $Z(G) = \bigcap\limits_{a \in G} C(a)$.

(a) Argue that $Z(G) = \{a \in G \mid ab = ba \text{ for all } b \in G\}$.
(b) Prove that $Z(G)$ is a subgroup of G.
(c) Prove that the automorphism of Part (d) of the last exercise is the identity map if and only if $x \in Z(G)$.

23. Prove that $Z(SL_2(\mathbb{R})) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{R},\ a \neq 0 \right\}$, where $SL_2(\mathbb{R})$ is the group of all 2×2 invertible matrices with entries from $\mathbb{R}$ under the operation of matrix multiplication.

24. Let G be a multiplicative group, and H a subgroup of G. Prove that the following conditions are equivalent.

(1) $ab \in H$ if and only if $ba \in H$ for all $a, b \in G$.
(2) $aH = Ha$ for all $a \in G$.
(3) $H = aHa^{-1}$ for all $a \in G$.
(4) $(aH)(bH) = abH$ for all $a, b \in G$.

If H satisfies any (and so all) of these equivalent conditions, it is called a *normal subgroup* of G. We often write this as $H \lhd G$.

25. **(a)** Prove that the trivial subgroups $\{e\}$ and G of G are normal.
(b) If G is abelian, prove that every subgroup of G is normal.
(c) Prove that the center $Z(G)$ of any group G is a normal subgroup of G.
(d) Give an example of a non-normal subgroup.

26. [*Quotient groups*] Let G be a (multiplicative) group, and H a normal subgroup of G. Define a relation $\equiv$ on G as $a \equiv b$ if and only if $a^{-1}b \in H$.

(a) Prove that $\equiv$ is an equivalence relation.
(b) Let G/H denote the set of equivalence classes of $\equiv$. Define multiplication on G/H as $[a][b] = [ab]$. Prove that this operation is well-defined.
(c) Prove that G/H is a group under this operation.

27. [*First isomorphism theorem*] Let $f : G \to H$ be a group homomorphism. Define the *kernel* of f as $\ker(f) = \{a \in G \mid f(a) = e_H\}$. Prove that $\ker(f)$ is a normal subgroup of G, $f(G)$ is a subgroup of H, and $G/\ker(f) \cong f(G)$.