CS21201 Discrete Structures
Practice and tutorial problems

Algebraic Structures

1. Let A = Z × Z, and λ a fixed (constant) positive integer. Define two operations ⊕ and ⊙ on A as (a, b) ⊕ (c, d) = (a + c, b + d), (a, b) ⊙ (c, d) = (ad + bc, bd + λ ac). Show that A is a commutative ring with identity under these two operations. You do not have to verify the ring axioms, but only mention the additive and multiplicative identities in A (no need to prove their identity properties). Also, prove that A is an integral domain if and only if λ is not a perfect square.
2. Let R be a ring, and S,T1, T2 subrings of R. If S ⊆ T1 ∪ T2, prove that S ⊆ T1 or S ⊆ T2.
3. Let G be a group. If $(ab)^3 = a^3b^3$ and $(ab)^5 = a^5b^5$ for all a,b in G, prove that G is abelian.
4. Let H and K be two subgroups of a (multiplicative) group G. Define HK = {hk | h ∈ H, k ∈ K}. Define KH analogously. Prove that HK is a subgroup of G if and only if HK = KH.

Practice Problems

5. Let G be a group, and H = {a ∈ G | ag = ga for all g ∈ G}. Prove that H is a subgroup of G.
6. Let G be a group, and H be a subgroup of G. For x, y ∈ G, define a relation R by "xRy if and only if xy^{-1} ∈H". Prove that R is an equivalence relation.
7. Let (G, o) and (H, *) be groups. The binary operation **.** is defined on G × H by $(g_1, h_1).(g_2, h_2) = (g_1 o\, g_2, h_1 * h_2)$. Prove that (G × H, **.**) is a group.
8. Let R be the set of all functions Z → Z. For f,g ∈ R, define (f + g)(n) = f(n)+g(n) and (f g)(n) = f(g(n)) for all n ∈ Z. Prove/Disprove: R is a ring under these two operations.
9. Let R be a commutative ring with identity, and R[x] the set of univariate polynomials with coefficients from R. Define the addition and multiplication of polynomials in the usual way.
   (a) Prove that R[x] is a ring.
   (b) Prove that R[x] is an integral domain if and only if R is an integral domain.

10.

Consider the following set of 2×2 matrices with real entries: $\mathbb{A} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| \, a, b \in \mathbb{R} \right\}$.

(a) Prove that $\mathbb{A}$ is a commutative ring with identity.

(b) Prove that A is isomorphic to the ring C of complex numbers.

11. Let (G, ◦) be a group, and c a fixed element of G. Define a binary operation ∗ on G by a ∗ b = a ◦ c ◦ b for all a, b ∈ G. Prove that (G, ∗) is a group, clearly showing that all the properties of a group are satisfied.