Math 453 Abstract Algebra Samplefinal
Solns to some Ring problems

Rings

1. Let R be a ring.

   (a) Suppose $a \in R$. Shown that $S = \{x \in R : ax = xa\}$ is a subring of R.

   (b) If R is commutative then show that the set defined as $\{x \in R : ax = 0\}$ is an ideal of R.

2. Let R be a ring. Prove that R is commutative if and only if $a^2 - b^2 = (a + b)(a - b)$ for all $a, b \in R$.

   Soln: $(a + b)(a - b) = a^2 + ba - ab - b^2$ Then for any a, b we have

   $a^2 - b^2 = (a + b)(a - b)$ iff $a^2 - b^2 = a^2 + ba - ab - b^2$ iff $ba = ab$

3. Find the characteristic of $Z_n \oplus Z_m$, the zero divisors and the units in the ring .

   Soln: The ring has unity $(1, 1)$ (check). Then the characteistic is the smallest positive integer k such that $k(1, 1) = (kmodn, kmodm) = 0$. whicm means $m|k$, and $n|k$, and thus $lcm(m, n)|k$. The smallest k with this property is $lcm(m, n)$ and this is the characteristic of $Z_n \oplus Z_m$

4. Let R_1 and R_2 be rings, and $\phi : R_1 \to R_2$ be a ring homomorphism such that $\phi(R) \neq \{0'\}$.

   (a) Show that if R_1 has unity and R_2 has no zero-divisors, then $\phi(1)$ is a unity of R_2.

   (b) Show that the conclusion in (a) may fail if R_2 has zero-divisors.

   Soln

   (a) $\phi(1) = \phi(1 \cdot 1) = \phi(1) \cdot \phi(1)$.

   Now for any $a \in R_2$, we have $\phi(1)a = \phi(1) \cdot \phi(1)a$ which implies $\phi(1)a - \phi(1) \cdot \phi(1)a = 0$.

   $\phi(1)(a - \phi(1)a) = 0$. If $\phi(1) = 0$ then for any $a \in R$ we have $\phi(a) = \phi(1 \cdot a) = \phi(1)\phi(a) = 0 \cdot \phi(a) = 0$, and $\phi(R) = 0$, A contradiction. Thus $\phi(1) \neq 0$ and since R_2 has no zero divisors $a - \phi(1)a = 0$. Thus $\phi(1)a = a$ for any $a \in R_2$. Similarly consider $a\phi(1) = a\phi(1) \cdot \phi(1)$ to prove $a\phi(1)a = a$ for any $a \in R_2$. Thus implies that that $\phi(1)$ is a unity of R_2.

   (b) similar

5. Let R_1 and R_2 be rings, and $\phi : R_1 \to R_2$ be a ring homomorphism.

   (a) Show that if A is an ideal of R_1, then $\phi(A)$ is an ideal of $\phi(R_1)$.

   (b) Show that if B is an ideal of R_2, then $\phi^{-1}(B)$ is an ideal of R_1.

   Solution:

   (a) Any element of $\phi(A)$ is of the form $\phi(a)$, where $a \in A$. Similarly any element of $\phi(R_1)$ is of the form $\phi(c)$, where $c \in R_1$. For any elements $\phi(a), \phi(b) \in \phi(A)$ with $a, b \in A$, we have $\phi(a) - \phi(b) = \phi(a - b)$. Since A is an ideal if $a, b \in A$ then $a - b \in A$. Thus

$\phi(a) - \phi(b) = \phi(a-b) \in \phi(A)$. Likewise for any elements $\phi(a), \in \phi(A)$, and $\phi(c), \in \phi(R_1)$, with $a \in A$, $c \in R_1$, we have and $\phi(c) \cdot \phi(a) = \phi(c \cdot a)$, and $\phi(a) \cdot \phi(c) = \phi(a \cdot c)$. Since A is an ideal if $a \in A$ and $c \in R_1$ then ac and ca are in R_1 . Thus $\phi(c)\phi(a) = \phi(ca) \in \phi(R_1)$, and $\phi(a) \cdot \phi(c) = \phi(a \cdot c) \in \phi(R_1)$.

6. Let D be an integral domain.

   Show that a nonconstant polynomial in $D[x]$ has no multiplicative inverse.

7. Find an multiplicative inverse of $2x+1$ in $\mathbb{Z}_4[x]$. Is the inverse unique?

   Soln: $(1+2x)^2 = 1+4x+4x^2 = 1$. The inverse of $2x+1$ is $2x+1$.

8. (a) Write $x^3+6 \in \mathbb{Z}_7[x]$ as a product of irreducible polynomials over $\mathbb{Z}_7$.

   (b) Write $x^3+x^2+x+1 \in \mathbb{Z}_2[x]$ as a product of irreducible polynomials over $\mathbb{Z}_2$.

   (c) Write $x^3+4 \in \mathbb{Z}_5[x]$ as a product of irreducible polynomials over $\mathbb{Z}_5$.

   Soln (a) Find a root 1 and divide the polynomial by $(x-1)$. Then check for roots and repeat the process. If there are no roots then the resulting factors are irreducible. Otherwise divide by the factor $x-a$, where a is a root.

9. Determine which of the polynomials $f(x)$ below is (are) irreducible over $\mathbb{Q}$. (Mod p test, Eisenstein, existence of roots, and long division)

   (a) x^3+x^2+x+1.

   (b) x^4+x+1.

   (c) x^5+5x^2+1.

   (d) $x^5+5x+15$

   Solution (a) Has a root and thus it is reducible

   (b) (c) Consider the polynomials $f(x)$ mod 2, and show that they have the same degree and are irreducible. Consider their possible irreducuble factor $g(x)$. Its degree is less than or equal to 2. If the degree of $g(x)$ is one show that the polynomial $f(x)$ has a root (which is not the cas- Show).

   If the degree of $g(x)$ is 2 then $g(x) = x^2+x+1$ (show!) and use long division to prove that the reduction of $f(x)$ does not divide $g(x)$.

   (d) Eisenstein for $p=5$.

10. Show that $f(x) = x^3+2x+1 \in \mathbb{Z}_3[x]$ is irreducible. Let $\mathbb{F} = \mathbb{Z}_3[x]/A$ with $A = \langle f(x) \rangle$.

    (a) Let $a = (x^2+1)+A$ and $b = (x^2+x+1)+A$ in $\mathbb{F}$. Compute ab, a^2.

    (b) Find an element in $\mathbb{F}$ satisfying $y^3+2y+1=0$.

    Soln: Prove that $f(x)$ has no roots and thus it is irreducible (degree 3).

    (a) Multiply elements ab, a^2,, and then apply long division by $f(x)$ and take the remainders.

Groups

1. Find $gcd(123, 745)$

2. Find the inverse of 23 in $\mathbb{Z}_{71}$

3. Find the last two digits of 15^{100}.

4. Prove that the set of all 2×2 matrices with entries from $\mathbb{R}$ and determinant 1 is a group under matrix multiplication.

5. Prove that a group G is Abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$.

6. Suppose a and b are elements in a group such that $|a| = 4, |b| = 2$, and $a^3b = ba$. Find $|ab|$.

7. Determine the subgroup lattice of $\mathbb{Z}_{12}$.

8. let G be a group and let a be an element of G.
   (1) if $a^{12} = e$, what can we say about the order of a?
   (2) if $a^m = e$, what can we say about the order of a?
   (3) suppose that $|G| = 24$ and that G is cyclic. If $a^8 \neq e$ and $a^{12} \neq e$, show that $G = \langle a \rangle$.

9. Consider $\sigma = (13256)(23)(46512)$.

   (a) Express σ as a product of disjoint cycles.

   (b) Find its order.

   (c) Find σ^{32}.

10. Let G be a group. Show that $\phi : G \to G$ defined by $\phi(g) = g^{-1}$ is an isomorphism if and only if G is Abelian.

11. Let G be a group with $|G| = pq$, where p, q are primes. Prove that every proper subgroup of G is cyclic.

12. Find all generators for $\mathbb{Z}/49\mathbb{Z}$.

13. Find the number of generators for $\mathbb{Z}/49000\mathbb{Z}$.

14. Let G be a finite group,and $H \leq K \leq G$. Prove that $|G : H| = |G : K||K : H|$.

15. (a) Prove that $\mathbb{R} \oplus \mathbb{R}$ under addition in each component is isomorphic to $\mathbb{C}$.

    (b) Prove that $\mathbb{R}^* \oplus \mathbb{R}^*$ under multiplication in each component is not isomorphic to $\mathbb{C}^*$.

    (c) Show that there is no isomorphism from $\mathbb{Z}_8 \oplus \mathbb{Z}_2 \to Z_4 \oplus Z_4$.

16. Prove that if $H \leq G$ and $|G : H| = 2$, then H is normal.

17. Find the centralizers of the elements r, r^3, sr in D_{12}

18. Show that if $f : G \to H$ is a surjective homomorphism and $K \lhd G$ then $f(K) \lhd H$.

19. Show that intersection $H_1 \cap H_2$ of two subgroups $H_1, H_2 \le G$. Show that if $H_1 \lhd G$ then $H_1 \cap H_2 \lhd H_2$.

20. Let G be a group and $S \subset G$ be its subset. Show that

$$H = \{g \in G : gx = xg, \quad for \quad any \quad x \in S\}$$

is a subgroup of G. (Hint: Prove the fact that $bb^{-1}x = bxb^{-1}$ for $b \in H$ and $x \in S$ and use cancellation.)

21. Let $G = \mathbb{Z}_4 \oplus \mathbb{Z}_2$, $H = \langle (2,1) \rangle$ and $K = \langle (2,0) \rangle$. Show that G/H is not isomorphic to G/K.

22. Let G be a finite group, and H be a normal subgroup of G.

    (a) Show that the order of aH in G/H must divide the order of a in G.

    (b) Show that it is possible that $aH = bH$, but $|a| \neq |b|$.

23. Suppose that $N \lhd G$ and $|G/N| = m$, show that $x^m \in N$ for all $x \in G$.

24. For each pair of positive integer m and n, show that the map from $\mathbb{Z} \to \mathbb{Z}_m \oplus \mathbb{Z}_n$ defined by $x \mapsto (x \bmod \text{m}, x \bmod \text{n})$ is a homorphism. Find its kernel.

25. How many (group) homomorphisms are there from $\mathbb{Z}_{20}$ onto $\mathbb{Z}_8$. How many are there to Z_8?

26. Prove that $\phi : \mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z}$ by $\phi(a,b) = a - b$ is a homomorphism. Determine the kernel.

27. Let G be the group of nonzero real numbers under multiplication. Suppose r is a positive integer. Show that $x \mapsto x^r$ is a homomorphism. Determine the kernel, and determine r so that the map is an isomorphism.

28. (a) Determine all (group) homomorphisms from $\mathbb{Z}_n$ to itself

    (b) Determine all (group) homomorphisms from $\mathbb{Z}_{30}$ to itself with kernel $3\mathbb{Z}_{30}$.