HW 12 - MATH403

Danesh Sivakumar

May 6th, 2022

Problem 1

Let $G = \langle a \rangle$ be a group of order 46. Classify the elements according to their order starting with the identity. Bunch the elements of the same order together.

Proof. We proceed by using the formula

$$\left|a^k\right| = \frac{n}{\gcd(n,k)}$$

given that $|a| = n = 46$ and $1 \leq k \leq 46$. Also, the order of an element always divides the order of the group by Lagrange's theorem, so it suffices to consider only the divisors of 46. Furthermore, observe that 46 is the product of two primes 23 and 2, meaning that $\gcd(46,k) = 2$ where $1 \leq k \leq 45$ is even and $\gcd(46,l) = 1$ where $1 \leq l \leq 45$ is odd and $l \neq 23$. Thus we have:

$$\text{Elements of order 1: } e$$

$$\text{Elements of order 2: } a^{23}$$

$$\text{Elements of order 23: } a^2, a^4, a^6, a^8, a^{10}, a^{12}, a^{14}, a^{16}, a^{18}, a^{20}, a^{22}, a^{24},$$
$$a^{26}, a^{28}, a^{30}, a^{32}, a^{34}, a^{36}, a^{38}, a^{40}, a^{42}, a^{44}$$

$$\text{Elements of order 46: } a, a^3, a^5, a^7, a^9, a^{11}, a^{13}, a^{15}, a^{17}, a^{19}, a^{21},$$
$$a^{25}, a^{27}, a^{29}, a^{31}, a^{33}, a^{35}, a^{37}, a^{39}, a^{41}, a^{43}, a^{45}$$

This checks out, because there are $\phi(d)$ elements of order d for every positive divisor d of 46, as per the Fundamental Theorem of Cyclic Groups. □

Problem 2

In any finite group G, show that the number of non-identity elements satisfying the equation $x^5 = e$ is a multiple of 4.

Proof. Observe that because $x^5 = e$, it follows that the order of x divides 5. But since x is not the identity, it follows that the order of x is 5. By a theorem covered in class, we have that the number of elements of order 5 in G is a multiple of $\phi(5) = 4$.

□

Problem 3

1. Find five distinct subgroups of order 12 in S_5

2. Is the subgroup $\langle(12345)\rangle$ of S_5 normal? Why or why not?

Proof.

1. We construct each subgroup by fixing an element, and permuting each of the other elements; this works because the order of A_4 is 12. To this end, let H_n be the subgroup obtained by fixing n and permuting all other elements with the actions of A_4:

   (a) $H_1 =$ actions of A_4 on the set $\{2, 3, 4, 5\}$

   (b) $H_2 =$ actions of A_4 on the set $\{1, 3, 4, 5\}$

   (c) $H_3 =$ actions of A_4 on the set $\{1, 2, 4, 5\}$

   (d) $H_4 =$ actions of A_4 on the set $\{1, 2, 3, 5\}$

   (e) $H_5 =$ actions of A_4 on the set $\{1, 2, 3, 4\}$

   These are each indeed subgroups, because they are closed and contain inverses by virtue of A_4 being a group, and each $H_n \subseteq S_5$

2. No, the subgroup is not normal; observe that

$$\langle(12345)\rangle = \{(12345), (13524), (14253), (15432), \epsilon\}$$

   but $(12)(12345)(12) = (13452) \notin \langle(12345)\rangle$.

□

Problem 4

Prove directly that if $G/Z(G)$ is cyclic, then G is Abelian.

Proof. We must show that if $G/Z(G)$ is cyclic, it follows that $Z(G) = G$, meaning that the only element of the factor group $G/Z(G)$ is $Z(G)$. Because $G/Z(G)$ is cyclic, it follows that $G/Z(G) = \langle gZ(g)\rangle$ for some $g \in G$. Now let $a \in G$ be arbitrary. It follows that $aZ(G) = (gZ(G))^i = g^i Z(G)$, which means that $a = g^i z$ for some $z \in Z(G)$. But observe that $z \in C(g)$ and $g^i \in C(g)$, meaning that $a = g^i z \in C(g)$. But since a was arbitrary, this means that every element is in $C(g)$; this means that g commutes with every element in G, meaning $g \in Z(G)$. Thus we conclude that $G/Z(G) = Z(G)$ and thus $G = Z(G)$ so that G is Abelian. □

Problem 5

Let K be a p-Sylow subgroup of a finite group G for some prime p and let $N(K)$ be the normalizer of K. If an element x of $N(K)$ has order a power of p, show that x is in K.

Proof. Observe that K is normal in $N(K)$. This means that K is the only p-Sylow subgroup of $N(K)$; this is because K is normal in $N(K)$ and by Sylow's Second Theorem, we have that K is the unique p-Sylow subgroup of $N(K)$. Now consider the subgroup generated by x, which has order p^k for some integer k; by definition, this is a p subgroup of $N(K)$. However, there is only one p-Sylow subgroup of $N(K)$, which is K itself, meaing that $\langle x \rangle$ must be contained in K; thus $x \in K$ because every p subgroup is contained within the p-Sylow subgroup. □

Problem 6

Let a be an element of order five. Show that $C(a) = C(a^3)$.

Proof. We must show that (1) $C(a) \subseteq C(a^3)$ and (2) $C(a^3) \subseteq C(a)$. To prove (1), suppose that $b \in C(a)$. Then $ab = ba$, so that

$$a^3 b = aaab = aaba = abaa = baaa = ba^3$$

showing that $b \in C(a^3)$, proving (1). To prove (2), suppose that $b \in C(a^3)$. Then $a^3 b = ba^3$; noting that because $|a| = 5 \implies a^5 = e$, observe

$$ab = a^5 ab = a^6 b = a^3 a^3 b = a^3 ba^3 = ba^3 a^3 = ba^6 = baa^5 = ba$$

showing that $b \in C(a)$, proving (2). Since $C(a) \subseteq C(a^3)$ and $C(a^3) \subseteq C(a)$, it follows that $C(a) = C(a^3)$. □

Problem 7

Prove directly that the ring $\mathbb{Z}[x]$ is an integral domain.

Proof. It suffices to show that $\mathbb{Z}[x]$ is a commutative ring that has no zero divisors. To this end, we will show that given $a, b \in \mathbb{Z}[x]$ with $ab = 0$, it follows that $a = 0$ or $b = 0$. Because a is a polynomial with int eger coefficients, its leading coefficient in particular will be an integer, call it m; similarly, b will have an integer as its leading coefficient, call it n. By multiplication of polynomials, it follows that the leading coefficient of ab is equal to mn; since the leading coefficient of 0 is 0, and the coefficients must match up, it follows that $mn = 0$. By the fact that $\mathbb{Z}$ is an integral domain, we deduce that either m or n must be zero, meaning that one of a or b must be equal to the zero polynomial. Clearly, multiplication in $\mathbb{Z}[x]$ is commutative because multiplication in $\mathbb{Z}$ is commutative. Thus $\mathbb{Z}[x]$ is an integral domain. □

Problem 8

Let $f(x)$ and $g(x)$ be polynomials with rational coefficients. Show that if $f(n) = g(n)$ for all integers n, then $f(x) = g(x)$.

Proof. Define $h(x) = f(x) - g(x)$. $h(x)$ is a polynomial over $\mathbb{Q}[x]$ because both $f(x)$ and $g(x)$ are polynomials over $\mathbb{Q}[x]$. Suppose that $h(x) \neq 0$; then it follows that $h(x)$ has degree k for some positive integer k. This means that $h(x)$ has at most k zeros. Because $f(n) = g(n)$ for all integers n, it follows that $h(n) = 0$ for all integers n, meaning that h has infinitely many zeros; but this contradicts the fact that $h(x)$ has degree k. Thus $h(x) = 0$, meaning that $f(x) = g(x)$. □

Problem 9

Prove that the set of polynomials whose coefficients are all even is a prime ideal in $\mathbb{Z}[x]$.

Proof. Denote the set A. First, we will show that A is an ideal. To this end, take $a, b \in A$. Because subtraction of even integers preserves parity, it follows that $a - b \in A$. Now take any polyomial $p \in \mathbb{Z}[x]$. Because multiplication of polynomials is commutative, it suffices to show that $pa = ap \in A$. Observe that the each coefficient of ap arises by multiplying one coefficient from a and p. Every coefficient of a is even, and the parity of the coefficients of p does not matter because an even number multipled by an odd number is always even. Thus all of the coefficients of ap are even, meaning that $ap \in A$, so A is an ideal. To show that it is prime, we will use the fact that $\mathbb{Z}[x]/A$ is an integral domain. It is well-defined as a ring because A is an ideal and it is commutative because $\mathbb{Z}[x]$ is commutative, so we must show that the factor ring has no zero divisors. To this end, observe that if $c + A$ and $d + A \in \mathbb{Z}[x]/A$ are non-trivial elements, it follows that c and d each have at least one odd coefficient because multiplication of an odd integer with another odd integer yields an odd integer, meaning that the product $(c + A)(d + A)$ will be non-trivial (because cd will have at least one part with an odd coefficient, meaning that part will not be absorbed into A).

□

Problem 10

1. Show that $g(x) = x^3 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$.
2. Show that the ideal $I = \langle g(x) \rangle$ is maximal in $\mathbb{Z}_2[x]$ directly.
3. Show that the factor ring $F = \frac{\mathbb{Z}_2[x]}{I}$ is a field. So the subset $F^\times = F - \{0\}$ is a group under multiplication.
4. What is the order of $x + 1$ in the group $F^\times$?

Proof.

1. Observe that $g(0) = 1$ and $g(1) = 1$, meaning that $g(x)$ has no roots over $\mathbb{Z}_2[x]$; thus $g(x)$ is irreducible over $\mathbb{Z}_2[x]$

2. Let J be any ideal such that $I \subseteq J \subseteq \mathbb{Z}_2[x]$. We have that $\mathbb{Z}_2[x]$ is a principal ideal domain, meaning that $J = \langle f(x) \rangle$ for some polynomial $f(x)$. Thus we have that $g(x) = f(x)h(x)$ for some polynomial $h(x)$. But because $g(x)$ is irreducible, it follows that either $f(x)$ or $h(x)$ is a constant; in the first case, we have that $J = \mathbb{Z}_2[x]$, and in the second case we have that $J = I$. Thus I is a maximal ideal by definition.

3. Because I is a maximal ideal of $\mathbb{Z}_2[x]$, it follows that the factor ring is a field; this means that the subset of nonzero elements of F form a group under multiplication, as there are multiplicative inverses by virtue of the subset being a field.

4. The order of $x+1$ is 7 in this group; we use the fact that $x^3 = -x^3 = x+1$ to show this. By repeatedly multiplying $x+1$ by itself until we get 1, we notice that
$$\begin{aligned}(x+1)^2 &= x^2 + 2x + 1 = x^2 + 1\\ (x+1)^3 &= x^3 + x^2 + x + 1 = x^2\\ (x+1)^4 &= x^3 + x^2 = x^2 + x + 1\\ (x+1)^5 &= x^3 + 1 = x\\ (x+1)^6 &= x^2 + x\\ (x+1)^7 &= x^3 + x = 1\end{aligned}$$
Also, we can use the observation that $F - \{0\}$ has 7 elements, so the order of $x+1$ must be 1 or 7 by Lagrange's theorem; clearly it is not the identity, so the order is 7.

□

Extra Credit

Let R be a ring with $x^2 = x$ for all $x \in R$. Prove that R is commutative.

Proof. First, we make the observation that R has characteristic 2. Note that for any $r \in R$, we have that $(r + r) = (r + r)^2 = (2r)^2 = 4r^2 = 4r$, which means that $r + r = 0$. Now take $x, y \in R$ and observe that $(x + y) = (x + y)^2 = x^2 + y^2 + xy + yx = x + y + xy + yx$, meaning that $xy + yx = 0$ so that $xy = -yx$; thus it follows that $xy = yx$ from the fact that the ring has characteristic 2. We conclude that R is commutative. □