MAT1100

Algebra I

Assignment 3

Contents

Tyler Holden - Fall 2011

999163934

1. Problem 1

Show that any group of order 56 has a normal Sylow-p subgroup, for some prime p dividing 56.

Let G be a group such that $|G| = 56 = 2^3 \cdot 7$. Let n_2 and n_7 denote the number of Sylow-2 and Sylow-7 subgroups respectively. By Sylow's theorems, we know that

$$\begin{array}{lll} n_2 & \equiv 1 \mod 2 & \qquad n_7 \equiv 1 \mod 7 \\ n_2 & \Big| 7 & \qquad n_7 \Big| 8 \end{array}$$

and so $n_2 \in \{1,3,5,7\}$ while $n_7 \in \{1,8\}$. Now if $n_7 = 1$ we are done since the Sylow-7 subgroup will be normal. Thus assume that $n_7 \neq 1$ so $n_7 = 8$.

For any two distinct Sylow-7 subgroups $P, Q \in \mathrm{Syl}_7(G)$ we must have that $P \cap Q = \{e\}$. This is because their intersection must also be a subgroup of G with order dividing 7, so the only possibility is the trivial subgroup. Since every non-identity element of a Sylow-7 subgroup has order 7, this accounts fo $8 \cdot (7-1) = 48$ elements of order 7. We claim that this forces $n_2 = 1$. Indeed, we note there are at most seven elements whose order is a power of 2, since the elements of order 7 and the identity element correspond to 49 of the 56 possible elements. Since there is at least one non-trivial Sylow-2 subgroup, there must also be at least 7 such elements, and between these two inequalities we conclude there are precisely seven such elements. This corresponds to the existence of exactly one Sylow-2 subgroup, and so $n_2 = 1$ as required.

2. Problem 2

Let S_5 act on $(\mathbb{Z}/5)^5$ by permuting the factors, and let G be the semi-direct product of S_5 and $(\mathbb{Z}/5)^5$.

2.1. **Part a. What is the order of G.** We first strive to make sense of the semi-direct product. We recall that a group action of G on a set X enduces a group homomorphism $G \to \mathrm{Aut}(X)$. For our purposes, define $\phi : G \to \mathrm{Aut}\left((\mathbb{Z}/5)^5\right)$ as the desired group homomorphism. Furthermore, in the direct product $N \ltimes H$ we require a group homomorphism $H \to \mathrm{Aut}(N)$. Identifying the roles of sets and groups above, we define

$$G = (\mathbb{Z}/5)^5 \rtimes_\phi S_5. \tag{1}$$

Via the characterization of semi-direct products, we can identify $(\mathbb{Z}/5)^5 \triangleleft G$ and $S_5 \leq G$ satisfying $G = (\mathbb{Z}/5)^5 S_5$ and $(\mathbb{Z}/5)^5 \cap S_5 = \{e\}$. Thus the order of G is the product of the order of the subgroups with which these are identified, and we conclude that $|G| = 5^5 \cdot 5! = 2^3 \cdot 3 \cdot 5^6$.

2.2. **Part b. How many Sylow-5 subgroups does G have? Write one of them down.**

The Sylow Theorems tell us that $n_5 \equiv 1 \mod 5$ and $n_5 \Big| 24$ hence $n_5 \in \{1, 6\}$. Now since $(\mathbb{Z}/5)^5$ is a p-group, the number of Sylow-5 subgroups will correspond to the number of Sylow-5 subgroups of S_5. Once again, since $|S_5| = 5 \cdot 3 \cdot 2^3$ we know that $n_5(S_5) \in \{1, 6\}$. Furthermore, every non-trivial element of a Sylow-5 subgroup of S_5 will have order 5. Since 5 is prime, the only elements of order 5 in S_5 are the 5-cycles, of which there are

$$\frac{5!}{5} = 4! = 24. \tag{2}$$

This implies that $n_5(S_5) = 6$. Hence there are precisely six Sylow-5 subgroups of $(\mathbb{Z}/5)^5 \rtimes_\phi S_5$.

Now every Sylow-5 subgroup of S_5 is a cyclic subgroup, so in particular let $G = \langle (1\ 2\ 3\ 4\ 5) \rangle$. Then $(\mathbb{Z}/5)^5 \times G$ is a Sylow-5 subgroup of $(\mathbb{Z}/5)^5 \rtimes_\phi S_5$.

3. Problem 3

Show that the group Q of unit quaternions ($\{\pm 1, \pm i, \pm j, \pm k\}$, subject to $i^2 = j^2 = k^2 = -1 \in Z(Q)$ and $ij = k$) is not a semi-direct product of two of its proper subgroups.

We begin by analyzing the subgroups of Q. Define the sets

$$H_1 = \{\pm 1\}, H_i = \{\pm 1, \pm i\}, H_j = \{\pm 1, \pm j\}, H_k = \{\pm 1, \pm k\}. \tag{3}$$

These are clearly subgroups of Q, and we claim that these are the only possible subgroups. Indeed, we note that $\langle H_i, j \rangle = Q$ since $ij = k$ meaning $\langle H_i, j \rangle$ contains all generators of Q. By precisely the same reasoning it is impossible to add additional elements to show listed in (3) without generating the entire group, so this enumerates all non-trivial proper subgroups of Q.

The subgroups $H_i, H_j, H_k \triangleleft Q$ since they have index 2, while $H_1 \triangleleft Q$ since $H_i \subseteq Z(Q)$. Now for two groups $G, H \leq Q$ to form a semi-direct product in Q, it must be true that $Q = GH$ and $G \cap H = \{1\}$. However, we note that no two subgroups intersect trivially, and so Q cannot be a semi-direct product of its subgroups.

4. Problem 4

Let G be a finite group and p be a prime. Show that if H is a p-subgroup of G, then $[N_G(H) : H]$ is congruent to $[G : H] \mod p$. You may wish to study the action of H on G/H by multiplication on the left.

We recall that we cal always write the order of a set as the sum of its transitive orbits. Hence if we act on G/H by H, we can write

$$|G/H| = \left| \begin{array}{c} \text{number of singleton} \\ \text{orbits} \end{array} \right| + \sum \left| \begin{array}{c} \text{non-trivial} \\ \text{orbits} \end{array} \right|. \tag{4}$$

Let $\bar{x} \in G/H$ be a representative of a non-trivial orbit. We know that for transitive action, the order of the orbit divides the order of the group and so $|H\bar{x}| \,\Big|\, |H|$. However, H is a p-group which implies that all non-trivial orbits are non-zero powers of p. If we calculate equation (4) modulo p we get

$$|G/H| \equiv \left| \begin{array}{c} \text{number of singleton} \\ \text{orbits} \end{array} \right| \mod p. \tag{5}$$

It is thus sufficient to show that every singleton orbit corresponds to elements of $N_G(H)/H$. Let $gH \in G/H$ be an arbitrary element. This corresponds to a fixed orbit if $hgH = gH$ for all $h \in H$. We can rewrite this as $g^{-1}hgH = H$ which implies that $g^{-1}hg \in H$ for all $h \in H$. This is precisely the condition for $g \in N_G(H)$ and so every singleton orbit arises from cosets on the normalizer so

$$\{\text{fixed orbits}\} \subseteq N_G(H)/H. \tag{6}$$

Conversely, if $g \in N_G(H)$ then consider hgH. We can write this as $gg^{-1}hgH = gH$ since $g^{-1}hg \in H$. Hence each gH is a singleton orbit which implies that

$$N_G(H)/H \subseteq \{\text{fixed orbits}\}. \tag{7}$$

Thus every element of the normalizer yields cosets with singleton orbits. Both inclusions imply that the total number of singleton orbits corresponds exactly to the number of cosets of H in $N_G(H)$ and so

$$[G : H] = \left|\frac{G}{H}\right| \equiv [N_G(H) : H] \mod p \tag{8}$$

which is what we wanted to show.

5. Problem 5

5.1. **Part a. Prove that in any ring, $(-a)^2 = a^2$ and hence $(-1)^2 = 1$.** Let R be a ring and denote the additive inverse of $a \in R$ as $-a$. Consider the following equation

$$\begin{aligned} (-a)\left[(-a) + a\right] &= (-a)(-a) + (-a)a \\ &= (-a)^2 + (-a)a \\ &= 0 \qquad\qquad \text{since } (-a) + a = 0 \quad . \end{aligned}$$

And so we conclude that $(-a)^2 = -\Big((-a)a\Big)$. Hence all that remains is to show that $-\Big((-a)a\Big) = a^2$, but this is true since

$$\begin{aligned} \Big(a + (-a)\Big)\, a &= a^2 + (-a)a \\ &= 0 \end{aligned}$$

which is precisely what we wanted to show. We conclude that $(-a)^2 = a^2$, and so if we substitute $a = 1$ we get that $(-1)^2 = 1$.

6. Problem 6

6.1. **Part a. Prove that a finite integral domain is a field.** Let R be a finite integral domain. Choose $x \in R \setminus \{0,1\}$ and enumerate the list $\{x, x^2, x^3, \dots, x^m, \dots\}$. Since R is finite, this list cannot be indefinitely distinct; that is, $\exists k, n \in \mathbb{N}$ such that $x^n = x^k$. Without loss of generality, assume $k < n$ so that

$$\begin{aligned} x^n = x^k &\Rightarrow x^{n-k}x^k = x^k \\ &\Rightarrow x^{n-k}x^k - x^k = 0 \\ &\Rightarrow (x^{n-k} - 1)x^k = 0 \end{aligned} \tag{9}$$

Claim 1. $x^k \neq 0$.

Proof. For the sake of contradiction, assume that $x^k = 0$ and write $x^k = xx^{k-1} = 0$. Since R is an integral domain and we assumed $x \neq 0$ then $x^{k-1} = 0$. By backwards induction, assume that $x^{j+1} = 0$ for $(j+1) < n$. Then $x^{j+1} = xx^j = 0$ implies that $x^j = 0$. Hence $x^j = 0$ for all $j < n$. However, this is a contradiction since inductively, we find that $x^2 = xx = 0$ but this cannot be the case since $x \neq 0$ and R is an integral domain. We conclude that $x^k \neq 0$. □

But if $x^k \neq 0$ then (9) implies that $x^{n-k} = 1$, so in particular $xx^{n-k-1} = 1$ which implies that x is a unit with inverse x^{n-k-1}. Since x was arbitrary, this must hold for all elements of R and we conclude that R is a field.

6.2. **Part b. Prove that in a finite commutative ring, every prime ideal is maximal.** Let R be a finite commutative ring and P a prime ideal. By definition (or equivalent consequence) we know that R/P is an finite integral domain. By part (a), it follows that R/P is a field, and so P is in fact maximal.

7. Problem 7

A ring R is called a Boolean ring if $a^2 = a$ for all $a \in R$.

7.1. **Part a. Prove that every Boolean ring is commutative.** Let R be a Boolean ring. We first note that

$$\begin{aligned} (1+1)^2 &= (1+1)(1+1) \\ &= 1+1+1+1 && \text{by expanding} \\ &= 1+1 && \text{since the ring is Boolean} \end{aligned}.$$

Hence $1+1+1+1 = 1+1$ implies that $1+1 = 0$ so $1 = -1$. Now let $a, b \in R$ and conduct the exact same calculation to find

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b) \\ &= a^2 + b^2 + ab + ba \\ &= a + b + ab + ba && \text{since } a^2 = a, b^2 = b \\ &= a + b && \text{since the ring is Boolean}\end{aligned}.$$

This means that $a+b = a+b+ab+ba$ and so by cancelling the a and b we get that $ab+ba = 0$ so $ab = -ba$. However, we showed earlier that $1 = -1$ so $ab = -ba = (-1)ba = ba$ and we conclude the ring is commutative.

7.2. **Part b. Prove that the only Boolean ring that is also an integral domain is $\mathbb{Z}/2$.**

Let R be a Boolean ring which is also an integral domain and take $a \in R \setminus \{0\}$. Then

$$\begin{aligned}a^2 = a &\Rightarrow a^2 - a = 0 \\ &\Rightarrow a(a-1) = 0.\end{aligned}$$

Since $a \neq 0$ this means that $a - 1 = 0$ so $a = 1$. We conclude that all non-zero elements are the multiplicative identity so $R = \{0, 1\}$ which is clearly $\mathbb{Z}/2$ as required.

8. Problem 8