HOMEWORK 3

LOUIS-PHILIPPE THIBAULT

Problem 1

Let G be a group of order 56. We have that $56 = 2^3 \cdot 7$. Then, using Sylow's theorem, we have that the only possibilities for the number of Sylow-p subgroups are:

(1) $n_2(G) = 1$ or 7;
(2) $n_7(G) = 1$ or 8.

We will show that the case $n_2(G) = 7, n_7(G) = 8$ is impossible. Two different Sylow-7 subgroups intersect only in the identity, so none of the elements of order 7 in a given Sylow-7 subgroup is in another Sylow-7 subgroup. Also, all the Sylow-7 subgroups are conjugate, by Sylow's theorem, hence isomorphic. Then, if $n_7(G) = 8$, we have that G has at least $8 \cdot 6 = 48$ elements of order 7. The remaining elements must form a Sylow-2 subgroup. So there are not enough elements of order 2 to form seven Sylow-2 subgroup, which is a contradiction.

We have shown that $n_2(G) = 1$ or $n_7(G) = 1$. Suppose without lost of generality that $n_2(G) = 1$. Then there is a unique Sylow-2 subgroup P_2. By the Sylow's theorem, every conjugate of P_2 is a Sylow-2 subgroups. So P_2 is equal to its conjugates. Hence P_2 is normal in G.

Problem 2

Part 1. We have that $G = (\mathbb{Z}/5)^5 \rtimes S_5$. As a set G is the direct product of $(\mathbb{Z}/5)^5$ and S_5, so $|G| = |(\mathbb{Z}/5)|^5|S_5| = 5^6 \cdot 2^3 \cdot 3 = 375000$.

Part 2. A Sylow-5 subgroup of G has order 5^6. We claim that $P = (\mathbb{Z}/5)^5 \rtimes \langle(1,2,3,4,5)\rangle$ is a Sylow-5 subgroup of G. In fact, $|P| = 5^6$. Also, it is a subgroup of G, because it is closed under multiplication. Indeed, the multiplication is clearly closed in the first variable, since we have all of $(\mathbb{Z}/5)^5$. It is also closed in the second variable, because $\langle(1,2,3,4,5)\rangle$ is a subgroup of S_5 and the multiplication in the second variable is the same as the multiplication in S_5.

We claim that there are six Sylow-5 subgroups of G. Indeed, all Sylow-5 subgroups are conjugate of P. Conjugating in the first variable does not change the group $(\mathbb{Z}/5)^5$. So, the number of Sylow-5 subgroups of G is equal to the number of groups conjugated to $\langle(1,2,3,4,5)\rangle \cong C_5$. Every conjugate P' of $\langle(1,2,3,4,5)\rangle$ is such that $|P'| = |\langle(1,2,3,4,5)\rangle| = 5$. Also, there are $4! = 24$ elements of order 5 in S_5. Since each conjugate in S_5 preserves the cycle type, we have that every conjugate of P contains four 5-cycles and the identity. So there is $24/4 = 6$ groups conjugated to $\langle(1,2,3,4,5)\rangle$. Hence $n_5(G) = 6$.

Problem 3

If Q was the semi-direct product of two of its proper subgroups, it would have to be of a group of order 4 with a group of order 2. The only group of order 2 is C_2 and the two only groups of order 4 are C_4 and $C_2 \times C_2 = V_4$. But V_4 is not a subgroup of Q, because V_4 has three elements of order 2 and Q has only one element of order 2. So if Q is a semi-direct product, then there is only two possibilities, namely

(1) $Q = C_4 \rtimes C_2$;
(2) $Q = C_2 \rtimes C_4$.

We will show that all of these possibilities are impossible. First of all, the only subgroup of order 2 in Q is $\{+1, -1\}$. Moreover,

$$Q/\{+1,-1\} \cong V_4.$$

Indeed, $Q/\{+1,-1\} = \{\bar{1}, \bar{i}, \bar{j}, \bar{k}\}$. Since $\bar{i}, \bar{j}, \bar{k}$ all have order 2, $Q/\{+1,-1\} \cong V_4$. So case 2 is impossible, because whenever a group $G = N \rtimes H$, then $G/N \cong H$.

We now analyze case 1. $Aut(C_4) \cong C_2$. We now imagine $C_2 = \{0, 1\}$ as the additive cyclic group. So there is only one non-trivial homomorphism $\phi : C_2 \to Aut(C_4)$, namely the one sending 0 to the identity automorphism and 1 to ϕ_1, where

$$\phi_1(0) = 0,\ \phi_1(1) = 3,\ \phi_1(2) = 2,\ \phi_1(3) = 1.$$

Then, $C_4 \rtimes C_2 = \{(0,1),(1,1),(2,1),(3,1),(0,0),(1,0),(2,0),(3,0)\}$ as a set. Clearly, the identity has to be $(0,0)$. We have that $(0,1)(0,1) = (0,0)$, under the operation of the semi-direct product. Also, $(2,1)(2,1) = (0,0)$. So there is two elements of order 2 in $C_4 \rtimes C_2$, but Q has only one element of order 2. If ϕ is trivial, then $C_4 \rtimes C_2 = C_4 \times C_2$. But $(0,1)$ and $(2,1)$ have order 2 in $C_4 \times C_2$, whereas Q has only one element of order 2. So case 1 is impossible.

So, none of the possible semi-direct products of order 8 is isomorphic to Q.

Problem 4

Suppose $|H| = p^\alpha$ for a given α. Let H acts on G/H by left multiplication. Then, $Orb(gH) = \{hgH | h \in H\}$. We have that

$$|Orb(gH)| = 1 \Leftrightarrow hgH = gH,\ \forall h \in H \Leftrightarrow g^{-1}Hg \subset H$$

$$\Leftrightarrow g \in N_G(H) \Leftrightarrow gH \in N_G(H)/H.$$

Let g_iH be representatives of the orbits that contain more than one element. Then,

$$|G/H| = |N_G(H)/H| + \sum_i |Orb(g_iH)|.$$

Now we have that for all i, $|Orb(g_iH)| > 1$ and $|Orb(g_iH)| \mid |H| = p^\alpha$. So $|Orb(g_iH)| \equiv 0 \, mod \, p$ for all i. Then

$$|G/H| \equiv |N_G(H)/H| \, mod \, p.$$

Problem 5

We will start by part 2. We have that $(-a)(a) = -(a^2)$. Indeed,

$$(-a)(a) + (a)(a) = (-a + a)(a) = 0,$$

where we have used the distribution property. Then,

$$(-a)(-a) + (-(a^2)) = (-a)(-a) + (-a)(a) = (-a)(-a + a) = 0.$$

So $(-a)^2 = a^2$, where we have used the fact that $-(-(a^2)) = a^2$. For part 1, we just need to take $a = 1$.

Problem 6

Part 1. Let D be a finite integral domain. By definition, an integral domain is commutative, so we only need to check that every nonzero element of D has a multiplicative inverse. Let $a \neq 0$ be an element of D. Then we have that

$$\{ax|x \in D\} = D. \ (*)$$

In fact, we have that whenever $x \neq y$, $ax \neq ay$, because D is a domain. Since D is finite, we have $|\{ax|x \in D\}| = |D|$, and this implies the result $(*)$. In particular, there exists an x such that $ax = 1$. So a has an inverse. Since a was arbitrary, we have that every element of D has an inverse. Hence D is a field.

Part 2. We have that an ideal P is prime in R if and only if R/P is an integral domain. Since R/P is a finite integral domain, it is a field (see part 1). We have proved in class that given a ring S and an ideal I, the quotient S/I is a field if and only if I is maximal. Then, using this theorem, P is maximal.

Problem 7

Part 1. We first show that for every $x \in R$, $2x = 0$. Indeed,

$$2x = x + x = (x + x)^2 = x^2 + 2x^2 + x^2 = x + 2x + x = 4x.$$

Subtracting by $2x$ both side, we have $2x = 0$. In particular, it means that $x = -x$.

Using this property, we prove the main result:

$$x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y.$$

Subtracting by x and y both side, we have $xy + yx = 0$, so $xy = -yx = yx$. Since x, y were arbitrary, we conclude that R is commutative.

Part 2. $\mathbb{Z}/2$ is clearly a Boolean ring. It is also a field, so it is an integral domain. Since $\mathbb{Z}/2$ is the only ring up to isomorphism of order 2, suppose we have a Boolean ring R such that $|R| > 2$. Take $a \neq 0, 1$ in R. Then, $a(a-1) = a^2 - a = 0$, but $a \neq 0$ and $a - 1 \neq 0$, because $a \neq 1$. So R is not an integral domain.

Problem 8

Part 1. By the Bolzano-Weiestrass theorem, every bounded sequence has a converging subsequence. So, intuitively, we want to define a map $\phi : S \to \mathbb{R}$ such that ϕ sends a sequence to the limit of one of its converging subsequence. We want to find a way to choose which subsequence to take. We will do this by using the fact that we want J to be in the kernel of ϕ.

Define $U_{\epsilon,(a_n)} = \{i \in \mathbb{N} | |a_i| < \epsilon\,, a_i \in (a_n)\}$, and $U_J = \{U_{\epsilon,(a_n)} | \epsilon > 0, (a_n) \in J\}$. We claim that the map $\phi : S \to \mathbb{R}$, $(a_n) \mapsto x$, where x is chosen such that for all $\epsilon > 0$,

$$\{i \in \mathbb{N} | |a_i - x| < \epsilon, a_i \in (a_n)\} \in U_J$$

(1) is well-defined, that is, x exists and is unique;
(2) is a surjective homomorphism;
(3) has $ker\phi = J$.

These three properties will complete the proof. Indeed, by the first isomorphism theorem, we will have $S/J \cong \mathbb{R}$.

We start by stating four properties of J and U_J.

a. We first notice that J cannot contain a sequence with a finite number of elements equal to 0 (or no element equal to 0), unless this sequence contains a subsequence that converges to 0. Otherwise, if $(a_n) \in J$ has only a finite number of elements equal to 0 and no subsequences converging to 0, then $J = S$. Indeed, we can take $(d_n) \in I$ such that $(\tilde{a}_n) = (a_n) + (d_n) \in J$ do not contain any zero, nor subsequences converging to 0. Then, for every $(b_n) \in S$, there exists a $(c_n) \in S$ such that $(b_n) = (\tilde{a}_n)(c_n)$. The sequence (c_n) can be chosen to be bounded because $(\tilde{a}_n)$ has no subsequence converging to 0. Thus, $(b_n) \in J$. Since (b_n) was arbitrary, $J = S$. In particular, $\emptyset \notin U_J$ and U_J contains no finite sets.

b. If $U_{\epsilon,(a_n)} \in U_J$ and $U_{\epsilon,(a_n)} \subset V$, then $V \in U_J$. Indeed, V is of the form $V = U_{\epsilon',(\tilde{a}_n)}$, where $\epsilon' > \epsilon$ and $(\tilde{a}_n) \in J$ is such that $U_{\epsilon,(a_n)} = U_{\epsilon,(\tilde{a}_n)}$. Note that every $(\tilde{a}_n)$ having the property $U_{\epsilon,(a_n)} = U_{\epsilon,(\tilde{a}_n)}$ are in J, as it suffices to obtain it from a multiplication of (a_n) by an appropriate sequence in S.

c. If $(a_n), (b_n) \in J$, $U_{\epsilon,(a_n)}, U_{\epsilon',(b_n)} \in U_j$, then $U_{\epsilon,(a_n)} \cap U_{\epsilon',(b_n)} \in U_J$. Indeed, $U_{\epsilon,(a_n)} \cap U_{\epsilon',(b_n)} \supset U_{\epsilon+\epsilon',(a_n)+(b_n)}$. Then the result follows from *b*.

d. If $U \notin U_J$, then $U^c \in U_J$. In fact, otherwise let (b_n) be the sequence such that $b_i = 0$ for every $i \in U^c$. Note that (b_n) have infinitely many 0, because otherwise $U \in U_I \subset U_J$. Then, $J[(b_n)]$, the smallest ideal containing both J and (b_n) is not all of S. This contradicts the maximality of J. Indeed, if $(s_n) \in S$ has sufficiently large entries at every index, it is clearly impossible to multiply (b_n) by a sequence of S to obtain (s_n), since (b_n) has infinitely many 0. Moreover, if $(b_n) + (c_n) = (s_n)$, with $(c_n) \in J$, then there exists $\epsilon > 0$ such that $U_{\epsilon,(c_n)} \subset U$. In fact, since $(c_n) \in J$, it has infinitely many small values. Those small values have to be at different indices that those of (b_n), since (s_n) has large values. So, by property *b*, $U \in U_J$. Since this is impossible, it implies that (c_n) cannot be in J, so $(s_n) \notin J[(b_n)]$ implies $J[(b_n)] \neq S$.

We now prove the uniqueness. Suppose x_1 and x_2 are good candidate for $\phi(a_n)$. Then there exists $\epsilon > 0$ such that

$$\{i \in \mathbb{N} | |a_i - x_1| < \epsilon\} \in U_J, \ \{i \in \mathbb{N} | |a_i - x_2| < \epsilon\} \in U_J$$

are disjoint. But, by properties *a* and *c*, this is impossible.

We want to prove the existence. Suppose that there exists (a_n) such that for all convergent subsequences (a_k), there exists $\epsilon_{(a_k)} > 0$ such that

$$\tilde{U}_{\epsilon_{(a_k)},(a_k)} = \{i \in \mathbb{N} | |a_i - x_{(a_k)}| < \epsilon_{(a_k)}\} \notin U_J,$$

where $x_{(a_k)}$ is the limit of (a_k). Then, since the complement $\tilde{U^c}_{\epsilon_{(a_k)},(a_k)}$ of every $\tilde{U}_{\epsilon_{(a_k)},(a_k)}$ is in U_J (property *d*), then $\cap \tilde{U^c}_{\epsilon_{(a_k)},(a_k)} \in U_J$ (property *c*) is finite, where the intersection is taken over all the converging subsequences of (a_n). This contradicts property *a*.

We now want to prove that ϕ is a surjective homomorphism. First, ϕ is clearly surjective, as $(\phi((r)_{i=0}^{\infty}) = r$ for all r in $\mathbb{R}$. If $\phi(a_n) = x_1$ and $\phi(b_n) = x_2$, then $(a_n) - (x_1) \in J$ and $(b_n) - (x_2) \in J$. So $((a_n) + (b_n) - ((x_1) + (x_2))) \in J$, where we view x_1, x_2 as sequences (x_1), (x_2), respectively. Thus, for all $\epsilon > 0$,

$$\{i \in \mathbb{N} | |a_i + b_i - (x_1 + x_2)| < \epsilon\} \in U_J.$$

Hence, $\phi(a_n + b_n) = x_1 + x_2$. Also, $(x_2)((a_n) - (x_1)) \in J$, because J is an ideal. Then, $((a_n)((b_n) - (x_2)) + (x_2)((a_n) - (x_1))) = ((a_n)(b_n) - (x_1)(x_2)) \in J$, so $\phi(a_n b_n) = x_1 x_2$ as

before. So ϕ is a homomorphism.

Finally, $ker\phi = J$. This is clear, because $J \subset ker\phi$. Then, by maximality of J, $J = ker\phi$.

So $S/J \cong \mathbb{R}$.

Part 2. The last two parts are due to the fact that Lim_J is a homomorphism. For the first part, let $Lim_J(a_n) = x$. Then, $((a_n) - (x)) \in J$. So, $(c)((a_n) - (x)) \in J$, because J is an ideal. Then, as in part 1, for all $\epsilon > 0$,

$$\{i \in \mathbb{N} || ca_i - cx| < \epsilon\} \in U_J.$$

So, $Lim_j(ca_n) = cx$.

Part 3. First of all, notice that all convergent sequences having limit 0 are in J. This is due to the fact that if $(a_n) \to 0$, then for all $\epsilon > 0$, there exists N such that for all $n > N$, $|a_n| < \epsilon$. Then, take $(b_n) \in I$ such that $b_n = 0$ for all n such that $|a_n| < \epsilon$. We have that

$$\{i \in \mathbb{N} || a_i| < \epsilon\} = U_{\epsilon,(b_n)} \in U_J.$$

Since $\epsilon > 0$ was arbirary, $Lim_J(a_n) = 0$. So, $(a_n) \in J$. Now take a convergent sequence $(c_n) \to x$. Then, $((c_n) - (x))$ is a sequence converging to 0. So $((c_n) - (x)) \in J$. Thus, $Lim_J((c_n) - (x)) = 0$. Hence, $Lim_J(c_n) = Lim_J(x) = x$.

Part 4. The answer is no. Indeed, take the sequences $((-1)^n)$ and $((-1)^{n+1})$. Then, if $Lim_J(((-1)^n)) = Lim_J(((-1)^{n+1}))$, we have $Lim_J(((-1)^n)) - ((-1)^{n+1})) = 0$. But, clearly $Lim_J(((-1)^n)) - ((-1)^{n+1})) = Lim_J(2(-1)^n) = 2$ or -2, depending on J.