2/13/17 Spring 2017, Intro to Modern Algebra II Test I Solutions Sitaraman

EACH PROBLEM 20 POINTS. ANSWER AS MANY AS YOU CAN.

1.(Could be harder than the other problems). If G is an abelian group of order 35, show that it is $P \times Q$ where P is a 5-Sylow subgroup and Q a 7-Sylow subgroup. You may use the following fact, if necessary (corollary to Theorem 2.9.4) :

If N_1, N_2 are normal subgroups of any group such that $G = N_1N_2$ and $N_1 \cap N_2 = \{e\}$ then G is the internal direct product of N_1, N_2

Use no other theorems. Show also that it is cyclic.

Solution: This is an application of lemma 2.10.1. You can use the same argument with $P = \{x \mid x^5 = e\}$ and $Q = \{x \mid x^7 = e\}$.

Here is another proof:

By Cauchy's theorem, we have an element a of order 5 and an element b of order 7.

Let $P =< a >$ and $Q =< b >$.

If we show that $P \cap Q = \{e\}$ and $G = PQ$ then we are done, by the fact stated in the question. Note that both subgroups here are normal because G is abelian.

Clearly $P \cap Q = \{e\}$ because otherwise we would have an element whose order divides both 5 and 7.

Now we claim Pb has order 7 in G/P: First $Pb \neq P$ because $b \in Q$ and thus $b \in P$ is impossible. Next G/P has 7 elements. So order of any element other than identity must be 7. So Pb has order 7 in G/P and thus it generates G/P.

So given $g \in G$, we have $Pg = Pb^k$ for $1 \leq k \leq 7$. This means $g \in Pb^k \implies g = a^m b^k$ for some $1 \leq m \leq 5$. So we have proved that $G = PQ$.

Proof that G is cyclic:

Look at $< ab >= \{(ab)^n\}$ for $1 \leq n \leq 35$. Clearly $< ab >\subset G$.

If $(ab)^n = e$ then $a^n b^n = e \implies a^n = b^{-n} \implies 5 \mid n\ AND\ 7 \mid n$ because $P \cap Q = \{e\}$ and so $a^n = b^{-n} = e$.

But 35 is the LCM of 5 and 7. So this cannot happen for $n < 35$.

Thus order of $< ab >$ is 35 and it must equal all of G.

BTW if you use the Chinese Remainder Theorem (we will see it later in the semester) we have that there is a bijection between $1 \leq n \leq 35$ and the 35 pairs of elements in $\{0, 1, 2, 3, 4\} \times \{01, 2, 3, 4, 5, 6\}$. In other words, given $n \in [1, 35]$ we can solve the two equations $m \equiv n\ mod\ 5$ and $k \equiv n\ mod\ 7$ simultaneously. So this gives that every element of the form $a^m b^k$ is a power of ab.

Chinese Remainder Theorem (CRT) basically says $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ if $(m, n) = 1$.

Alternate proof that $PQ = G$

Clearly $PQ \subset G$.

On the other hand $a^m b^k = a^{m'} b^{k'} \implies a^{m-m'} = b^{k'-k}$. Since $P \cap Q = \{e\}$ this can only happen if $5 \mid (m - m')$ AND $7 \mid (k - k')$.

But there are 35 distinct pairs (x, y) such that no two pairs (x_1, y_1) and (x_2, y_2) among tham have $5 \mid (x_1 - x_2)$ AND $7 \mid (y_1 - y_2)$. (It is just $\{0, 1, 2, 3, 4\} \times \{0, 1, 2, 3, 4, 5, 6\}$).

This gives 35 distinct elements of the form $a^m b^k$ in G.

So we get that $PQ = G$.

Note: Combined with the fact that $G =< ab >$ this gives an alternate proof of CRT ! This is not surprising, since, as mentioned above, CRT essentially says that $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ if $(m, n) = 1$. Here we can make $< ab >\simeq \mathbb{Z}_{35}$ and $P \simeq \mathbb{Z}_5$ and $Q \simeq \mathbb{Z}_7$. But it must be mentioned that CRT goes further. It also gives a formula to find (m, k) such that, given $1 \leq n \leq 35$, we can get $m \equiv n\ mod\ 5$ and $k \equiv n\ mod\ 7$.

2. List all the 2-Sylow and 3-Sylow subgroups of S_4. [Hint: For the 2-Sylow subgroups, think of dihedral groups, and the fact that the $p-$Sylow subgroups are conjugate].

Solution: 3-Sylow subgroups are of order 3, and the only elements of order 3 are the 3-cycles. Thus there are 4 3-Sylow subgroups, each having a distinct set of numbers. They are {(123. (132), id }, {(124), (142), id }, {(134),(143),id} and {(234), (243), id }.

2-Sylow subgroups are of order 8. These turn out to be the three subgroups isomorphic to D_8, the dihedral group of order 8. The number of 2-Sylow subgroups divides $24/8 = 3$, so 3 has to be the right number and it cannot be bigger than 3.

Here is one of them. The other two can be obtained by conjugation.

{ (1234),(13)(24),(1432),(13),(24),(12)(34),(13)(24) }.

3. Prove the following:

(a) The normalizer $N(H)$ of a subgroup H in a group G is the largest subgroup of G in which H is normal.

(b) The center of G is the intersection of all the centralizers of all the elements of G.

Solution: a) This follows almost from the definition. If any subgroup K has H as a normal subgroup, then it has to be contained in $N(H)$ because every element $k \in K$ satisfies $kHk^{-1} = H$ and this by definition makes $k \in N(H)$.

b) This also follows from the definition of a centralizer. If $x \in Z(G)$ then $x \in C(a)$ for any $a \in G$ because x commutes with any element so it certainly commutes with a. But then $Z(G) \subseteq C(a)$ for all $a \in G$ and thus $Z(G) \subseteq \bigcap_{a \in G} C(a)$. Conversely any element in the intersection of the centralizers is contained in the center because such an element has to commute with all $a \in G$. Therefore $Z(G) = \bigcap_{a \in G} C(a)$.

4. Write down all possible isomorphism types of abelian groups of order 60 in two different ways: one in terms of prime powers and another in terms of ascending order of divisors. For example, the isomorphism types of abelian groups of order 36 are $\mathbb{Z}_9 \times \mathbb{Z}_4, \mathbb{Z}_9 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_4, \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ in terms of prime powers and $\mathbb{Z}_{36}, \mathbb{Z}_{18} \times \mathbb{Z}_2, \mathbb{Z}_{12} \times \mathbb{Z}_3, \mathbb{Z}_6 \times \mathbb{Z}_6$ in terms of divisors of 12. Note that 2 divides 18 in $\mathbb{Z}_{18} \times \mathbb{Z}_2$, 3 divides 12 in $\mathbb{Z}_{12} \times \mathbb{Z}_3$ etc., Also note that each group in the first set is isomorphic to the corresponding group in the second set.

Solution: We have $60 = 2^2 \times 3 \times 5$. So the isomorphism types in terms of prime powers (these are called the elementary divisors) are $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$.

The isomorphism types in terms of the divisors (the invariant factors) are $\mathbb{Z}_{60}, \mathbb{Z}_{30} \times \mathbb{Z}_2$.

You can try arranging the divisors in any other form but you will see that you won't get such a sequence where each divisor divides the next biggest. For example, {3, 20 } has 3 not dividing 20 and {3, 12, 36 } does not multiply together to give 60.

5. Give on example for each. Explain how they satisfy each of the conditions given.

a) (12 points) A ring with unit element that is not commutative, has zero divisors and has an infinite number of elements.

b) (8 points) Three subsets of the ring of integers that are rings themselves (hence subrings) but with no unit element.

Solution:

a) As shown in class, the ring of square matrices (of any size) with integer entries or entries in any infinite field satisfies all of these conditions.

b) In fact any ring of the form $n\mathbb{Z}$ with $n \geq 1$ satisfies these conditions.

6. Show that in a non-abelian group G of order p^3, p being a prime, the center Z must have order p. You might need to use the fact that G is abelian if G/Z is cyclic.

Solution: By Lagrange's theorem the center could have $1, p, p^2$ or p^3 elements. The center cannot be the whole group because it is non-abelian. The center has to be non-trivial, as can be seen using the class equation. If it is of order p^2 then the factor group would be of order p and hence cyclic. But then if G/Z is cyclic then whole group has to be abelian. So it has to be of order p.