Algebra I, Fall 2016

Solutions to Problem Set 3

1. We have proved if p, q, r are prime numbers, then groups of order p^n, pq, pqr (Question 2), p^2q have normal subgroups. Also groups of order pq^n have normal subgroups if $p < q$. This covers all numbers between 31 and 59 except for 36, 40, and 56.

Let $|G| = 36$, and let a be the number of 3-Sylow subgroups. Then $a \equiv 1 \mod 3$, and $a|4$, so $a = 1$ or $a = 4$. If $a = 1$, we are done, so assume $a = 4$. and Let X be the set of subgroups of order 9 in G. Then X has 4 elements and G acts on X via conjugation and the action is transitive by the Sylow theorem. If we denote by S_X the group of permutations of X, then the action gives a group homomorphism $\phi : G \to S_X$. The homomorphism ϕ is not sending every element to the identity element of S_X since the action is transitive, so the Kernel of ϕ is not G. Also, since $G/\mathrm{Ker}(\phi) \simeq \mathrm{Im}(\phi)$, and the image of ϕ is a subgroup of S_X which has 24 elements, $\mathrm{Ker}(\phi)$ cannot be equal to $\{e\}$. So $\mathrm{Ker}(\phi)$ is a non-trivial normal subgroup of G.

If $|G| = 40 = 2^3\,5$, and if q is the number of 5-Sylow subgroups then $a|8$ and $a \equiv 1 \mod 5$, so $a = 1$, and so there is a normal subgroup of order 5.

If $|G| = 56 = 2^3\,7$, and a is the subgroups of order 8 and b is the subgroups of order 7, then if $a = 1$ or $b = 1$ we are done, other wise $a = 7$ and $b = 8$, two subgroups of order 7 have only the identity element if common, and since any two distinct subgroups of order 8 have at most 4 elements in common, we get

$$|G| > 1 + b(7-1) + (8-1) + 4 \geq 1 + 48 + 7 + 4 = 60$$

a contradiction.

2. We can assume $p < q < r$. Let a be the number of r-Sylow subgroups. Then $a|pq$ and $a \equiv 1 \mod r$. So $a = 1$ or $a = pq$. ($a \neq p$ since $p < r$ and hence is it not $\equiv 1 \mod p$; Similarly $a \neq q$.) If $a = 1$, then we are done, so assume $a = pq$. Let b be number of q-Sylow subgroups. Then $b|pr$ and $b \equiv 1 \mod q$. So $b = 1, r$, or rq. If $b = 1$, then we are done, otherwise $b \geq r$. Finally let c be the number of p-Sylow subgroups, then a similar argument shows $c = 1$, or $c \geq q$, so we assume $c \geq q$.

Now any two subgroups of prime orders have only the identity in common. And since there are pq subgroups of order r and at least r subgroups of order q, and at least q subgroups of order p. we get

$$|G| \geq 1 + pq(r-1) + r(q-1) + q(p-1) = pqr + (r-1)(q-1) > pqr$$

which is a contradiction.

3. Let p be a prime number and p^n the largest power of p dividing $|G_1|$ and p^m the largest power of p dividing $|G_2|$. Then p^{n+m} is the largest power of p which divides $|G_1 \times G_2|$. Let now P_1 be a subgroup of order p^n in G_1 and P_2 a subgroup of order p^m in G_2. Then clearly $P_1 \times P_2$ has order p^{n+m} and is therefor a p-Sylow subgroup of $G_1 \times G_2$. Let P be any other p-Sylow subgroup of $G_1 \times G_2$. Then by the Sylow theorem, P is conjugate to $P_1 \times P_2$, so

$$P = g\ P_1 \times P_2\ g^{-1} = \{(gag^{-1}, gbg^{-1}) | a \in P_1, b \in P_2\} = (gP_1g^{-1}, gP_2g^{-1}) = (gP_1g^{-1}) \times (gP_2g^{-1})$$

and gP_1g^{-1} and gP_2g^{-1} are Sylow subgroups of G_1 and G_2.

5. Let r and ρ be the generators of the Dihedral group corresponding to rotation and reflection. Then $r^n = e, \rho^2 = e$ and $r\rho = \rho r^{n-1} = \rho r^{-1}$, so $r^i\rho = \rho r^{-i}$ for every integer i. Therefore $r^i\rho^j r^{i'}\rho^{j'}$ is equal to $r^{i+j}\rho^{j+j'}$ if $j = 0$ and to $r^{i-i'}\rho^{j+j'}$ if $j = 1$. This shows that the map

$$\alpha : \mathbf{Z}_n \rtimes \mathbf{Z}_2 \to D_{2n}, \quad \alpha(i,j) = r^i\rho^j$$

is a group homomorphism. The map α is clearly a bijective map.