7510 HW 6

Duncan Wilkie

6 October 2022

Problem 1 (D&F 4.5.4). *Exhibit all Sylow 2-subgroups and Sylow 3-subgroups of D_{12} and $S_3 \times S_3$.*

Solution. $|D_{12}| = 12 = 2^2 \cdot 3$ and $|S_3 \times S_3| = 3! \cdot 3! = 3^2 \cdot 2^2$, so the Sylow 2-subgroups are of order 4 in each case, and the Sylow 3-subgroups of order 3 and 9, respectively. By Sylow's theorem, the number of Sylow p-subgroups must divide m, if $|G| = p^\alpha m$. Therefore, $n_2(D_{12}) \mid 3$, $n_3(D_{12}) \mid 4$, $n_2(S_3 \times S_3) \mid 9$, and $n_3(S_3 \times S_3) \mid 4$. Accordingly, $n_2(D_{12}) \in \{1, 3\}$, $n_3(D_{12}) \in \{1, 2, 4\}$, $n_2(S_3 \times S_3) \in \{1, 3, 9\}$, and $n_3(S_3 \times S_3) \in \{1, 2, 4\}$. The condition $n_p \equiv 1 \pmod p$ eliminates $n_3 = 2$ for both groups. The standard presentation for D_{12} is $\langle s, r | s^2 = r^6 = 1, sr = r^{-1}s \rangle$. Some subgroups of order 4 are:

$$\langle s, r^3 \rangle = \{1, s, r^3, sr^3\}$$
$$\langle sr, r^3 \rangle = \{1, sr, r^3, sr^4\}$$
$$\langle sr^5, r^3 \rangle = \{1, sr^2, r^3, sr^5\}$$

By the above, this is exhaustive for $n_2(D_{12})$. All groups of order 3 are cyclic, and any cyclic group involving s is of order 2, so the only possible groups come from the rotations. The only Sylow 3-subgroup one is therefore $\langle r^2 \rangle$.

Now for $S_3 \times S_3$. Subgroups in each axis of order 2 will generate product subgroups of order 4. Subgroups of S_3 of order 2 are generated by transpositions: $(1\ 2), (2\ 3)$, and $(1\ 3)$. The corresponding subgroups of order 4 are constructed by making two choices with replacement from this list, and taking the product of subgroups of S_3 so-generated. There are $3^2 = 9$ ways to choose 2 items from a list of 3 elements with replacement, which is the largest possibility, so this is an exhaustive description of $Syl_2(S_3 \times S_3)$. The unique subgroup S_3 of order 3 consists of 3-cycles: $\{1, (1\ 2\ 3), (1\ 3\ 2)\}$. It is also normal, since it's of index 2; if N, N' are normal, then $N \times N'$ is a normal subgroup as well: $(g, g')(n, n')(g, g')^{-1} = (gng^{-1}, g'n'g'^{-1})$, and each element is in N and N' by normality of the axis subgroups. Therefore, the product of the 3-cycle subgroups is a normal Sylow p-subgroup, and $n_3(S_3 \times S_3) = 1$. □

Problem 2 (D&F 4.5.17). *If $|G| = 105$, then G has a normal Sylow 5-subgroup and a normal Sylow 7-subgroup.*

Proof. $|G| = 3 \cdot 5 \cdot 7$; accordingly, by Sylow's theorem, $n_5 \mid 21$ and $n_7 \mid 15$. Additionally, $n_5 \cong 1 \pmod 5$ and $n_7 \cong 1 \pmod 7$, and since $3 \equiv 3 \pmod 5$, $7 \equiv 2 \pmod 5$, and all the factors of 15 are less than 7, the only admissible values are $n_5 = n_7 = 1$. By Corollary 20, then, the Sylow 5- and 7-subgroups of G are normal. □

Problem 3 (D&F 4.5.33). *If P is a normal Sylow p-subgroup of G and H is any other subgroup of G, then $P \cap H$ is the unique Sylow p-subgroup of H.*

Proof. Since $P \trianglelefteq G$, $N_G(P) = G$, so $H \leq N_G(P)$. Then by the diamond isomorphism theorem, $P \cap H \trianglelefteq H$, and $PH/P \cong H/P \cap H$. In particular,

$$|PH|/|P| = |H|/|P \cap H| \Leftrightarrow |P \cap H| = \frac{|H||P|}{|PH|}$$

Since PH is a group, and trivially $H \leq PH$, by Lagrange's theorem $|H| \mid |PH|$, so letting $|PH|/|H| = k$,

$$|P \cap H| = \frac{|P|}{k} = \frac{p^\alpha}{k}$$

This must be an integer, which can only happen if $k = p^{\alpha'}$, meaning $|P \cap H| = p^{\alpha-\alpha'}$, i.e. $P \cap H$ is a p-subgroup. We now need to prove $p \nmid |H|/p^{\alpha-\alpha'} = |PH|/|P| = |PH|/p^\alpha$. Since $PH \leq G$, $|PH| \mid |G|$, so $|PH|/p^\alpha \mid |G|/p^\alpha$. The latter has no factor of p by assumption that P is a Sylow p-subgroup, so $P \cap H$ is in fact a Sylow p-subgroup. Since it's normal, it's unique. □

Problem 4 (D&F 5.1.4)**.** *If A and B are finite groups and p is a prime, then any Sylow p-subgroup of $A \times B$ is of the form $P \times Q$, where $P \in Syl_p(A)$ and $Q \in Syl_p(B)$. Additionally, $n_p(A \times B) = n_p(A)n_p(B)$, and both results generalize to a direct product of arbitrary arity.*

Proof. We may write $|A \times B| = |A| \cdot |B| = p^\alpha m$, where $p \nmid m$ and $1 \leq \alpha$. Take $A \times 1$ and $1 \times B$; these are subgroups of $A \times B$, and so have orders dividing $p^\alpha m$. Accordingly, their orders can be written $p^{\alpha'} m'$ and $p^{\alpha''} m''$, where $p \nmid m', m''$. Now, consider any of the Sylow p-subgroups H of $A \times B$; it will be of order p^α. The intersections of H with $A \times 1$ and $1 \times B$ are in fact subgroups of both parents by trivial application of the subgroup criterion. Their orders must divide both p^α and $p^{\alpha'} m'$ or $p^{\alpha''} m''$ by Lagrange's theorem; they then must be of the form p^β, and so their isomorphic image according to $A \times 1 \cong A$ and $1 \times B \cong B$ are Sylow p-subgroups A and B, since $p \nmid m', m''$ and isomorphisms preserve orders in the subgroup lattice.

We have by Sylow's theorem that if $|A \times B| = p^\alpha m$ where $p \nmid m$, then $n_p(A \times B) \mid m$ and $n_p \cong 1 \pmod p$. Additionally, from the property of the product group $|A \times B| = |A| \cdot |B|$, so $n_p(A \times B) \mid |A| \cdot |B|/p^\alpha$. $n_p(A)n_p(B) = \frac{|A|}{p^\alpha} \frac{|B|}{p^{\alpha'}} = \frac{|A \times B|}{p^{\alpha+\alpha'}}$. According to the above, $p^\alpha p^{\alpha'}$ is the order of Sylow p-subgroups, since they're the product of component p-subgroups. Therefore, the above is equal to $n_p(A \times B)$.

□

Problem 5 (D&F 7.1.11)**.** *If R is an integral domain and $x^2 = 1$ for some $x \in R$ then $x = \pm 1$.*

Proof. By un-distributing,

$$0 = 1 - 1 = 1 - x^2 = 1 - (x - x) - x^2 = (1 - x) + x(1 - x) = (1 + x)(1 - x),$$

Since integral domains don't have zero divisors, for the last term to equal zero, then either one or both terms must equal zero. So, $1 + x = 0 \Leftrightarrow x = -1$, or $1 - x = 0 \Leftrightarrow x = 1$. It should be noted that the "or" in $x = \pm 1$ is not exclusive, as $1 = -1 \Leftrightarrow 1 + 1 = 0$ holds in e.g. fields of characteristic 2, which are perfectly good integral domains. □

Problem 6 (D&F 7.1.14)**.** *If x is a nilpotent element of a commutative ring R, then*

1. *x is either zero or a zero-divisor,*

2. *rx is nilpotent for all $r \in R$,*

3. *$1 + x$ is a unit in R, and*

4. *the sum of a nilpotent element and a unit is a unit.*

Proof. If there exists positive integral m such that $x^m = 0$, then x is nilpotent. x can be zero or nonzero; if it's nonzero, then the set of positive integral n for which $x^n = 0$ is nonempty (according to existence of m) and bounded below by 2, so there's a least element m' (the smallest power to which x may be taken yielding zero). Then $x^{m'} = x(x^{m'-1}) = 0$; x and $x^{m'-1}$ are nonzero elements of R that multiply to zero, and so are zero divisors.

Applying commutativity,

$$(rx)^m = \underbrace{rx \cdot rx \cdots rx}_{m \text{ times}} = \underbrace{r \cdot r \cdots r}_{m \text{ times}} \overbrace{x \cdot x \cdots x}^{m \text{ times}} = r^m x^m = r^m \cdot 0 = 0$$

so rx is nilpotent for all $r \in R$.

Note that in

$$(1+x)(1 - x + x^2 + \cdots \pm x^{m'-1}) = 1 - x + x^2 + \cdots + x^{m-1} + x - x^2 + x^3 + \cdots \pm x^{m'}$$

all the inner terms additively cancel and $x^{m'} = 0$, yielding an overall result of 1. So, $(1+x)$ is a unit with inverse equal to the alternating polynomial.

Suppose $a \in R$ is a unit, i.e. there exists $a^{-1} \in R$ such that $aa^{-1} = 1$. Then $a + x = a(1 + a^{-1}x)$; $a^{-1}x$ is nilpotent by part 2, and by part 3, $1 + a^{-1}x$ is then a unit itself. So this is a product of two units, which has inverse $(1 + a^{-1}x)^{-1}a^{-1}$, and so the sum of a unit an a nilpotent element is a unit. $\square$