Math 541
Problem Set 8

4.5.8. The order or S_5 is $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 2^3 \cdot 3 \cdot 5$, so a Sylow 2-subgroup will have order $2^3 = 8$. The dihedral group D_8 has order 8 and acts naturally on the 4 corners of the square, so it can be made to act on 5 elements by leaving the fifth alone. The only group element that does nothing in this action is the identity, so the map $D_8 \to S_5$ given by $r \mapsto (1\ 2\ 3\ 4)$, $s \mapsto (2\ 4)$ is injective. Thus $\langle (1\ 2\ 3\ 4), (2\ 4) \rangle$ is a subgroup of S_5 of order 8. If we conjugate this by $(1\ 2)$, we have $(1\ 2)(1\ 2\ 3\ 4)(1\ 2) = (1\ 3\ 4\ 2)$ and $(1\ 2)(2\ 4)(1\ 2) = (1\ 4)$, so $\langle (1\ 3\ 4\ 2), (1\ 4) \rangle$ is another Sylow 2-subgroup.

7.1.5. (a) If a/b and c/d have odd denominators then so too does $a/b - c/d = (ad - bc)/bd$, and this will still be true after we write it in lowest terms; thus the set is closed under subtraction. Similarly, it is closed under multiplication since $a/b \times c/d = ac/bd$. It is not empty since $1/3$ is an element. Thus it is a subring of $\mathbb{Q}$.

(b) This is not closed under addition, since $1/6 + 1/6 = 1/3$.

(c) This is does not contain additive inverses, hence is not a group under addition.

(d) This is not closed under addition, since $1/4 + 1/4 = 1/2$.

(e) This is not closed under addition, since $1 + 1 = 2$.

(f) If a/b is written in lowest terms and a is even then b is odd. If a/b and c/d have even numerators and odd denominators then so too does $a/b - c/d = (ad - bc)/bd$, and this will still be true after we write it in lowest terms, so the set is closed under subtraction. Similarly, it is closed under multiplication since $a/b \times c/d = ac/bd$. It is not empty since $2/3$ is an element. Thus it is a subring of $\mathbb{Q}$.

7.1.6. Throughout, let S denote the subset.

(a) Let $f, g \in S$, so $f(q) = g(q) = 0$ for all $q \in \mathbb{Q} \cap [0, 1]$. S is closed under subtraction since $(f - g)(q) = f(q) - g(q) = 0 - 0 = 0$, so $f - g \in S$. S is closed under multiplication since $(fg)(q) = f(q)g(q) = 0 \cdot 0 = 0$. S is not empty since $0 \in S$. Thus S is a subring.

(b) It is well-known that this is closed under subtraction and multiplication and is not empty.

(c) This is not closed under subtraction. Let

$$f(x) = \begin{cases} 0 & \text{if } x = \frac{1}{3} \\ 1 & \text{otherwise} \end{cases} \qquad g(x) = \begin{cases} 0 & \text{if } x = \frac{2}{3} \\ 1 & \text{otherwise} \end{cases}.$$

Then $f \in S$ and $g \in S$, but $f - g$ vanishes on an infinite set.

(d) This is not closed under subtraction. Let

$$f(x) = \begin{cases} 0 & \text{if } x < \frac{1}{2} \\ 1 & \text{otherwise} \end{cases} \qquad g(x) = \begin{cases} 0 & \text{if } x > \frac{1}{2} \\ 1 & \text{otherwise} \end{cases}.$$

Then $f, g \in S$, but $f - g$ vanishes only at $\frac{1}{2}$.

(e) Let $f, g \in S$. S is closed under subtraction since

$$\lim_{x \to 1^-} [f(x) - g(x)] = \lim_{x \to 1^-} f(x) - \lim_{x \to 1^-} g(x) = 0 - 0 = 0.$$

S is closed under multiplication since

$$\lim_{x \to 1^-} f(x)g(x) = \lim_{x \to 1^-} f(x) \cdot \lim_{x \to 1^-} g(x) = 0 \cdot 0 = 0.$$

S is not empty since $0 \in S$. Thus S is a subring.

(f) Clearly S is nonempty and closed under subtraction. To show that it is closed under multiplication, it suffices to observe that

$$\begin{aligned}\sin mx \cos nx &= \tfrac{1}{2}[\sin(m+n)x + \sin(m-n)x] \\ \cos mx \cos nx &= \tfrac{1}{2}[\cos(m+n)x + \cos(m-n)x] \\ \sin mx \sin nx &= \tfrac{1}{2}[-\cos(m+n)x + \cos(m-n)x].\end{aligned}$$

If $m-n$ is negative, we can rewrite $\sin(m-n)x$ as $-\sin(n-m)x$ and $\cos(m-n)x$ as $\cos(n-m)x$. Thus S is a subring.

7.2.2. Let $p(x) = a_n x^n + \cdots + a_0 \in R[x]$, where $a_n \neq 0$. If there is a nonzero $b \in R$ such that $bp(x) = 0$ then $p(x)$ is a zero divisor. Conversely, suppose that $p(x)$ is a zero divisor and let $g(x) = b_m x^m + \cdots + b_0$, where $b_m \neq 0$, be of minimal degree such that $g(x)p(x) = 0$. The leading term of $g(x)p(x)$ is $b_m a_n x^{m+n}$, so $b_m a_n = 0$. Since R is commutative, $a_n b_m = 0$ as well. Now

$$a_n g(x) = a_n b_m x^m + a_n b_{m-1} x^{m-1} + \cdots = 0 + a_n b_{m-1} x^{m-1} + \cdots$$

has lower degree than $g(x)$ and $(a_n g(x))p(x) = a_n(g(x)p(x)) = 0$, but we assumed that $g(x)$ had minimal degree among such polynomials, so $a_n g(x) = 0$. Now

$$\begin{aligned}0 = g(x)p(x) &= g(x)(a_n x^n + a_{n-1}x^n + \cdots) \\ &= g(x)a_n x^n + g(x)(a_{n-1}x^{n-1} + \cdots) = 0 + g(x)(a_{n-1}x^{n-1} + \cdots)\end{aligned}$$

so $b_m a_{n-1} = 0$, so $a_{n-1}g(x) = 0$ by the same argument as above. Similarly $b_m a_{n-2} = 0$, $b_m a_{n-3} = 0$, and so on, so $b_m g(x) = 0$, as desired.

7.2.3. (a) Since addition in $R[[x]]$ is done componentwise, it is an abelian group under $+$ because R is; in fact, $R[[x]] \equiv R \times R \times R \times \cdots$ as abelian groups. For the rest, let $a(x) = a_0 + a_1 x + a_2 x^2 + \cdots$ be an element of $R[[x]]$ and similarly $b(x)$ and $c(x)$. The nth coefficient of $a(x)b(x)$ is

$$\sum_{i=0}^{n} a_i b_{n-i} = \sum_{\substack{0 \le i,j \le n \\ i+j=n}} a_i b_j$$

and since multiplication in R is commutative, this is the same as the nth coefficient of $b(x)a(x)$. The nth coefficient of $(a(x)b(x))c(x)$ is

$$\sum_{\substack{0 \le m,k \le n \\ m+k=n}} \left(\sum_{\substack{0 \le i,j \le m \\ i+j=m}} a_i b_j \right) c_k = \sum_{\substack{0 \le i,j,k \le n \\ i+j+k=n}} (a_i b_j) c_k$$

and since multiplication in R is associative, this is the same as the nth coefficient of $a(x)(b(x)c(x))$. The nth coefficient of $(a(x) + b(x))c(x)$ is

$$\sum_{\substack{0 \le i,j \le n \\ i+j=n}} (a_i + b_i)c_j = \sum_{\substack{0 \le i,j \le n \\ i+j=n}} (a_i c_j + b_i c_j) = \sum_{\substack{0 \le i,j \le n \\ i+j=n}} a_i c_j + \sum_{\substack{0 \le i,j \le n \\ i+j=n}} b_i c_j$$

which is the nth coefficient of $a(x)c(x) + b(x)c(x)$. The proof of distributivity on the other side is similar. The identity is $1 + 0x + 0x^2 + 0x^3 + \cdots$, since the nth coefficient of $1a(x)$ is $1a_n + 0a_{n-1} + 0a_{n-2} + \cdots + 0a_1 + 0a_0 = a_n$ and similarly $a(x)1 = a(x)$.

(b)

$$\begin{aligned}(1-x)(1+x+x^2+\cdots) &= (1+x+x^2+\cdots) - x(1+x+x^2+\cdots) \\ &= 1 + x + x^2 + \cdots - x - x^2 - x^3 - \cdots \\ &= 1.\end{aligned}$$

(c) Suppose that $a(x) = a_0 + a_1x + a_2x^2 + \cdots$ is a unit in $R[[x]]$, and let $b(x) = b_0 + b_1x + b_2x^2 + \cdots$ be its inverse. Then $1 = a(x)b(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots$, so $a_0b_0 = 1$, so a_0 is a unit in R. Convsersely, suppose $a(x)$ is given and we wish to find a $b(x)$ such that $a(x)b(x) = 1$; then we need to solve the equations

$$\begin{aligned}
1 &= a_0b_0 \\
0 &= a_0b_1 + a_1b_0 \\
0 &= a_0b_2 + a_1b_1 + a_2b_0 \\
0 &= a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0 \\
&\cdots
\end{aligned}$$

and if a_0 is invertible then we can do it:

$$\begin{aligned}
b_0 &= {a_0}^{-1} \\
b_1 &= -{a_0}^{-1}(a_1b_0) \\
b_2 &= -{a_0}^{-1}(a_1b_1 + a_2b_0) \\
b_3 &= -{a_0}^{-1}(a_1b_2 + a_2b_1 + a_3b_0) \\
&\cdots.
\end{aligned}$$