PMATH 347 Groups and Rings, Solutions to Assignment 7

1: Find all Sylow subgroups, and all normal subgroups, of S_4.

Solution: We have $|S_4| = 24$. Recall that in S_4, two permutations are conjugate if and only if they have the same form when written in cycle notation (that is, when they have the same number of cycles of each length). In S_4 there are six 4-cycles (of order 4), there are eight 3-cycles (of order 3), there are three pairs of disjoint 2-cycles (of order 2), there are six 2-cycles (also of order 2), and there is the identity element (or order 1).

Each Sylow 3-subgroup contains 2 elements of order 3 along with the identity element. Since S_4 has a total of eight elements of order 3, it follows that there are exactly 4 distinct Sylow 3-subgroups, each generated by one of the 3-cycles. Thus the Sylow 3-subgroups are

$$\begin{aligned}\big\langle(123)\big\rangle &= \big\{(1),(123),(132)\big\}\\ \big\langle(124)\big\rangle &= \big\{(1),(124),(142)\big\}\\ \big\langle(134)\big\rangle &= \big\{(1),(134),(143)\big\}\\ \big\langle(234)\big\rangle &= \big\{(1),(234),(243)\big\}\end{aligned}$$

The number of Sylow 2-subgroups divides 24 and is equal to 1 mod 2, so there are 1 or 3 Sylow 2-subgroups. There cannot be only 1 Sylow 2-subgroup, because each Sylow 2-subgroup contains 8 elements, and the union of all the Sylow 2-subgroups includes all 15 elements of order $1, 2, 4$ or 8. Thus there are 3 Sylow 2-subgroups. One of the Sylow 3-subgroups is $D_4 = \big\langle(1234),(13)\big\rangle$ and the others are conjugate to D_4. The Sylow 2-subgroups are

$$\begin{aligned}\big\langle(1234),(13)\big\rangle &= \big\{(1),(1234),(13)(24),(1432),(13),(14)(23),(24),(12)(34)\big\}\\ \big\langle(1243),(14)\big\rangle &= \big\{(1),(1243),(14)(23),(1342),(14),(13)(24),(23),(12)(34)\big\}\\ \big\langle(1324),(12)\big\rangle &= \big\{(1),(1324),(12)(34),(1423),(12),(14)(23),(34),(13)(24)\big\}\end{aligned}$$

Since normal subgroups are closed under conjugation, each normal subgroup must be a disjoint union of conjugacy classes, and it must include $\mathrm{Cl}(1) = \{(1)\}$. The sizes of the distinct conjugacy classes in S_4 are 1, 3, 6, 6 and 8 $\big($with $\big|\mathrm{Cl}(1)\big| = 1$, $\big|\mathrm{Cl}(12)\big| = 6$, $\big|\mathrm{Cl}(12)(34)\big| = 3$, $\big|\mathrm{Cl}(123)\big| = 8$ and $\big|\mathrm{Cl}(1234)\big| = 6\big)$. The only sums of some of the numbers 1, 3, 6, 6, 8, including 1, which are divisors of 24 are the sums 1, $1+3=4$, $1+3+8=12$ and $1+3+6+6+8=24$, and so the only possible normal subgroups are

$$\begin{aligned}\mathrm{Cl}(1) &= \big\{(1)\big\}\\ \mathrm{Cl}(1)\cup\mathrm{Cl}(12)(34) &= \big\{(1),(12)(34),(13)(24),(14)(23)\big\}\\ \mathrm{Cl}(1)\cup\mathrm{Cl}(12)(34)\cup\mathrm{Cl}(123) &= \big\{(1),(12)(34),(13)(24),(14)(23),(123),(132),(124),(142),(234),(242)\big\} = A_4\\ \mathrm{Cl}(1)\cup\mathrm{Cl}(12)\cup\mathrm{Cl}(12)(34)\cup\mathrm{Cl}(123)\cup\mathrm{Cl}(1234) &= S_4\,.\end{aligned}$$

Each of the above four sets is indeed a subgroup, so these are all of the normal subgroups of S_4.

2: (a) Prove that there is no simple group G with $|G| = 56$.

Solution: Suppose $|G| = 56$. The number of Sylow 7-subgroups divides 56 and is equal to 1 modulo 7, so there are 1 or 8 Sylow 7-subgroups. The number of Sylow 2-subgroups divides 56 and is equal to 1 modulo 2, so there are 1 or 7 Sylow 2-subgroups. The union of 8 Sylow 7-subgroups includes 48 elements of order 7. The union of 2 or more Sylow 2-subgroups (each containing 8 elements) includes at least 12 elements of orders 1, 2, 4 or 8 (since the intersection is a proper subgroup which contains at most 4 elements). Thus we cannot have both 8 Sylow 7-subgoups and 7 Sylow 2-subgroups (since $48 + 12 > 56$). Thus either G has a unique Sylow 7-subgroup or G has a unique Sylow 2-subgroup, and in either case, G is not simple.

(b) Show that every group of order 66 is isomorphic to one of the groups $\mathbb{Z}_{66}$, $\mathbb{Z}_{11} \times D_3$, $\mathbb{Z}_3 \times D_{11}$ or D_{33}.

Solution: Let G be a group with $|G| = 66$. Let H be a Sylow 11-subgroup of G and let K be a Sylow 3-subgroup of G. The number of Sylow 11-subgroups divides 66 and is equal to 1 mod 11, so there is only 1 Sylow 11-subgroup. Since H is the unique Sylow 11-subgroup, we have $H \trianglelefteq G$. Since $H \trianglelefteq G$, recall (or verify) that $HK \leq G$. Since $H \cap K = \{e\}$ (indeed the non-identity elements in H have order 11 and the non-identity elements in K have order 3), we have $HK = \{hk \mid h \in H\,,\ k \in K\}$ with the $11 \cdot 3 = 33$ listed elements distinct. Since HK is a group with $|HK| = 3 \cdot 11$, and since 3 does not divide $11 - 1 = 10$, we have $HK \cong \mathbb{Z}_{33}$ (by the classification of groups of order pq). Choose $a \in HK$ with $|a| = 33$ and choose $b \in G$ with $|b| = 2$ (which we can do by Cauchy's Theorem). Since $b \notin \langle a \rangle$ (because $|b|$ does not divide $|a|$), it follows that G is the disjoint union $G = \langle a \rangle \cup \langle a \rangle b$, that is

$$G = \{e, a, a^2, \cdots, a^{32}, b, ab, a^2b, \cdots, a^{32}b\}.$$

Since $|G/\langle a \rangle| = 2$ we have $\langle a \rangle \trianglelefteq G$. Since $\langle a \rangle \trianglelefteq G$ we have $bab^{-1} \in \langle a \rangle$, say $bab^{-1} = a^r$ with $r \in \mathbb{Z}_{33}$. Since $b^2 = e$ we have $a = b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^rb^{-1} = (bab^{-1})^r = (a^r)^r = a^{r^2}$. Since $|a| = 33$ and $a^{r^2} = a$, we have $r^2 = 1 \in \mathbb{Z}_{33}$. By listing the powers of 2 modulo 13, we see that in order to get $r^2 = 1 \in \mathbb{Z}_{33}$ we must have $r \in \{\pm 1, \pm 10\}$. Note that the value of $r \in \mathbb{Z}_{33}$ completely determines the operation on G: indeed when $bab^{-1} = a^r$ so that $ba = a^rb$, we have $ba^2 = a^rba = a^ra^rb = a^{2r}b$, and $ba^3 = a^{2r}b = a^{2r}a^rb = a^{3r}b$, and so on, so that in general $ba^k = a^{kr}b$. To be explicit, the operation on G is given by $(a^k)(a^\ell) = a^{k+\ell}$, and $(a^k)(a^\ell b) = a^{k+\ell}b$, and $(a^kb)(a^\ell) = a^ka^{\ell r}b = a^{k+\ell r}b$, and $(a^kb)(a^\ell b) = a^ka^{\ell \cdot r}b^2 = a^{k+\ell r}$. Since there only four possible values for r ($r = \pm 1, \pm 10$) it follows that, up to isomorphism, there are only 4 possibilities for G. Since the four listed groups are non-isomorphic (indeed $\mathbb{Z}_{66}$ has exactly 1 element of order 2, and $\mathbb{Z}_{11} \times D_3$ has exactly 3 elements of order 2, and $\mathbb{Z}_3 \times D_{11}$ has exactly 11 elements of order 2, and D_{33} has exactly 33 elements of order 2), it follows that G must be isomorphic to one of these four groups.

3: (a) List all irreducible polynomials of degree 1, 2 and 3 in $\mathbb{Z}_2[x]$, and determine the number of irreducible polynomials of degree 4 in $\mathbb{Z}_2[x]$.

Solution: The linear polynomials x and $x+1$ are both irreducible. The reducible quadratic polynomials are all products of two linear factors; x^2, $x(x+1) = x^2+x$ and $(x+1)^2 = x^2+1$. The other quadratic polynomial x^2+x+1 is irreducible. Each reducible cubic polynomial is either a product of 3 linear factors, or the product of a linear factor with the irreducible quadratic x^2+x+1; so the reducible cubics are x^3, $x^2(x+1) = x^3+x^2$, $x(x+1)^2 = x^3+x$, $(x+1)^3 = x^3+x^2+x+1$, $x(x^2+x+1) = x^3+x^2+x$ and $(x+1)(x^2+x+1) = x^3+1$. The other 2 cubics, x^3+x+1 and x^3+x^2+1 are irreducible.

The reducible quartic polynomials may be factored in one of the following ways; 5 of the reducible quartics factor into 4 linear factors (namely x^4, $x^3(x+1)$, $x^2(x+1)^2$, $x(x+1)^3$ and $(x+1)^4$); 3 of them factor into 2 linear factors and 1 irreducible quadratic factor (namely $x^2(x^2+x+1)$, $x(x+1)(x^2+x+1)$ and $(x+1)(x^2+x+1)$); 4 of them factor into 1 linear factor and one irreducible cubic factors (namely $x(x^3+x+1)$, $x(x^3+x^2+1)$, $(x+1)(x^3+x+1)$ and $(x+1)(x^3+x^2+1)$); and 1 of them factors into 2 irreducible quadratic factors (namely $(x^2+x+1)^2$). Thus there are $5+3+4+1 = 13$ reducible quartics, and so there are $16-13 = 3$ irreducible quartics. (If you *do* list them, you will find that the irreducible quartics are x^4+x+1, x^4+x^3+1 and $x^4+x^3+x^2+x+1$).

(b) Let $p \in \mathbb{Z}^+$ be an odd prime number. Find the number of irreducible monic cubic polynomials in $\mathbb{Z}_p[x]$.

Solution: In $\mathbb{Z}_p[x]$ there are p monic linear polynomials (namely $x-a$, $a \in \mathbb{Z}_p$). The reducible monic quadratics are as follows: there are p of the form $(x-a)^2$ and there are $\binom{p}{2} = \frac{p(p-1)}{2}$ of the form $(x-a)(x-b)$, where $a, b \in \mathbb{Z}_p$ with $a \neq b$. Thus there are $p+\frac{p(p-1)}{2} = \frac{p(p+1)}{2}$ reducible monic quadratics. There are p^2 monic quadratics (reducible or irreducible), so the number of irreducible monic quadratics is $p^2 - \frac{p(p+1)}{2} = \frac{p(p-1)}{2}$.

The reducible monic cubics are as follows: There are p of the form $(x-a)^3$, there are $p(p-1)$ of the form $(x-a)^2(x-b)$, there are $\binom{p}{3} = \frac{p(p-1)(p-2)}{6}$ of the form $(x-a)(x-b)(x-c)$, and there are $p \cdot \frac{p(p-1)}{2}$ of the form $(x-a)g(x)$, where $a, b, c \in \mathbb{Z}_p$ are distinct and g is a monic irreducible quadratic. Thus the number of reducible monic cubics is $p+p(p-1)+\frac{p(p-1)(p-2)}{6}+\frac{p^2(p-1)}{2} = \frac{1}{6}\,p\big(6+6(p-1)+(p-1)(p-2)+3p(p-1)\big) = \frac{1}{6}(2p^3+p)$. There are p^3 monic cubics, so the number of monic irreducible cubics is $p^3 - \frac{1}{6}(2p^3+p) = \frac{1}{3}(p^3-p)$.

4: (a) Determine which of the following polynomials $f(x)$ are irreducible in $\mathbb{Q}[x]$.

(i) $f(x) = \frac{5}{2}x^5 + \frac{9}{2}x^4 + 15x^3 + \frac{3}{7}x^2 + 6x + \frac{3}{14}$.

Solution: We multiply by 14 to get $5 \cdot 7\,x^5 + 9 \cdot 7\,x^4 + 15 \cdot 14\,x^3 + 3 \cdot 2\,x^2 + 6 \cdot 14\,x + 3$. This is irreducible by Eisenstein's criterion (with $p = 3$).

(ii) $f(x) = 55x^5 + 21x^2 + 45$

Solution: In $\mathbb{Z}_2[x]$ we have $f(x) = x^5 + x^2 + 1$. In $\mathbb{Z}_2$ we have $f(0) = 1$ and $f(1) = 1$, so f has no roots in $\mathbb{Z}_2$ and hence no linear factors in $\mathbb{Z}_2[x]$. If f is reducible in $\mathbb{Z}_2[x]$ then it must factor into an irreducible quadratic factor and an irreducible cubic factor. From Question 1(a), the only possibilities are $(x^2+x+1)(x^3+x+1)$ and $(x^2+x+1)(x^3+x^2+1)$. Neither of these is equal to f, so f is irreducible in $\mathbb{Z}_2[x]$, hence also in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$.

(iii)$f(x) = x^4 + x^3 + 3x^2 + 2x + 2$

Solution: The only possible roots in $\mathbb{Q}$ are ± 1 and ± 2. These are not roots, so f has no linear factors. If f is reducible, it must factor into 2 irreducible monic quadratics in $\mathbb{Z}[x]$. Say $f = (x^2+ax+b)(x^2+cx+d)$. Expand and equate coefficients and solve the resulting 4 equations to find that f factors as $f = (x^2+x+1)(x^2+2)$.

(b) Factor each of the following polynomials $f(x)$ into irreducible factors in $\mathbb{Q}[x]$, in $\mathbb{R}[x]$ and in $\mathbb{C}[x]$.

(i) $f(x) = 15x^4 - 2x^3 + 4x^2 + 11x + 2$

Solution: By the Rational Roots Theorem (the RRT), the only possible rational roots of $f(x)$ are the numbers $x = \pm 1, \pm 2, \pm\frac{1}{3}, \pm\frac{2}{3}, \pm\frac{1}{5}, \pm\frac{2}{5}, \pm\frac{1}{15}$ and $\pm\frac{2}{15}$. We try the first few of these and find that $f(1) = 30$, $f(-1) = 12$, $f(2) = 264$, $f(-2) = 252$, $f(\frac{1}{3}) = \frac{56}{9}$, $f(-\frac{1}{3}) = -\frac{26}{27}$ and $f(\frac{2}{3}) = 0$, so $x = \frac{2}{3}$ is a root of $f(x)$. We divide $f(x)$ by $3x+2$ and find that $f(x) = (3x+2)g(x)$ where $g(x) = (5x^3-4x^2+4x+1)$. The remaining roots of $f(x)$ must be roots of $g(x)$. By the RRT the only possibilities are $x = \pm 1$ and $\pm\frac{1}{5}$. We have already tried $x = \pm 1$, so the only possible roots are $x = \pm\frac{1}{5}$. We have $g(\frac{1}{5}) = \frac{546}{125}$ and $g(-\frac{1}{5}) = 0$, so the only rational root of $g(x)$ is $x = -\frac{1}{5}$. We divide by $5x+1$ to get $g(x) = (5x+1)h(x)$ where $h(x) = (x^2 - x + 1)$. By the Quadratic Formula, the complex roots of $h(x)$ are $\frac{1\pm\sqrt{3}\,i}{2} = e^{\pm i\pi/3}$. Since $h(x)$ is of degree 2 and has no roots in $\mathbb{Q}$ or in $\mathbb{R}$, it follows that $h(x)$ is irreducible in $\mathbb{Q}[x]$ and in $\mathbb{R}[x]$. Thus in both $\mathbb{Q}[x]$ and $\mathbb{R}[x]$, $f(x)$ factors into irreducible polynomials as

$$f(x) = (3x + 2)(5x + 1)(x^2 - x + 1)$$

and in $\mathbb{C}[x]$, $f(x)$ factors further as

$$f(x) = (3x + 2)(5x + 1)(x - e^{\frac{i\pi}{3}})(x - e^{-i\pi/3}).$$

(ii) $f(x) = 3x^5 - x^4 - 6x^3 + 2x^2 - 6x + 2$.

Solution: First we find all rational roots. By the RRT the only possibilities are $x = \pm 1, \pm 2, \pm\frac{1}{3}$ and $\pm\frac{2}{3}$. We try the first few of these and find $f(1) = -6$, $f(-1) = 12$, $f(2) = 30$, $f(-2) = -42$), $f(\frac{1}{3}) = 0$ and so $x = \frac{1}{3}$ is a root. Use long division to get $f(x) = (3x-1)g(x)$ where $g(x) = (x^4 - 2x^2 - 2)$. By the Quadratic Formula, $g(x) = 0 \iff x^2 = \frac{2\pm\sqrt{4+8}}{2} = 1 \pm \sqrt{3}$. When $x^2 = 1 + \sqrt{3}$ we obtain two real roots $x = \pm\sqrt{1+\sqrt{3}}$, and when $x^2 = 1 - \sqrt{3}$ we find two imaginary roots $x = \pm i\sqrt{\sqrt{3}-1}$. Thus

$$\begin{aligned}
f(x) &= \big(3x-1\big)\big(x-\sqrt{\sqrt{3}+1}\big)\big(x+\sqrt{\sqrt{3}+1}\big)\big(x-i\sqrt{\sqrt{3}-1}\big)\big(x+i\sqrt{\sqrt{3}-1}\big) \in \mathbb{C}[x]\,,\\
f(x) &= \big(3x-1\big)\big(x-\sqrt{\sqrt{3}+1}\big)\big(x+\sqrt{\sqrt{3}+1}\big)\big(x^2+(\sqrt{3}-1)\big) \in \mathbb{R}[x]\,, \text{ and}\\
f(x) &= (3x-1)(x^4-2x^2-2) \in \mathbb{Q}[x].
\end{aligned}$$

Note that $x^2 + \sqrt{\sqrt{3}-1}$ is irreducible in $\mathbb{R}[x]$ because it has no real roots, and note that $g(x) = x^4 - 2x^2 - 2$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein's Criterion.