October 6, 2025

Problem Set 4 Solutions

Exercise 1. Let D_n be the dihedral group of rigid symmetries of a regular n-gon, $n \geq 3$:

$$D_n = \langle r, s \mid r^n = 1, s^2 = 1, srs = r^{-1} \rangle = \{1, r, \dots r^{n-1}, s, sr, \dots sr^{n-1}\}.$$

(a) Show that $sr^i s = r^{-i}$ for all $0 \leq i \leq n-1$.

(b) Identify the element $r^2 sr^{-1} sr^{-4} s \in D_n$ in the list of all elements of D_n.

(c) Find all elements $x \in D_n$ such that $gxg^{-1} = x$ for all $g \in D_n$. The elements with this property are called *central* in the group.

(d) Find the order of the elements $x = sr^2$ and $y = r^2$ in D_n.

Solution 1. (a) The equation $srs = r^{-1}$ (for $i = 1$) holds as one of the defining relations in D_n. If $i = 0$ we have $s^2 = r^0 = 1$ which is one of the defining relations. Now let $i \geq 2$. Using the defining relation $s^2 = 1$, we can write

$$sr^i s = (srs)(srs) \dots (srs) = (r^{-1})^i = r^{-i}.$$

The factors (srs) are repeated i times.

(b) Using the relations of the form $sr^i s = r^{-i}$, we compute (remember that the powers of r are integers modulo n):

$$r^2 sr^{-1}(sr^{-4}s) = (r^2 s)r^{-1} r^4 = sr^{-2} r^{-1} r^4 = sr.$$

(c) Let $x \in D_n$. Then $gxg^{-1} = x$ for all $g \in D_n$ if and only if $sxs = x$ and $rxr^{-1} = x$. "Only if" holds because s and r are elements of D_n. "If" holds because any element of D_n is a product of the generators s and r.

Now let $x = r^k$, $0 \leq k \leq n-1$. Clearly $rr^k r^{-1} = r^k$ for all k, so that r^k commutes with all rotations. Suppose that $sr^k s = r^k$. By the relation obtained in (1) we have $sr^k s = r^{-k}$. If $r^k = r^{-k}$, then $r^{2k} = 1$. This is only possible if $2k = tn$ for a nonnegative integer t. Since $2k \leq 2(n-1)$, the only possibilities for t are $t = 0$ and $k = 0$, or $t = 1$ and $2k = n$. In the first case, $x = 1$, and in the second case n must be even and $x = r^{n/2}$ satisfies the condition.

Suppose $x = sr^k$. Then $rxr^{-1} = rsr^{k-1} = sr^{-1} r^{k-1} = sr^{k-2}$. The equation $sr^{k-2} = sr^k$ implies $r^2 = 1$, which is false in D_n. Therefore no elements of the form sr^k satisfy the condition.

Finally, if n is odd, the only element $x \in D_n$ such that $gxg^{-1} = x$ for all $g \in D_n$ is 1. If n is even, then $x \in \{1, r^{n/2}\}$.

(d) We need to find the smallest positive integer k such that $x^k = (sr^2)^k = 1$. Using the relations $sr^i s = r^{-i}$, we compute

$$sr^2 sr^2 = r^{-2} r^2 = 1.$$

Therefore, the order of $x = sr^2$ in any group D_n, $n \geq 3$, is 2.
Now consider the element $r^2 \in D_n$. We have to find the smallest positive integer k such that $r^{2k} = 1$. This is equivalent to the requirement $n | 2k$. If n is even, the smallest positive integer solution is $k = n/2$. If n is odd, then $k = n$. Therefore, the order of r^2 is $n/2$ if n is even, and n if n is odd. For example, the order of r^2 is 5 in D_5 and 4 in D_8.

Exercise 2. Consider the dihedral group $D_6 = \langle s, r \mid s^2 = 1, r^6 = 1, srs = r^{-1} \rangle$.

(a) Show that $R = \{1, r, r^2, r^3, r^4.r^5\} \subset D_6$ is a normal subgroup.

(b) Show that $H = \{1, r^3\} \subset D_6$ is a normal subgroup.

(c) Show that $T = \{1, sr^3\} \subset D_6$ is a subgroup in D_6 that is not normal.

Solution 2. (a) For any rotation r^k we have $r^k r^i r^{-k} = r^i$ and for any element of the form sr^k we compute $(sr^k)r^i(sr^k)^{-1} = sr^k r^i r^{-k} s^{-1} = sr^i s = r^{-i} \in R$. Here we used the relations $s^2 = 1$, $sr^i s = r^{-1}$. Therefore, the subgroup of rotations is normal in D_6 (the same holds for any dihedral group).

(b) Clearly H is a subgroup because $(r^3)^2 = 1$ in D_6. We have to show that for any $g \in D_6 = \{1, r, \dots r^5, s, sr, \dots sr^5\}$, $gr^3g^{-1} \in H$. We compute:

$$r^i r^3 r^{-i} = r^3 \in H, \qquad (sr^i)r^3(sr^i)^{-1} = sr^i r^3 r^{-i} s = sr^3 s = r^{-3} = r^3 \in H.$$

The last equality holds because $r^6 = 1$ in D_6. So $H \subset D_6$ is a normal subgroup.

(c) First we have to check that T is a subgroup. We have $(sr^3)^2 = sr^3 sr^3 = r^{-3}r^3 = 1$. So T is a subgroup of two elements in D_6. Next we need to determine if the condition $g(sr^3)g^{-1} \in T$ holds for all $g \in D_6 = \{1, r, \dots r^5, s, sr, \dots sr^5\}$. We compute $r(sr^3)r^{-1} = rsr^2 = sr^{-1}r^2 = sr \notin T$. Here we used the identity $rs = sr^{-1}$. Therefore $T \subset D_6$ is not a normal subgroup.

Exercise 3. (a) Show that if G is such that $a^2 = e$ for all $a \in G$ then G is abelian.

(b) Show that any group of order 4 is abelian.

(b) Let G be an abelian group and $a, b \in G$ two elements of finite order. Suppose that $\mathrm{o}(a)$ and $\mathrm{o}(b)$ are mutually prime. Show that ab is of finite order $\mathrm{o}(ab) = \mathrm{o}(a)\mathrm{o}(b)$.

Solution 3. (a) Let a, $b \in G$. We need to show that $ab = ba$. By the hypothesis $a^2 = e$, $b^2 = e$ and $(ab)^2 = e$. Multiply the last equation on both sides on the right by b:

$$b = (a \cdot b)^2 \cdot b = a \cdot b \cdot a \cdot b \cdot b = a \cdot b \cdot a \cdot b^2 = a \cdot b \cdot a.$$

Then multiply on the right by a:

$$a \cdot b \cdot a \cdot a = a \cdot b \cdot a^2 = a \cdot b = b \cdot a.$$

Therefore G is abelian.

(b) Let $x \in G$, $x \neq e$. Then x has order 2 or 4. If x has order 4, then x is a generator of the group G and G is cyclic and so is abelian. If G is not cyclic then all elements of G satisfy the identity $x^2 = e$ and then by part (a), G is abelian.

(c) Suppose m is the order of $a \in G$ and n is the order of $b \in G$ and that m and n are coprime. This means that, m and n are the minimum natural values such that $a^m = e$ and $b^n = e$ and $\gcd(m, n) = 1$. Then, since G is abelian, $(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e$ (here we use that G is abelian). This implies that $\mathrm{o}(ab)|mn$.

Conversely, let $\mathrm{o}(ab) = h$, we want to prove that $mn|h$. As $e = (ab)^h = (ab)^{mh} = (a^m)^h \cdot b^{mh}$, we have that $b^{mh} = e$ and so $n|(mh)$. Therefore, since $(m, n) = 1$, n divides h. With the same argument prove that $m|h$. This implies that $lcm(m, n) = mn$ divides h. We can conclude that $\mathrm{o}(ab) = mn = \mathrm{o}(a)\mathrm{o}(b)$, as desired.

Exercise 4. Let p be a prime. Show that any group of order p is cyclic.

Solution 4. Let p be a prime number and G a group of order p. Then G has order bigger than 1. Let $g \in G$ such that $g \neq e$. Then the group generated by g, denoted by $\langle g \rangle$, contains more than one element. Since $\langle g \rangle \subseteq G$, by Lagrange theorem its order divides p. By the fact that $\langle g \rangle$ has more than one element, it follows that the order of $\langle g \rangle$ is p. Therefore, we can conclude that $\langle g \rangle = G$.

Exercise 5. Pollard's algorithm for factorizing large integers works as follows:
Suppose you are given an integer n and you want to find its prime factors. Take a small number a and check that $\gcd(a, n) = 1$ (if not, you already have found a nontrivial factor of n). For $m = 2, 3, \dots$, compute $\gcd(a^K - 1, n)$, where $K = \mathrm{lcm}(2, 3, \dots m)$. If $\gcd(a^K - 1, n) > 1$, then you have found a nontrivial factor of n. If $\gcd(a^K - 1, n) = 1$, increase $m \leq \sqrt{n}$ until you get a nontrivial factor of n.

(a) Explain why Pollard's algorithm works well for finding prime factors p of n in case when $(p - 1)$ is a product of small powers of small primes. Use Fermat's little theorem.

(b) Obtain the prime factorization of $n = 15041$ using Pollard's algorithm. You can take $a = 2$ and use the following website to compute the gcd of two integers: `http://www.alcula.com/calculators/math/gcd/`.

Solution 5. (a) Suppose that p is a prime factor of n, and a is not divisible by p. Then Fermat's little theorem tells us that $a^{p-1} \equiv 1 \bmod(p)$, therefore $a^{p-1} - 1$ is divisible by p and so $\gcd(a^{p-1} - 1, n)$ is a multiple of p. If $(p-1)$ is a product of small powers of small primes, the number $K = \operatorname{lcm}(2, 3, \dots m)$ is a multiple of $(p-1)$ for a relatively small m. Then we have $K = t(p-1)$ for some integer t, and $a^K = a^{t(p-1)} \equiv 1 \bmod(p)$. Therefore, $a^K - 1$ is divisible by p, and $\gcd(a^K - 1, n) > 1$ produces a multiple of p. We can obtain the prime factor p in a relatively small number of steps m, if $p - 1$ divides $\operatorname{lcm}(2, 3, \dots m)$ of the first few natural numbers. This happens when $p - 1$ is a product of small powers of small primes (such numbers are also called *powersmooth*).

(b) Let $n = 15041$. Then $a = 2$ is coprime with n.
Step 1: Let $m = 2$, we have $K = m = 2$ and $\gcd(a^K - 1, n) = \gcd(2^2 - 1, 15041) = 1$.
Step 2: Let $m = 3$. Then $K = \operatorname{lcm}(2, 3) = 6$ and $\gcd(a^K - 1, n) = \gcd(2^6 - 1, 15041) = \gcd(63, 15041) = 1$.
Step 3: Let $m = 4$. Then $K = \operatorname{lcm}(2, 3, 4) = 12$ and $\gcd(a^K - 1, n) = \gcd(2^{12} - 1, 15041) = \gcd(4095, 15041) = 13$.
Therefore, 15041 is divisible by 13, and we have $15041 : 13 = 1157$. Repeating the same algorithm for $n = 1157$ and $a = 2$, we get
Step 1: Let $m = 2$, we have $\gcd(a^K - 1, n) = \gcd(2^2 - 1, 1157) = 1$.
Step 2: Let $m = 3$. Then $\gcd(a^K - 1, n) = \gcd(2^6 - 1, 1157) = \gcd(63, 1157) = 1$.
Step 3: Let $m = 4$. Then $\gcd(a^K - 1, n) = \gcd(2^{12} - 1, 1157) = \gcd(4095, 1157) = 13$.
Therefore, 1157 is divisible by 13 and we get $1157 : 13 = 89$, which is a prime. Finally we get $15041 = 13^2 \cdot 89$.

Note that in our case $p - 1 = 12 = 2^2 \cdot 3$. In practice Pollard's algorithm can be efficient to find much larger prime factors p of large integers n, but only if $p - 1$ is a product of many relatively small primes.