Group Theory 2014–2015

Solutions to the exam of 4 November 2014

13 November 2014

Question 1

(a) For every number n in the set $\{1, 2, \ldots, 2013\}$ there is exactly one transposition $(n\, n+1)$ in σ, so σ is a product of an odd number of transpositions. We conclude that σ is an odd permutation, hence its sign is -1.

(b) Starting, as always, from the right, we see that $\sigma = (123 \ldots 2014)$, a 2014-cycle.

(c) We have that $11 \equiv 1 \bmod 2$ and $2014 \equiv 14 \equiv 6 \bmod 8$. This gives $r^4 s^{11} r^{2014} = r^4 s^1 r^6$. Now notice that $r^{-a} s = s r^a$ for any integer a. We use this to obtain:

$$r^4 s^{11} r^{2014} = r^4 s^1 r^6 = r^4 r^{-6} s = r^{-2} s = r^6 s.$$

(d) Take for example

$$M = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

It is easy to check that

$$M^t M = MM = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Moreover, we have $\det(M) = -1$. We conclude that $M \in O_3(\mathbb{R})$, but $M \notin SO_3(\mathbb{R})$. Furthermore, M is of course not a diagonal matrix.

Question 2

(a) This is false. Let for example $G = \mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$. Then G is abelian, so its conjugacy classes all consist of just one element. This means that we can pick $H = \{\overline{1}\}$. This is not even a subgroup of G, since $\overline{1} + \overline{1} = \overline{0} \notin H$ so, in particular, H is not a normal subgroup of G.

It *is* true that, if H is a subgroup of G and moreover a union of conjugacy classes, then H is normal in G. This happens to be the definition of a normal subgroup.

(b) This is true. We show that $G \times \{e_H\} \subset G \times H$ is a proper normal subgroup of $G \times H$. Because G is nontrivial, $G \times \{e_H\}$ also is nontrivial and because H is nontrivial, $G \times \{e_H\}$ is not the entire group $G \times H$. Let $\varphi\colon G \times H \to H$ be the map given by $(g, h) \mapsto h$. This is a homomorphism, since $\varphi\big((g_1, h_1)\big)\varphi\big((g_2, h_2)\big) = h_1h_2 = \varphi\big((g_1g_2, h_1h_2)\big)$ for $g_1, g_2 \in G$, $h_1, h_2 \in H$. Furthermore, $(g, h) \in \ker\varphi \Leftrightarrow \varphi\big((g, h)\big) = e_H \Leftrightarrow h = e_H$, so $\ker\varphi = G \times \{e_H\}$ and the latter group is a normal subgroup of $G \times H$ by the first isomorphism theorem.

One can also avoid using the first isomorphism theorem and prove directly that $G \times \{e_H\} \subset G \times H$ is a normal subgroup.

(c) This is false. Let G be any group with $|G| = 3 \cdot 2014 = 2 \cdot 3 \cdot 19 \cdot 53$. Apply the Sylow theorems with $p = 53$. We get that the number n of subgroups of G of order 53 satisfies $n \equiv 1 \bmod 53$ and $n | 2 \cdot 3 \cdot 19 = 114$. The latter gives $n \leq 114$, so $n \equiv 1 \bmod 53$ implies $n \in \{1, 54, 107\}$. Only $n = 1$ satisfies $n|114$, so there is a unique $H \leq G$ of order 53. By the reasoning on page 114 of Armstrong, H is normal. Since $1 < |H| < |G|$, the group G can not be simple.

Note that $p = 19$ also works, while $p = 2$ and $p = 3$ do not.

(d) This is true. Recall from Theorem 5.2 in Armstrong's book that $H \cap K$ is indeed a subgroup. So we only need to show that it is normal in G. Let $x \in H \cap K$ and $g \in G$. Because $x \in H$ and H is normal in G, we have that $gxg^{-1} \in H$. Similarly, $gxg^{-1} \in K$. Therefore, $gxg^{-1} \in H \cap K$, which shows what we wanted.

(e) This is true. We first prove that $x \ker\varphi \subseteq \{g \in G : \varphi(g) = \varphi(x)\}$. Let $g \in x\ker\varphi$. Then $g = xh$ for some $h \in \ker\varphi$. Because φ is a homomorphism, we have $\varphi(g) = \varphi(xh) = \varphi(x)\varphi(h) = \varphi(x)e_H = \varphi(x)$. For the reverse inclusion, let $g \in G$ be such that $\varphi(g) = \varphi(x)$. Then, again using that φ is a homomorphism, $\varphi(x^{-1}g) = \varphi(x)^{-1}\varphi(g) = e_H$. Therefore $x^{-1}g \in \ker\varphi$, which is equivalent to $g \in x\ker\varphi$.

(f) This is true. That G/Z is cyclic means that there exists an $x \in G$ such that every element of G/Z is of the form $(xZ)^n$ for some integer n. Remember that $(xZ)^n$ is defined as x^nZ. Because the elements of G/Z, that is, the left cosets of Z in G, partition G, this implies that for every $g \in G$ there is some power n and some $z \in Z$ such that $g = x^nz$. If also $h \in G$, then similarly $h = x^mz'$ for some integer m and $z' \in Z$. Hence $gh = x^nzx^mz' = x^mz'x^nz = hg$, where we used that powers of x commute with each other and elements of Z commute with everything. This shows that G is abelian.

Note that G being abelian implies that $Z = G$, which means that G/Z is trivial. So we actually proved that if G/Z is cyclic, then it is automatically trivial.

Question 3

(a) The dihedral group D_5 can be represented by the set of elements

$$\{e, r, r^2, r^3, r^4, s, sr, sr^2, sr^3, sr^4\}$$

which satisfy $r^5 = s^2 = e$ and $srs = r^{-1}$. For every group G the identity element e is conjugate only to itself, so one conjugacy class is given by $\{e\}$. To find all the elements conjugate to r^k for $k \in \{1,2,3,4\}$ notice first that $r^l r^l (r^l)^{-1} = r^l r^k r^{-l} = r^{l+k-l} = r^k$ for all $l \in \{0,1,2,3,4\}$. Conjugation of r^k with sr^l gives $sr^l r^k (sr^l)^{-1} = sr^l r^k r^{-l} s = sr^k s = r^{-k}$, which shows that r is conjugate to $r^{-1} = r^4$ and r^2 is conjugate to $(r^2)^{-1} = r^3$. So two conjugacy classes are $\{r, r^4\}$ and $\{r^2, r^3\}$. To determine the elements conjugate to s let us first determine $r^l s (r^l)^{-1} = r^l s r^{-l} = sr^{-2l}$. For $l = 1$ this gives that s is conjugate to $sr^{-2} = sr^3$, for $l = 2$ it follows that s is conjugate to $sr^{-4} = sr$, for $l = 3$ the element s is conjugate to $sr^{-6} = sr^{-1} = s^4$ and for $l = 4$ the element s is conjugate to $sr^{-8} = sr^{-3} = sr^2$. So s, sr, sr^2, sr^3 and sr^4 are all in the same conjugacy class. Since all other elements of D_5 are found to be in other classes these five elements must form a conjugacy class. So the conjugacy classes of D_5 are

$$\{e\}, \quad \{r, r^4\}, \quad \{r^2, r^3\} \quad \text{and} \quad \{s, sr, sr^2, sr^3, sr^4\}.$$

Here is an alternative argument: recall from Example (v) on page 93 and 94 of the book that for a finite group, the size of each conjugacy class divides the order of the group. Knowing this, less computations have to be performed to determine the conjugacy classes of D_5. These must then namely have 1, 2, 5 or 10 elements because the order of D_5 is 10. Since $\{e\}$ is a conjugacy class, the remaining 9 elements in D_5 can not form a conjugacy class of order 10. By checking that s is conjugate to sr, sr^2, sr^3 and sr^4 (as above, using $r^l s (r^l)^{-1} = r^l s r^{-l} = sr^{-2l}$ for $l \in \{1,2,3,4\}$) one can immediately conclude that these 5 elements must form one conjugacy class (more than 5 is not possible). It is also not possible that the remaining 4 elements, r, r^2, r^3 and r^4, are all in one conjugacy class because 4 is not a factor of 10. By checking that $srs = r^{-1} = r^4$ and $sr^2 s = r^{-2} = r^3$ it follows that $\{r, r^4\}$ and $\{r^2, r^3\}$ are conjugacy classes.

(b) By the Counting Theorem we know that the total number of distinct colorings of the 5 diagonals is given by

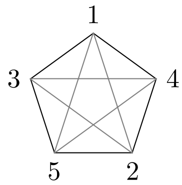
$$\frac{1}{|D_5|} \sum_{g \in D_5} |X^g|$$

where X^g is the set of distinct colorings of the 5 diagonals which are left invariant under the action (in this case rotation in 3-space) by $g \in D_5$. If g and h are conjugate, then $|X^g| = |X^h|$, so one has to determine the sizes of $|X^g|$ only for 4 representatives of the 4 conjugacy classes of D_5. Take e, r, r^2 and s as the representatives.

For e, all 5 diagonals are left invariant and each diagonal can have n different colors, so there are n^5 distinct ways of coloring the 5 diagonals.

For r (rotation by $\frac{2\pi}{5}$), none of the diagonals are left invariant, so all diagonals must have the same color, which leaves n distinct possibilities for coloring the diagonals. The same is true for r^2.

To visualize the action of s, associate s with rotation (mirroring) around the diagonal through 1 and the midpoint between 2 and 5. The diagonal 3—4 is then sent to itself, the diagonals 1—2 and 1—5 are interchanged and the diagonals 3—2 and 5—4 are interchanged. This shows that 3 diagonals can be colored independently, giving n^3 possibilities.



The total number of distinct colorings of the 5 diagonals is therefore given by

$$\frac{|X^e| + 2|X^r| + 2|X^{r^2}| + 5|X^s|}{10} = \frac{n^5 + 4n + 5n^3}{10}.$$

Question 4

We will show that the symmetric group S_n and the dihedral group $D_{n!/2}$ are only isomorphic for $n = 2$ and $n = 3$.

Case $n = 2$: Both $S_2 = \{e, (12)\}$ and $D_1 = \{e, s\}$ consist of just two elements and are thus isomorphic to $\mathbb{Z}_2$.

Case $n = 3$: The group S_3 is generated by the permutations $\rho = (123)$ and $\sigma = (12)$, which satisfy the relations $\rho^3 = e$, $\sigma^2 = e$ and $\sigma\rho = \rho^{-1}\sigma$. Since $\#S_3 = 6$, the elements $\rho^k\sigma^l$ for $k = 0, 1, 2$ and $l = 0, 1$ are all distinct, allowing us to conclude that $S_3 = \{e, \rho, \rho^2, \sigma, \rho\sigma, \rho^2\sigma\}$, which is isomorphic to D_3.

An explicit isomorphism $\varphi\colon S_3 \to D_3$ is given by $\varphi(\rho^k\sigma^l) = r^k s^l$. This is a (well-defined) group homomorphism because ρ and σ satisfy the same relations as r and s. It is surjective because the generators r and s of D_3 are both in the image of φ, so bijectivity of φ follows from the fact that $\#S_3 = \#D_3 = 6$.

Case $n \geq 4$: We can show that S_n and $D_{n!/2}$ are not isomorphic for $n \geq 4$ by finding some property which they do not share. We give some examples. So let $n \geq 4$.

- The number of 3-cycles in S_n is $2 \cdot \binom{n}{3} \geq 8$, so S_n contains at least 8 elements of order 3. On the other hand, $D_{n!/2}$ has just 2 elements of order 3, namely $r^{n!/6}$ and $(r^{n!/6})^2$. (Elements of the form $r^k s$ all have order 2 and $(r^k)^3 = e$ if and only if $3k$ is a multiple of $\frac{1}{2}n!$.)

- Every n-cycle in S_n can be uniquely written as $(1a_2a_3 \ldots a_n)$ with $a_i \in \{2, 3, \ldots, n\}$ all distinct, so there are $(n-1)!$ of them. This means that S_n contains at least $(n-1)!$ elements of order n. The only elements of $D_{n!/2}$ that could have order n are of the form $r^{i(n-1)!/2}$ for $i = 1, 2, \ldots, n-1$ (with $\gcd(i, n) = 1$), so $D_{n!/2}$ contains at most $n - 1$ elements of order n, which is less than $(n-1)!$.

- The element $r \in D_{n!/2}$ has order $\frac{1}{2}n!$, while S_n contains no elements of this order. This is true because any element $\sigma \in S_n$ is either an n-cycle, in which case $\operatorname{ord}(\sigma) = n = \frac{n!}{(n-1)!} < \frac{1}{2}n!$, or it can be written as a product of disjoint cycles of length strictly smaller than n, in which case $\operatorname{ord}(\sigma) \leq (n-1)! = \frac{1}{n}n! < \frac{1}{2}n!$.

- The dihedral group $D_{n!/2}$ has two conjugacy classes that consist of just one element, namely $\{e\}$ and $\{r^{n!/4}\}$. The only conjugacy class in S_n consisting of just one element is $\{e\}$ since permutations of the same cycle type are conjugate in this group and one can write down multiple permutations for every other cycle type. (An alternative formulation: $D_{n!/2}$ has center $\{e, r^{n!/4}\}$, while the center of S_n is trivial.)
- The commutator subgroup $[D_{n!/2}, D_{n!/2}] = \langle r^2 \rangle = \{e, r^2, r^4, \ldots, r^{n!/2-2}\}$ has $n!/4$ elements (and is abelian) if $n \geq 4$, while $[S_n, S_n] = A_n$ has $n!/2$ elements (and is not abelian). (See Example (viii) and Example (ix) from chapter 15 of the book for the computations.)

Question 5

Let p denote a prime number, let G be a finite group and let $\varphi \colon G \to G$ denote the map $x \mapsto x^p$. We will first show that if φ is a bijection, then the order of G is not divisible by p. We do this by contraposition. Assume the order of G is divisible by p. By Cauchy's theorem, this implies the existence of an element $x \in G$ with order p. We then see that $\varphi(x) = x^p = e = e^p = \varphi(e)$. Since $x \neq e$, we see that φ is not injective, hence it is not a bijection.

We will now show that if the order of G is not divisible by p, then φ is a bijection. Denote the order of G by n. Note that for any finite set X, a map $X \to X$ is surjective if and only if it is injective. Therefore, in order to prove that φ is a bijection, it is enough to prove that it is an injection or to prove that it is a surjection. We will present two different proofs. The first one proves the injectivity of φ, and also provides us with an inverse function. The second one proves the surjectivity of φ.

- We will first show that φ is injective. Note that φ is not, in general, a homomorphism. It is therefore not enough to show that the set $\{x \in G : \varphi(x) = e\}$ is trivial. To show injectivity, assume that $\varphi(x) = \varphi(y)$ for some $x, y \in G$. Then by definition $x^p = y^p$. By Lagrange's theorem, we also see that $x^n = e = y^n$, where n denotes the order of G. Since we assumed that p does not divide n, and p is prime, we see that $\gcd(n, p) = 1$. By Euclid's algorithm, there exist $a, b \in \mathbb{Z}$ such that $an + bp = 1$. We now see that

  $$x = x^{an+bp} = (x^n)^a (x^p)^b = (y^n)^a (y^p)^b = y^{an+bp} = y,$$

  so $\varphi(x) = \varphi(y)$ implies that $x = y$. We therefore conclude that φ is injective, hence bijective. This method also gives us the inverse function of φ. If we define $\psi \colon G \to G$ by $x \mapsto x^b$, where b is as above, then

  $$\psi\big(\varphi(x)\big) = \varphi\big(\psi(x)\big) = x^{bp} = x^{1-an} = x(x^n)^{-a} = xe^{-a} = x.$$

  Using modular arithmetic, we can also write down the above proof in a more compact way. Since $\gcd(p, n) = 1$, we know that there exists a $b \in \mathbb{Z}$ such that $bp \equiv 1 \bmod n$). Since $x^n = e$ for any $x \in G$, we see that this implies $x^{bp} = x^1 = x$. Hence the map $x \mapsto x^b$ is an inverse for φ.
- We now give a proof that shows that φ is surjective. It is based on the fact that, if p does not divide the order of G, then φ preserves the order of elements (i.e. $\operatorname{ord}(x) = \operatorname{ord}(x^p)$ for all $x \in G$). We will first show that

this holds. Let $x \in G$, and let $k = \mathrm{ord}(x)$. We see that $(x^p)^k = (x^k)^p = e$, so $\mathrm{ord}(x^p)$ divides k. Let $l = \mathrm{ord}(x^p)$. We see that $(x^l)^p = (x^p)^l = e$, so $\mathrm{ord}(x^l)$ divides p. Since it also divides G by Lagrange's theorem, we see that $\mathrm{ord}(x^l) = 1$, so $x^l = e$. Therefore $k = \mathrm{ord}(x)$ divides l. We already saw that l divides k, so $l = k$. Hence x and x^p have the same order for any $x \in G$. We will now use this to prove surjectivity of φ. Let $x \in G$. Then x and x^p have the same order, hence $|\langle x^p \rangle| = |\langle x \rangle|$. Since $x^p \in \langle x \rangle$ by definition, we see that $\langle x^p \rangle \subset \langle x \rangle$. Because they have the same number of elements, we see that $\langle x^p \rangle = \langle x \rangle$. Therefore $x \in \langle x^p \rangle$, so there is an $m \in \mathbb{Z}$ such that $x = (x^p)^m = (x^m)^p$. By definition, we now see that $\varphi(x^m) = x$. Hence we see that for every $x \in G$, there exists a $y \in G$ such that $\varphi(y) = x$. We conclude that φ is surjective, hence it is bijective.