AM 106: Applied Algebra

Prof. Madhu Sudan

Problem Set 3 - Solution

Assigned: Wed. Sept. 20, 2017
Due: Tue. Sept. 26, 2017 (11:59 PM)

• You may submit your solutions via assignment page on the canvas website of the course.

• For collaboration and late days policy, see course website at http://madhu.seas.harvard.edu/courses/Fall2017

• Aim for clarity and conciseness in your solutions, emphasizing the main ideas over low-level details. Justify your answers except when otherwise specified.

Problem 1. (Cyclic groups) Which of the following are cyclic groups? For those that are not, justify your answers. For those that are, list all generators.

1. \(\mathbb{Z}_{18}\).

2. \(\mathbb{Z}_{8}^*\).

3. \(\mathbb{Z}_{19}^*\).

4. \(D_5\). (Please use the \(\text{Rot}_k\) and \(\text{Ref}_k\) notation for elements of \(D_n\) from lecture.)

5. \(\mathbb{R}\).

Solution.

1. \(\mathbb{Z}_{18}\) is cyclic. We saw in lectures that for every positive \(n \in \mathbb{Z}\), \(\mathbb{Z}_n\) is cyclic. Its generators are numbers that are relatively prime to the order and so we have \(\mathbb{Z}_{18} = \langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle = \langle 13 \rangle = \langle 17 \rangle\).

2. \(\mathbb{Z}_{8}^*\) is not cyclic. We mentioned in lecture the fact that \(\mathbb{Z}_{n}^*\) is cyclic only if \(n = 4\) or \(n = p^k\) or \(n = 2p^k\) for odd prime \(p\) and positive integer \(k\). \(n = 8\) does not meet this criterion. We can also check this by enumerating elements of \(\mathbb{Z}_{8}^*\) which are \{1, 3, 5, 7\}. Each one of these elements has order at most 2 and so the group is not cyclic.

3. \(\mathbb{Z}_{19}^*\) is cyclic, since 19 is a prime (by the fact above). One generator of \(\mathbb{Z}_{19}^*\) happens to be 2. The others can be inferred from Part (1) to be \{2^5, 2^7, 2^{11}, 2^{13}, 2^{17}\} = \{13, 14, 15, 3, 10\}.

4. \(D_5\) is not cyclic. Recall that the elements of \(D_5\) are \{\text{Rot}_k|k \in \mathbb{Z}_5\} \cup \{\text{Ref}_k|k \in \mathbb{Z}_5\} where The multiplication table is given by \(\text{Rot}_k \circ \text{Rot}_\ell = \text{Rot}_{k+\ell}\), \(\text{Rot}_k \circ \text{Ref}_\ell = \text{Ref}_{k+\ell}\), \(\text{Ref}_\ell \circ \text{Rot}_k = \text{Ref}_{\ell-k}\) and \(\text{Ref}_k \circ \text{Ref}_\ell = \text{Rot}_{k-\ell}\). It follows that the rotations (\(\text{Rot}_k\)) cannot generate the whole group, since they do not generate any reflection (any of the \(\text{Ref}_k\)). And the Reflections can not generate the whole group since any one of them always has a fixed point. In particular \(\text{Ref}_k(3k) = 3k(\text{mod } 5)\) for every \(k\) and so they do not generate any non-identity rotation.
5. \( \mathbb{R} \) is not cyclic due to the presence of irrational numbers. If some element \( \tau \) could generate \( \sqrt{2} \) and 1, then we have \( a\tau = \sqrt{2} \) and \( b\tau = 1 \) and so \( \sqrt{2} = a/b \) which would contradict the irrationality of \( \tau \).

Common Errors. Some of you used the fact that \( \mathbb{R} \) is uncountable to assert that it is not cyclic. While this is correct, I’d recommend a more first principle approach. One nice proof actually even implied (though it didn’t assert this) that \( \mathbb{Q} \) is not cyclic: Suppose \( \mathbb{Q} = \langle a \rangle \) then \( a/2 \in \mathbb{Q} \) but \( a/2 \not\in \langle a \rangle \) since it is not an integer multiple of \( a \). So one does not need the uncountability of \( \mathbb{R} \) to prove it is not cyclic!

Some stated that all elements in \( \mathbb{Z}_19^* \) were generators - \( \mathbb{Z}_19^* \) being cyclic implies that it has a generator, not that all elements are generators.

Problem 2. (Subgroups) Draw the subgroup lattices for each of the following groups.

1. \( \mathbb{Z}_{18} \)
2. \( \mathbb{Z}_{8}^* \)
3. \( \mathbb{Z}_{19}^* \)
4. \( D_5 \). (Please use the \( \text{Rot}_k \) and \( \text{Ref}_k \) notation for elements of \( D_n \) from lecture.)

Solution.

1. \( \mathbb{Z}_{18} = \langle 1 \rangle > \). The subgroup lattice is derived from the closure of
   \( \langle 0 \rangle \leq \langle 9 \rangle, \langle 6 \rangle, \langle 9 \rangle \leq \langle 3 \rangle, \langle 6 \rangle \leq \langle 2 \rangle, \langle 3 \rangle, \langle 3 \rangle \leq \langle 1 \rangle, \langle 2 \rangle \leq \langle 1 \rangle. \)

2. \( \langle 1 \rangle \leq \langle 3 \rangle, \langle 5 \rangle, \langle 7 \rangle \leq \mathbb{Z}_{8}^* \).

3. \( \mathbb{Z}_{19}^* \). This group is isomorphic to \( \mathbb{Z}_{18} \) with the isomorphism being given by \( x \in \mathbb{Z}_{18} \) mapping to \( 2^x \in \mathbb{Z}_{19}^* \). So we get the following lattice by cut-and-paste-and-edit. \( \langle 1 \rangle \leq \langle 18 \rangle, \langle 7 \rangle, \langle 18 \rangle \leq \langle 8 \rangle, \langle 7 \rangle \leq \langle 4 \rangle, \langle 8 \rangle, \langle 8 \rangle \leq \langle 2 \rangle, \langle 4 \rangle \leq \langle 2 \rangle. \)

4. \( D_5 \). (Please use the \( \text{Rot}_k \) and \( \text{Ref}_k \) notation for elements of \( D_n \) from lecture.) The subgroups are \( \langle \text{Rot}_1 \rangle \) which has order 5 and \( \langle \text{Ref}_k \rangle \) for \( k \in \{0, \ldots, 4\} \) each of which has order 2. We have \( \langle \text{Rot}_0 \rangle \leq \langle \text{Rot}_1 \rangle, \langle \text{Ref}_0 \rangle, \langle \text{Ref}_1 \rangle, \langle \text{Ref}_2 \rangle, \langle \text{Ref}_3 \rangle, \langle \text{Ref}_4 \rangle \leq D_5. \)

Common Errors. No common errors! Some had errors stemming from part 1 being incorrect - no additional points were deducted.
Problem 3. (Cauchy’s Theorem) Let $G$ be a finite group, and $p$ a prime number. Let $S$ be the set of all $p$-tuples of group elements $(g_0, \ldots, g_{p-1})$ whose product $g_0 g_1 \cdots g_{p-1}$ equals the identity $e$. Define an equivalence relation $\sim$ on $S$ where $(g_0, \ldots, g_{p-1}) \sim (h_0, \ldots, h_{p-1})$ if the two $p$-tuples are cyclic shifts of each other, i.e. there is an $k \in \mathbb{Z}_p$ such that $h_i = g_{i+k \mod p}$ for all $i \in \mathbb{Z}_p$.

1. Prove that all of the equivalence classes of $\sim$ are of size $p$ or of size 1, and characterize all of the equivalence classes of size 1.

2. Show that if $p$ divides $|G|$, then the number of equivalence classes of size 1 must be divisible by $p$. (Hint: analyze $|S|$.)

3. Deduce Cauchy’s Theorem: if a prime $p$ divides the order of a finite group $G$, then $G$ has an element of order $p$.

Solution.

1. Note that if $(g_0, \ldots, g_{p-1}) \in S$ then so is $(g_1, \ldots, g_{p-1}, g_0)$ since $g_1 \cdots g_{p-1}g_0 = g_0^{-1}(g_0 g_1 \cdots g_{p-1})g_0 = g_0^{-1}eg_0 = e$. Thus every cyclic shift of every sequence in $S$ is also in $S$. Thus the size of the equivalence class containing $(g_0, \ldots, g_{p-1})$ is determined by the minimal shift that preserves the sequence. Such a shift must have size dividing the length of the sequence. (If a $k$-shift preserves the sequence, then so does every $sk + tp$ shift, and thus so does the shift of length $\gcd(k, p)$.) Since $p$ is a prime, this shift must either be of length $p$ or 1, giving equivalence classes of size $p$ or 1. A sequence falls in an equivalence class of size 1 only if $g_0 = g_1 = \cdots = g_{p-1} = g$ and $g^p = e$, or $g$ is an element of order dividing $p$, or in other words $g = e$ or $g$ has order exactly $p$.

2. We first note that $|S| = |G|^{p-1}$: For every $g_1, \ldots, g_{p-1}$ there exists exactly one $g_0 = (g_1 \cdots g_{p-1})^{-1}$ that puts $(g_0, \ldots, g_{p-1}) \in S$. In particular, we have $p$ divides $|S|$ since $p$ divides $|G|$. Let $A$ be the number of equivalence classes of size $p$ and $B$ be the number of equivalence classes of size 1. We have $A \cdot p + B \cdot 1 = |S| = |G|^{p-1}$, yielding $B = |G|^{p-1} - A \cdot p$. The right hand side is 0 modulo $p$ and so $B$ must be 0 modulo $p$.

3. We conclude that the number of element $g$ such that $g^p = e$ is a multiple of $p$. Exactly one such element has order 1, namely the identity. Thus there must be at least $p - 1$ other elements in $G$ whose order is exactly $p$.

Comment Errors.

Several solutions skipped over the part explaining why $(g_0, \ldots, g_{p-1}) \in S$ implies $(g_1, \ldots, g_{p-1}, g_0) \in S$. For part 3, it was necessary to explain that we know of the existence of at least one tuple of order 1, the tuple of identities. From here, we could show that there are at least $p - 1$ other tuples. Otherwise, 0 is also a multiple of $p$.

Problem 4. (Diffie–Hellman in groups with small factors) Let $G = \langle g \rangle$ be a cyclic group of order $q$, and let $d$ be a divisor of $q$.

1. For an element $a = g^x$ of $G$, show that $d$ divides $x$ if and only if $a^{q/d} = e$. Thus, one can efficiently test whether an element $a$ is a $d$’th power in $G$ by exponentiation.
2. Suppose we choose \( x, y, z \in \mathbb{Z}_q \) uniformly at random. Calculate the probability that both \( g^x \) and \( g^{xy} \) are \( d \)'th powers, and the probability that both \( g^x \) and \( g^z \) are \( d \)'th powers.

3. Deduce that the Decisional Diffie–Hellman Assumption is false for \( G \) if the (known) order of \( G \) has a small factor (e.g. 2).

Solution.

1. Suppose \( d|x \) and say \( x = dy \). Then we have \( a^{x/d} = g^{xq/d} = (g^q)^y = e^y = e \) giving us one direction. To see the other direction, suppose \( g^{xq/d} = e \). Then \( xq/d \equiv 0 \pmod{q} \) since \( g^i = e \) if and only if \( i \equiv 0 \pmod{q} \). In turn this can happen if and only \( x/d \) is an integer, i.e., if \( d|x \).

2. The probability that \( g^x \) is a \( d \)'th power is 1 \( /d \) since this happens if and only if \( d \) divides \( x \). The probability that both \( g^x \) and \( g^{xy} \) are \( d \)'th powers is also exactly 1 \( /d \) since \( g^{xy} \) is a \( d \)'th power whenever \( g^x \) is. On the other hand the probability that \( g^x \) and \( g^z \) are both \( d \)'th powers when \( x \) and \( z \) are independent is 1 \( /d^2 \).

3. We have a distinguishing test for a triple \((A, B, C)\) to see if it comes from the distributions \( D_1 = (g^x, g^y, g^{xy}) \) and \( D_0 = (g^x, g^y, g^z) \): “Repeat \( O(d) \) times: Check if \( C \) is not a \( d \)'th power when \( A \) is. If this happens at least once, declare \( D_0 \) or else declare \( D_1 \).” This procedure runs in time \( \text{poly}(\log q, d) \) and distinguishes \( D_1 \) from \( D_0 \) with high (constant) probability, falsifying the DDH assumption.

Common Errors. No common errors here. A lot of solutions did not come up with an algorithm to falsify the DDH assumption, instead relying on assumptions that \( q \) is a large prime and testing small values of \( d \).