Math 100A hw3 Sample solution

Tianhao Wang

October 25, 2017

Hi, I am the grader of this course and I will write the sample solution if I have time. Usually, I would let the computer to generate two random numbers and grade those two problems unless I really want to grade a certain problem.

Some comments on this homework: I think some of students don't understand why we need to check a function is well-defined sometime. Usually when we have a function defined on a set of equivalence classes(cosets), we need to check it is well-defined. Essentially coset(equivalence class) is a set and we choose explicitly a **representative** for the coset. For example, let $G = \mathbb{Z}$ under addition and $H = 5\mathbb{Z} = \{\ldots, -5, 0, 5, 10, \ldots\}$ be a subgroup(easy check). Then consider the coset (we are in abelian group and left coset is the same as right coset), $0+H = H = \{\ldots, -5, 0, 5, 10, \ldots\}$. Then 0 is a representative of the coset $0 + H$. However any element in the coset to be chosen to be the representative. In this case $0 + H = 5 + H = 10 + H = 15 + H = -5 + H$. The problem is that, when we define a function from the set of cosets to another set and use the representative in definition(e.g question 4), it not guaranteed that the image of a coset is independent of the choice of its representative. However a function should send one element to exactly one element and hence the choice of representative should not influence the image of the coset. This is what we are checking when we check a function defined on a set of cosets is well-defined.

1. We first check that $\sim$ defines a equivalence relation. Let G be a group and $H \subset G$ be a subgroup, $\forall\, a, b, c \in G$, we have

   (a) $a^{-1}a = e \in H \implies a \sim a$

   (b) $b \sim a \implies b^{-1}a \in H \implies a^{-1}b = (b^{-1}a)^{-1} \in H \implies a \sim b$

   (c) $a \sim b, b \sim c \implies a^{-1}b, b^{-1}c \in H \implies a^{-1}c = (a^{-1}b)(b^{-1}c) \in H \implies a \sim c$

   Hence $\sim$ is a equivalence relation.

   Then $\forall\, a \in G$, we will prove that $[a] = aH$.

   Pick $g \in [a]$, we have $a \sim g$ and $a^{-1}g \in H$ which gives that $a^{-1}g = h$ for some $h \in H$. Hence $g = ah \in aH$ and we have $[a] \subset aH$

   For the other direction, pick $g \in aH$, we have $g = ah$ for some $h \in H$ and hence $a^{-1}g = h \in H$. Then we conclude that $a \sim g$ and $g \in [a]$. Hence $aH \subset [a]$. We conclude that $aH = [a]$ for all $a \in G$.

2. Let H be a subgroup of a group G. Pick $a \in G$ and let aH be a left coset, we have $aH = Hb$ for some $b \in G$. Then $ae = a \in aH = Hb$. Then we have $aH = Hb = Ha$.(if this is not proved in your lecture, try to prove it yourself that $Ha = Hb$ is equivalent to $a \in Hb$)

   $\forall\, a \in G$, we have $Ha = aH$. Pick $aha^{-1} \in aHa^{-1}$, we have $ah \in aH = Ha$ which gives that $ah = h'a$ for some $h' \in H$. Hence $aha^{-1} = h'aa^{-1} = h' \in H$, and we conclude that $aHa^{-1} \subset H$.

Pick $h \in H$, since $ha \in Ha = aH$, we have $ha = ah'$ for some $h' \in H$. Then $h = ah'a^{-1} \subset aHa^{-1}$ gives that $H \subset aHa^{-1}$. Hence we conclude that $H = aHa^{-1}$

3. Here are all the cosets:

   $[0] + H = \{[0], [4], [8], [12]\}$

   $[1] + H = \{[1], [5], [9], [13]\}$

   $[2] + H = \{[2], [6], [10], [14]\}$

   $[3] + H = \{[3], [7], [11], [15]\}$

4. Let $L = \{aH \mid a \in G\}$ be the set of left cosets and $R = \{Ha \mid a \in G\}$ be the set of right cosets. Define
$$f : L \mapsto R \qquad \text{via} \qquad aH \mapsto Ha^{-1}$$
   We will check that this function is well-defined and bijective.

   Let $aH = bH$ be two representative of the same coset, we need to check they have the same image. Since $aH = bH$, we have $a = bh$ for some $h \in H$. Then we have $a^{-1} = h^{-1}b^{-1}$ with $h^{-1} \in H$ as H is a subgroup. Hence we have $Ha^{-1} = Hb^{-1}$ and the function is well-defined.

   The surjective is obvious, for every $Ha \in R$, we have $a^{-1}H \in L$ such that $f(a^{-1}H) = Ha$.

   Suppose $f(aH) = f(bH)$, then we have $Ha^{-1} = Hb^{-1}$ and hence $a^{-1} = hb^{-1}$ for some $h \in H$. Then taking the inverse, we have $a = bh^{-1}$ with $h^{-1} \in H$. Hence $aH = bH$ and the function is injective.

   Then we have a bijection between set of left cosets and set of right cosets, hence there are same number of distinct left, right cosets.

5. the order of U_{18} (the standard symbol should be $(\mathbb{Z}/_{18\mathbb{Z}})^{\times}$, which is more common in a modern algebra book) is $\varphi(18) = \varphi(2 \cdot 3^2) = (2-1) \cdot (3-1) \cdot 3^{2-1} = 6$.

   $U_{18} = \{[1], [5], [7], [11], [13], [17]\}$. By a tedious calculation, we find that the order of $[5]$ is $6 = |U_{18}|$. Hence U_{18} is cyclic. (a little bit digression: U_n is cyclic if and only if $n = 2, 4, p^n, 2p^n$ for prime $p \neq 2$ and $n \in \mathbb{Z}^+$)

6. Since G is finite, we list its element as $G = \{a_1, \ldots, a_n\}$. Consider $x^2 = (a_1 \cdots a_n)(a_1 \cdots a_n)$. Since G is abelian and each elements a_i will have distinct inverse, then by reordering the multiplication, we have $x^2 = (a_1 \cdots a_n)(a_1 \cdots a_n) = (a_1 {a_1}^{-1}) \cdots (a_n {a_n}^{-1}) = e$

7. Let $D_8 = \{e, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$ where σ is rotation and τ is reflection. Here are all the 5 conjugation classes of D_8:
$$\{e\}, \{\sigma^2\}, \{\sigma, \sigma^3\}, \{\tau, \sigma^2\tau\}, \{\sigma\tau, \sigma^3\tau\}$$

8. Suppose n is not a prime, then we have $n = ab$ for $1 < a, b < n$. Then we have $[a], [b] \in \mathbb{Z}_n - \{[0]\}$, but $[a][b] = [ab] = [n] = [0] \notin \mathbb{Z}_n - \{[0]\}$ which contradicts that G is a group and should be closed under multiplication.

   Let n be a prime, then $[1]$ is clearly the identity, and associativity is obvious since the regular multiplication of integers are associative. Let $[a], [b] \in \mathbb{Z}_n - \{[0]\}$, we have $[a][b] \neq [0]$ since if so, we would have $n|ab$ and n is prime would imply $n|a$ or $n|b$. Then $[a] = [0]$ or $[b] = [0]$ would be a contradiction. Hence $\mathbb{Z}_n - \{[0]\}$ is closed under the multiplication. Then you can either use the Euclidean Algorithm or the Fermat's Little Theorem(Lagrange Theorem) to prove the existence of inverse.

9. Let $G = < a >$ be a cyclic group with a generator a and has order n. Then $G = \{a, a^1, \ldots, a^n\}$. Let $o(a)$ to denote the order of a. We have

$$o(a^i) = \frac{o(a)}{\gcd(i, o(a))} = \frac{n}{\gcd(i, n)}$$

Then a^i with $1 \le i \le n$ is an generator of G if and only if $o(a^i) = o(a) = n$ which is equivalent to $\gcd(i, n) = 1$. Then by Euler, we have exactly $\phi(n)$ generators and they are exactly a^i with $1 \le i \le n$ coprime to n.

10. Let $G = < a >$ be a cyclic group with a generator a and has order n. Then $G = \{a, a^1, \ldots, a^n\}$. Let $o(a)$ to denote the order of a. We have

$$o(a^i) = \frac{o(a)}{\gcd(i, o(a))} = \frac{n}{\gcd(i, n)}$$

Then for every $m|n$, $a^i \in G$ with $1 \le i \le n$ has order m if and only if $\gcd(i, n) = n/m$. Since $(n/m)|n$, the previous statement is equivalent to $\gcd(i, m) = 1$ and we have exactly $\phi(m)$ of them.

Then let's try to count the number of elements of G in 2 ways. We know that there are exactly n elements. On the other hand, each element has a unique order $m|n$. Hence we can sum up the number of elements of each order $m|n$ and still count the total number of elements. Also we know that for each order $m|n$, there are exactly $\phi(m)$ elements and hence we have

$$n = \sum_{m|n} \phi(m)$$