7th April, 2022

MAT 2200

Mandatory assignment 1 of 1

Submission deadline

Thursday 31st March 2022, 14:30 in Canvas (canvas.uio.no).

Instructions

Note that you have **one attempt** to pass the assignment. This means that there are no second attempts.

You can choose between scanning handwritten notes or typing the solution directly on a computer (for instance with LaTeX). The assignment must be submitted as a single PDF file. Scanned pages must be clearly legible. The submission must contain your name, course and assignment number.

It is expected that you give a clear presentation with all necessary explanations. Remember to include all relevant plots and figures. All aids, including collaboration, are allowed, but the submission must be written by you and reflect your understanding of the subject. If we doubt that you have understood the content you have handed in, we may request that you give an oral account.

In exercises where you are asked to write a computer program, you need to hand in the code along with the rest of the assignment. It is important that the submitted program contains a trial run, so that it is easy to see the result of the code.

Application for postponed delivery

If you need to apply for a postponement of the submission deadline due to illness or other reasons, you have to contact the Student Administration at the Department of Mathematics (e-mail: studieinfo@math.uio.no) no later than the same day as the deadline.

All mandatory assignments in this course must be approved in the same semester, before you are allowed to take the final examination.

Complete guidelines about delivery of mandatory assignments:

uio.no/english/studies/admin/compulsory-activities/mn-math-mandatory.html

GOOD LUCK!

You are highly encouraged to collaborate with other students on the problem set. If you need help connecting with others in the course, let me know by email. You must include the names of any students who you collaborated with. Remember: the write up of all solutions must be your own!

Problem 1. Let A be any non-empty subset of a group G. Define

$$C(A) = \{g \in G \mid g^{-1}ag = a \text{ for all } a \in A\}.$$

1. Show that $C(A)$ is a subgroup of G.

   Solution

   To show that $C(A)$ is a subgroup of G it suffices to show that:

   a) $e \in C(A)$ where e is the identity element of G,

   b) $C(A)$ is closed under the group operation of G,

   c) $g^{-1} \in C(A)$ for all $g \in C(A)$.

   Notice that the associativity of the group operation on $C(A)$ is inherited from associativity of the same operation on G.

   We begin with a). If $e \in G$ is the identity element then for all $a \in A$ we have

   $$e^{-1}ae = e^{-1}(ae) = e^{-1}a = ea = a.$$

   Therefore, $e \in C(A)$ and a) is satisfied.

   To show b), consider $g_1, g_2 \in C(A)$ and we will show that $g_1g_2 \in C(A)$. For every $a \in A$ we have

   $$(g_1g_2)^{-1}ag_1g_2 = g_2^{-1}g_1^{-1}ag_1g_2 = g_2^{-1}(g_1^{-1}ag_1)g_2.$$

   Since $g_1, g_2 \in C(A)$, for all $a \in A$ we have $g_1^{-1}ag_1 = a$ and $g_2^{-1}ag_2 = a$. Therefore,

   $$(g_1g_2)^{-1}ag_1g_2 = g_2^{-1}ag_2 = a.$$

   Therefore, $g_1g_2 \in C(A)$ and $C(A)$ is closed under the group operation.

   Lastly for c), suppose $g \in C(A)$, then $g^{-1}ag = a$ for all $a \in A$. Multiply the previous equality on the left by g and on the right by g^{-1}. Then we have,

   $$gg^{-1}agg^{-1} = gag^{-1}$$
   $$eae = gag^{-1}$$
   $$a = (g^{-1})^{-1}ag^{-1}.$$

Therefore g^{-1} satisfies the condition to be in $C(A)$ and c) holds.

It follows that $C(A)$ is a subgroup of G.

2. The automorphism group of G is

$$Aut(G) = \{f : G \to G \mid f \text{ is an isomorphism}\}$$

with group operation given by function composition (convince yourself that this is a group). Let $\phi : G \to Aut(G)$ be defined by $\phi(g) = \gamma_g$ where $\gamma_g(h) = ghg^{-1}$. Show that ϕ is a homomorphism. What is its kernel?

Solution

First convince yourself $Aut(G)$ is a subgroup (this did not need to be written in your solution). The group operation is function composition which we showed to be associative. Function composition gives a binary operation on $Aut(G)$ since we know that the composition of two homorphisms is a homomorphism and the composition of two bijections is a bijection. The identity element is the map $e : G \to G$ defined by $e(g) = g$ for all $g \in G$. If $f : G \to G$ is in $Aut(G)$ then there is an inverse map f^{-1} since f is a bijection. Moreover, the inverse f^{-1} satisfies the homomorphism property. Let a, b be in G. Suppose $f^{-1}(a) = g$ $f^{-1}(b) = h$. By definition this means that $f(g) = a$ and $f(h) = b$. Since f is a homomorphism we have $f(gh) = f(g)f(h) = ab$ and thus $f^{-1}(ab) = gh$. It follows that $f^{-1}(a)f^{-1}(b) = gh = f^{-1}(ab)$ and f^{-1} is a bijective homomorphism thus is in $Aut(G)$.

Now for the actual solution to the problem. For any $g, h \in G$ we must prove $\phi(gh) = \phi(g) \circ \phi(h)$, which is equivalent to proving for all $a \in G$ that

$$\gamma_{gh}(a) = \gamma_g \circ \gamma_h(a).$$

For $a \in G$ we have $\gamma_{gh}(a) = gha(gh)^{-1} = ghagh^{-1}g^{-1}$. Whereas, $\gamma_g \circ \gamma_h(a) = \gamma_g(hah^{-1}) = ghah^{-1}g^{-1}$. So we have $\gamma_{gh}(a) = \gamma_g \circ \gamma_h(a)$ for all $g, h, a \in G$. Thus ϕ satisfies the homomorphism property.

The kernel of ϕ is

$$Ker(\phi) = \{g \in G \mid \gamma_g = e\} = \{g \in G \mid gag^{-1} \text{ for all } a \in G\}.$$

Notice that $gag^{-1} = a$ is equivalent to $g^{-1}ag = a$ by the proof of part c) of Problem 1.1. Therefore $Ker(\phi) = \{g \in G \mid g^{-1}ag \text{ for all } a \in G\} = C(G)$.

3. Let $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Is the homomorphism $\phi : G \to Aut(G)$ surjective? Justify your answer.

   Solution Notice that the group G is abelian and for any abelian group G and any $a, g \in G$ we have $\gamma_g(a) = gag^{-1} = gg^{-1}a = a$. Therefore, the map $\gamma_g : G \to G$ is $e : G \to G$ the identity map. Therefore, the image of the map $\phi : G \to Aut(G)$ is $Im(\phi) = \{e\}$ and ϕ is surjective if and only if $Aut(G) = \{e\}$.

   However, consider the map $f : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ which exchanges the first and second coordinate. Namely, $f(x, y) = (y, x)$ for $x, y \in \mathbb{Z}/2\mathbb{Z}$. The map f is bijection (it is its own inverse), and it is not equal to e. Moreover, it satisfies the homomorphism property since for any $(x, y), (w, z) \in \mathbb{Z}/2\mathbb{Z}$, we have

$$f(x, y) + f(w, z) = (y + z, x + w) = f(x + w, y + z).$$

   Therefore, $f \in Aut(G)$ which shows that ϕ is surjective.

   Remark: Many of you pointed out that $Aut(G)$ is isomorphic to S_3. This is true, but more work is required to prove it and it is not necessary in order to conclude that the map is not surjective!

Problem 2. Let G be a finite group acting transitively on the finite set X and suppose $|X| > 1$. Show that there is an element $g \in G$ that fixes no element of X, i.e. there exists a $g \in G$ such that $X_g = \{x \in X \mid gx = x\} = \emptyset$.

Hint: Use that G acts transitively to compare the size of X and G and then apply Burnside's formula.

Solution Since the action of G on X is transitive, there is only one orbit. By Burnside's Formula, $1 = \frac{1}{|G|} \sum_{g \in G} |X_g|$, where recall

$$X_g := \{x \in X : g \cdot x = x\}.$$

Suppose for a contradiction that every element $g \in G$ fixes at least one element of X. Then $|X_g| \geq 1$ for all $g \in G$. Notice also that $X_e = X$ and so $|X_e| = |X|$ and we have

$$|G| = \sum_{g \in G} |X_g| = |X| + \sum_{g \in G, g \neq e} |X_g| \geq |X| + (|G| - 1).$$

This leads to the inequality $|X| \leq 1$ which is contrary to our assumption. Therefore, we have a contradiction and there must exists a $g \in G$ such that $X_g = \emptyset$.

Problem 3. Let G be a finite group and $\varphi : G \to G$ be a group homomorphism. Let p be a prime number dividing $|G|$.

1. Show that if the order of $g \in G$ is a power of p, then the order of $\varphi(g) \in G$ is also a power of p (not necessarily the same power).

   Solution: Suppose the order of g is p^r. Since φ is a homomorphism, we have
   $$\varphi(g)^{p^r} = \varphi(g^{p^r}) = \varphi(e) = e.$$
   Recall that for any $h \in G$ if $h^a = e$ then $ord(h)$ divides a. Therefore, the order of $\varphi(g)$ divides p^r and must be a power of p itself since p is prime.

2. Suppose the p-Sylow subgroup P of G is normal. Show that $\varphi(P) \subseteq P$.

   Hint: You may assume Corollary 36.4 from Fraleigh, i.e., the size of a (sub)group is a power of p if and only if every element of the (sub)group is a power of p (not necessarily the same power).

   Solution: By Corollary 36.4, the order of every element of the p-Sylow subgroup P is a power of p. Therefore, by part a), the order of every element of $\varphi(P)$. Moreover, the image of a subgroup P under a homomorphism is again a subgroup. Applying Corollary 36.4 again, we obtain that $\varphi(P)$ is a subgroup of size p^k for some k.

   By the stronger form of Sylow's first theorem, the subgroup $\varphi(P)$ is contained in some p-Sylow subgroup. By Sylow's second theorem this p-Sylow subgroup must be conjugate to P. However, P is a normal subgroup so $gPg^{-1} = P$ and P is the unique p-Sylow subgroup of G. Therefore, $\varphi(P) \subseteq P$.

Problem 4. A ring $(R, +, \cdot)$ is a *Boolean ring* if $a^2 = a$ for every $a \in R$.

1. Show that in a Boolean ring, $a + a = 0$ for every element a. (Hint: consider $(a + a)^2$.)

   Solution: We have $(a + a)^2 = a + a$ by the assumption. Expanding the left hand side and applying $a^2 = a$ we have $a^2 + a^2 + a^2 + a^2 = a + a + a + a = a + a$. Upon cancellation we obtain $a + a = 0$. Notice that this implies that for all $a \in R$ we have $a = -a$.

2. Show that a Boolean ring is necessarily commutative. (Hint: consider $(a+b)^2$.)

   Solution: For arbitrary $a, b \in R$, we have $(a+b)^2 = a+b$ by the assumption. Expanding the left hand side and applying $a^2 = a$ and $b^2 = b$ we obtain

   $$a^2 + ab + ba + b^2 = a + ab + ba + b = a + b.$$

   Subtracting $a + b$ from both sides of the last equality we obtain $ab + ba = 0$ and $ab = -ba$. By part 4.1 we know $ba = -ba$ so that $ab = ba$ and R is commutative.

3. Suppose R is a Boolean ring with more than 2 elements including a unity 1. Show that R can not be an integral domain.

   Solution: Since R has more than two elements we can choose $a \in R$ such that $a \neq 0, 1$. Then $a \neq 0$ and $a - 1 \neq 0$. However, $a(a-1) = a^2 - a = 0$, since $a^2 = a$. Therefore, a and $a - 1$ are zero divisors and R is not an integral domain.