Abstract Algebra Problem Set 1

Big Chungus

Problem 1: Let x and y be elements of a group G. Assume that each of the elements x, y and xy has order 2. Prove that the set $H = \{\mathbb{1}, x, y, xy\}$ is a subgroup of G, and that it has order 4. [Artin 4.7]

Proof. We begin by checking the group axioms:
1) Closure: the only non-obvious ones are the products of x and y with xy.
$\rightarrow xxy = x^2y = y \in H$
$\rightarrow xyx = h \Rightarrow xyxy = \mathbb{1} = hy$ thus h must be the inverse of y which is its own inverse (order 2)
$\rightarrow yxy = h \Rightarrow xyxy = \mathbb{1} = xh$ thus h must be the inverse of x which is its own inverse (order 2)
$\rightarrow xyy = xy^2 = x \in H$
2) Identity: $\mathbb{1} \in H$
3) Inverse: All non-identity elements are of order 2 so they are their own inverses
4) Associativity: Inherited from the group G □

Problem 2: Let G be a group and let $a \in G$ have order k. If p is a prime divisor of k, and if there is $x \in G$ with $x^p = a$, prove that x has order pk. [Rotman, Advanced Modern Algebra Exercise 2.24]

Proof. Let the order of x be some positive integer e. We know that $a^k = \mathbb{1}$ and also $x^p = a$ thus $a^k = x^{pk} = \mathbb{1}$. So pk ia a multiple of the order e of x i.e. for some $N \in \mathbb{N}$ we have $pk = Ne$.
Now observe the following relations:

$$\begin{aligned} a^1 &= x^p \neq \mathbb{1} \\ a^2 &= x^{2p} \neq \mathbb{1} \\ a^3 &= x^{3p} \neq \mathbb{1} \\ &\dots \\ a^k &= x^{kp} = \mathbb{1} \end{aligned}$$

This tells us that $e \neq p, 2p, 3p, ..., (k-1)p$ and since $pk = Ne$ we have two options:
1) p does not divide e
2) p divides e
We start with option 1): as $pk = Ne$ and p does not divide e, then that means that p^2 divides N (since k is divisible by p too). So $\exists n \in \mathbb{N} : \frac{k}{p} = ne \Rightarrow x^{ne} = x^{\frac{k}{p}} = \mathbb{1} = x^k x^{-p} = x^k a^{-1}$ so $x^k a^{-1} = \mathbb{1}$ so $x^k = a$. Now raise both sides by p: $(x^k)^p = a^p = \mathbb{1}$ but $p \leq k$ which would mean that k cannot be the order of a unless $k = p$. Back to the initial equation: $pk = p^2 = Ne$ and p does not divide $e \Rightarrow e = 1$ i.e. $x^e = x = \mathbb{1} = a$ which would mean that the order of a is now $k = 1$ - incompatible with $k = p$ ↯

We now check option 2): p divides e. We know, from above, that the first multiple of p that works for us is kp, so $e = kp$ which would make $N = 1$. □

Problem 3: If G is a group in which $x^2 = \mathbb{1} \quad \forall x \in G$, prove that G must be an abelian group. [Rotman, Advanced Modern Algebra Exercise 2.26]

Proof. $x^2 = \mathbb{1} \Rightarrow x = x^{-1} \quad \forall x \in G$. Let $x, y \in G$ and consider xy:
$(xy)(xy) = \mathbb{1} \Rightarrow xy = (xy)^{-1} = y^{-1}x^{-1} = yx$ which completes the proof since x, y are arbitrary. □

Problem 4: If G is a group with an even number of elements, prove that the number of elements in G of order 2 is odd. In particular, G must contain an element of order 2. [Rotman, Advanced Modern Algebra Exercise 2.27]

Proof. There is only one element of order 1, the identity $\mathbb{1}$ and it is its own inverse. From the other elements, suppose that there is no element of order 2 meaning that no element is its own inverse. This means that non-identity elements and their inverses are distinct i.e. the number of non-identity elements will always be even, making the total number of elements in the group odd ↯. $\Rightarrow$ there is at least one element in G that is of order 2.

Now suppose that there is an even number of elements of order 2. Since they are their own inverses, these account for an even number of distinct elements in the group. Adding the identity to these, we now have an odd number of distinct elements in the group (accounting for identity + order 2 elements). Using the logic above, all the rest pair up - all the other elements differ from their inverses, so these will account for an even number of elements. Adding all of these together, we get a group of an odd number of elements, contradicting our initial assumption ↯So there is an odd number of elements of order 2. □

Problem 5: Let H be a subgroup of G and $C(H) = \{g \in G : gh = hg \ \forall h \in H\}$. Prove that $C(H)$ is a subgroup of G. This subgroup is called the ***centralizer*** of H in G. [Judson Exercise 3.4.53]

Proof. 1) Closure: let $a, b \in C(H) \Rightarrow ah = ha$ and $bh = hb \ \forall h \in H$. So now we have for the product: $abh = ahb = hab$ for any $h \in H$. As $abh = hab \ \forall h \in H \Rightarrow ab \in C(H)$.
2) Identity: $\mathbb{1}h = h\mathbb{1} = h \ \forall h \in H \Rightarrow \mathbb{1} \in C(H)$.
3) Inverse: suppose that we have $a \in C(H) \Rightarrow ah = ha \ \forall h \in H \Rightarrow (ah)^{-1} = (ha)^{-1} \ \forall h \in H \Rightarrow h^{-1}a^{-1} = a^{-1}h^{-1} \ \forall h \in H$; Now since H is a subgroup, we know that if $h \in H$ then $h^{-1} \in H$. Thus: $h^{-1}a^{-1} = a^{-1}h^{-1} \ \forall h^{-1} \in H$ or letting $\tilde{h} = h^{-1} \Rightarrow \tilde{h}a^{-1} = a^{-1}\tilde{h} \ \forall \tilde{h} \in H$ so $a^{-1} \in C(H)$.
4) Associativity is inherited from the group G.
Thus $C(H)$ is a subgroup of G. □

Problem 6: Let G be a group, let X be a set, and let $f : G \to X$ be a bijection. Show that there is a unique operation on X so that X is a group and f is an isomorphism. [Rotman, Intro to Theory of Groups: Exercise 1.44]

Proof. Define a binary operation $*$ on the set x s.t. $*(x_1, x_2) \equiv x_1 * x_2 = f(f^{-1}(x_1)f^{-1}(x_2))$. This is a unique definition since f is a bijection. We see that $f(f^{-1}(x_1)f^{-1}(x^2)) = f(f^{-1}(x_1)) * f(f^{-1}(x_2))$ or just writing $g_1 = f^{-1}(x_1) \in G$ and $g_2 = f^{-1}(x_2) \in G$ we see $f(g_1g_2) = f(g_1) * f(g_2)$. This makes f a homomorphism. Since f is also bijective, this makes f into an isomorphism.

Now we need to show that $(X, *)$ is a group:
1) Closure: let $x_1, x_2 \in X \Rightarrow x_1 * x_2 = f(g_1g_2)$. As $g_1g_2 \in G$ due to G being a group and as $f : G \to x \Rightarrow x_1x_2 \in X$
2) Identity: we know that homomorphisms map identities to identities, so $f(\mathbb{1}_G) = \mathbb{1}_X \in X$
3) Inverse: let $x_1, x_2 \in X \Rightarrow x_1 * x_2 = f(g_1g_2)$. Suppose we fix x_1 and consequently $g_1 = f^{-1}(x_1)$. So we need such an x_2 (i.e. g_2) s.t. $f(g_1g_2) = \mathbb{1}_X$. Since G is a group, we can pick $g_2 = g_1^{-1} \in G$ i.e. $x_2 = f(g_1^{-1})$ so $x_1 * x_2 = f(g_1g_1^{-1}) = f(\mathbb{1}_G) = \mathbb{1}_X$ i.e. $x_2 = x_1^{-1} \in X$.
4) Associativity: I'll be lazy here and say that isomorphisms preserve this lol □

Problem 7: Determine the centre of $GL_n(\mathbb{R})$. [Artin, Exercise 5.6]

Proof. Since matrix multiplication is distributive w.r.t. addition we can work with the basis of $GL_n(\mathbb{R})$ which consists of matrices of the type $\mathbb{1}_n + A_{ij}$ where $\mathbb{1}_n$ is the identity matrix and A_{ij} is the matrix consisting of only one non-zero entry that is on the i'th row and the j'th column. Thus a matrix $Z \in GL_n(\mathbb{R})$ is in the centre of $GL_n(\mathbb{R})$ iff $(\mathbb{1}_n + A_{ij})Z = Z(\mathbb{1}_n + A_{ij})$ for all $(\mathbb{1}_n + A_{ij}) \in GL_n(\mathbb{R})$. So really $\mathbb{1}_nZ + A_{ij}Z = Z\mathbb{1}_n + ZA_{ij}$ so $A_{ij}Z = ZA_{ij}$ i.e. $\delta_{ik}\delta_{jl}z_{lm} = z_{ks}\delta_{is}\delta_{jm}$ so $\delta_{ik}z_{jm} = z_{ki}\delta_{jm}$. This represents the element on the k'th row and the m'th column on both sides. Now let's explore $k \neq m$.

We can choose a particular case now: $i = k, j \neq m$ so we get that $z_{jm} = 0$. Since we have left out j for iteration, this means that all elements in column m of Z must be zero, apart from possibly z_{mm}. Since this holds for all columns, then we can only have non-zero elements on the diagonal. The requirement $Z \in GL_n(\mathbb{R})$ now requires that all elements in the diagonal must be non-zero, otherwise the matrix will have zero determinant and thus not be invertible.
Now we choose another particular case: $i = k, j = m \Rightarrow z_{mm} = z_{kk}$. Since this holds for all m and k, this means that the diagonal consists of the same number.
We conclude that the centre of $GL_n(\mathbb{R})$ is $\{\lambda \mathbb{1}_n, \lambda \in \mathbb{R}\backslash\{0\}\}$. □

Problem 8: Suppose given on E an (associative and commutative) addition under which all the elements of E are invertible and a multiplication which is non-associative, but commutative and doubly distributive w.r.t. addition. Suppose further that $n \in \mathbb{Z}$, $n \neq 0$ and $nx = 0$ imply $x = 0$ in E. Show that if, writing $[x, y, z] = (xy)z - x(yz)$, the identity:

$$[xy, u, z] + [yz, u, z] + [zx, u, y] = 0$$

holds, then $x^{m+n} = x^m x^n$ for all x (show, by induction on p, that $[x^q, y, x^{p-q}] = 0$ holds for $1 \leq q < p$). [N. Bourbaki,Algebre, Vol.I: Exercise 9,§3.]

Proof. TBA □