1 Problem 1

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

Proof. First, note that since each element has order 2, each is its own inverse, so

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx.$$

Using this, it's easy to fill out the following multiplication table. For example, $(xy)x = (yx)x = yx^2 = y1 = y$.

$\times$	1	x	y	xy
1	1	x	y	xy
x	x	1	xy	y
y	y	xy	1	x
xy	xy	y	x	1

Reading the table, we see that the set H is closed under inverses and closed under multiplication, so it is a subgroup of G.

□

2 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. Notes: (1) I'll be using Lagrange's Theorem, which we haven't gotten to in Artin yet.
(2) Let's let $o(x)$ denote the order of x.
(3) Since p divides k, $k = pn$ for some $n \geq 1$.

Since $x^{pk} = a^k = 1$, we see that $o(x) \leq pk$. Also, since $< a >$ is a subgroup of $< x >$, Lagrange's Theorem tells us that $k = o(a)$ divides $o(x)$. Therefore, $o(x) = mk$ for some $1 \leq m \leq p$. So $a^{mn} = x^{mpn} = x^{mk} = 1$. Since $mn \geq 1$, mn must be a multiple of $o(a) = pn$, so $m \geq p$. $\implies$ $m = p$ and $o(x) = pk$.

□

3 Problem 3

If G is a group in which $x^2 = 1$ for every $x \in G$, prove that G must be abelian. [**Rotman, *Advanced Modern Algebra* Exercise 2.26**]

Proof. Let a and b be any two elements of G. Since $a^2 = b^2 = (ab)^2 = 1$,

$$ab = a1b = a(ab)^2b = a(abab)b = a^2(ba)b^2 = 1ba1 = ba.$$

□

4 Problem 4

If G be a group with an even number of elements, prove that the number of elements in G of order 2 is odd. [**Rotman, *Advanced Modern Algebra* Exercise 2.27**]

Proof. Notice that an element $x \neq 1$ has order 2 if and only if $x^{-1} = x$. With this in mind, let's go through the elements in G, placing them in two sets. If $x^{-1} = x$, we place x in set A, and if $x^{-1} \neq x$, we place both x and x^{-1} in set B. Since $y = x^{-1} \iff x = y^{-1}$, the elements of set B can be grouped as non-overlapping pairs, showing that B contains an even number of elements. Since we are given that the order of G is even, this means that set A also has an even number of elements, and in this set all but the identity element will be of order 2.

$\square$

5 Problem 5

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

Proof. First, note that $1 \in C(H)$, since $1h = h1$ for all $h \in H$.
Next, if $a, b \in C(H)$, then for all $h \in H$,

$$(ab)h = abh = ahb = hab = h(ab),$$

so $C(H)$ is closed under multiplication.
Finally, if $a \in C(H), h \in H$,

$$\begin{aligned} ha &= ah \\ a^{-1}(ha)a^{-1} &= a^{-1}(ah)a^{-1} \\ a^{-1}h &= ha^{-1}, \end{aligned}$$

$\implies a^{-1} \in H$, hence $C(H)$ is closed under taking inverses. $\square$

6 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. Notice that there is only one possible way to define a product in X such that f is an isomorphism, namely,
$$x \cdot y := f(f^{-1}(x)f^{-1}(y)),$$
where the product $f^{-1}(x)f^{-1}(y)$ is taken in G.
Since f is a bijection, and the product above is equivalent to the requirement for f to be a homomorphism, we need only check that with this product X is indeed a group.
Suppose $x, y, z \in X$, and set $a = f^{-1}(x), b = f^{-1}(y), c = f^{-1}(z)$. With this notation, our product is defined as $x \cdot y := f(ab)$.
The product is associative, since $(x \cdot y) \cdot z = f((ab)c) = f(a(bc)) = x \cdot (y \cdot z)$. (The second equality comes from associativity in G.)
The identity element in X will be $1_X = f(1_G)$. Note that $1_X \cdot x = f(1_G a) = f(a) = x$, and similarly $x \cdot 1_X = x$.
Finally, note that the inverse of x will be $f(a^{-1})$, for $x \cdot f(a^{-1}) = f(aa^{-1}) = f(1_G) = 1_X$, and similarly, $f(a^{-1}) \cdot x = 1_X$.

$\square$

7 Problem 7

Determine the center of $GL_n(\mathbb{R})$ **[Artin, Exercise 5.6]**

Solution. We'll show that the center of $GL_n(\mathbb{R})$ is the isomorphic image of $\mathbb{R}^\times$ under the mapping $a \mapsto aI$. First, notice that for $a \neq 0$, the matrix $aI \in Z(GL_n(\mathbb{R})$. We will now show that every matrix in the center is of this form. We'll do this in two steps. First, we'll show that every matrix in Z is diagonal, and then we'll show that all the diagonal entries must be equal.
Suppose $A = (a_{ij}) \in Z(GL_n(\mathbb{R})$. Consider the diagonal matrix B in which $b_{ii} = i$ (and all off-diagonal entries are zero). Since A is in the center, $AB = BA$, but notice that $[AB]_{ij} = ja_{ij}$, while $[BA]_ij = ia_{ij}$. For $i \neq j$, this shows that $a_{ij} = 0$, so A is a diagonal matrix.
Now, for $p \neq q$, let D be the matrix with 1 in the pq-position and zeros elsewhere. ($d_{ij} = \delta_{ip}\delta_{jq}$.) Since $I + D \in GL_n(\mathbb{R})$, we must have $A(I + D) = (I + D)A$, hence $AD = DA$. Notice, though, that $[AD]_{pq} = a_{pp}$, while $[DA]_{pq} = a_{qq}$. Thus all the diagonal entries of A must be equal, and $A = a_{11}I$.

□

8 Problem 8

[Optional] 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 wih respect to 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

$$[uz, y, x] + [zx, y, u] + [xu, y, z] = 0$$

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

Proof. **Part I** We'll begin by proving that $[x^m, y, x] = 0$ for all $m \geq 1$. Note that commutativity of multiplication guarantees that the statement is true for $m = 1$.

Also, notice that commutativity shows $(*)[a, b, c] = -[c, b, a]$.
To make the notation less cumbersome, for fixed p, let's set $c_i = [x^{p-j}, y, x^i]$. Note that substituting $z = x^{p-i-1}, u = x^i$ into the identity above, we obtain

$$[x^{p-1}, y, x] + [x^{p-i}, y, x^i] + [x^{i+1}, y, x^{p-i-1}] = 0$$

That is, $c_1 + c_i - c_{i+1} = 0$. Let's call this equation E_i.
Now we'll consider separately the cases when m is even and when m is odd.

Part I, Case I: m **odd**
Suppose $m = 2N + 1$. Set $p = 2N$. Then we have the equations
$E_1 : 2c_1 - c_2 = 0$
$E_2 : c_1 + c_2 - c_3 = 0$
$E_3 : c_1 + c_3 - c_4 = 0$
$\vdots$
$E_{N-1} : c_1 + c_{N-1} - c_N = 0$
In addition, using (*), we have $[x^N, y, x^N] = -[x^N, y, x^N]$, whence
$E_N : c_N = 0$.

Adding these N equations together, we see $Nc_1 = 0$,so $c_1 = 0$, that is,

$$0 = [x^{p-1}, y, x] = [x^m, y, x].$$

Part I, Case II: m **even**
Suppose $m = 2N$. Set $p = 2N + 1$. Then we have the equations
$E_1 : 2c_1 - c_2 = 0$
$E_2 : c_1 + c_2 - c_3 = 0$
$E_3 : c_1 + c_3 - c_4 = 0$
$\vdots$

$E_{N-1} : c_1 + c_{N-1} - c_N = 0$
$E_N : c_1 + c_N - c_{N+1} = 0$ In addition, using (*), we have $[x^{N+1}, y, x^N] = -[x^N, y, x^{N+1}]$, whence
$E_N : c_N + c_{N+1} = 0$.

This time, consider the sum $(2E_1 + \dots 2E_{N-1}) + (E_N + E_{N+1})$. this gives us $0 = (2Nc_1 - 2c_N) + (c_1 + 2c_N) = (2N+1)c_1$, and again $Nc_1 = 0$, so $c_1 = 0$, and

$$0 = [x^{p-1}, y, x] = [x^m, y, x].$$

Part II We'll now use the fact that $[x^m, y, x] = 0$ for all $m \geq 1$ to prove that $x^m x^n = x^{m+n}\ \forall m, n \geq 1$.
Fix m. By definition, when $n = 1$, we have $x^m x^1 = x^{m+1}$. Now suppose we have shown that the statement above is true for $k = n - 1$, that is, $x^m x^{n-1} = x^{m+n-1}$. Substituting $y = x^{n-1}$ into $[x^m, y, x] = 0$, we find

$$(x^m x^{n-1})x = x^m (x^{n-1} x)$$

$$(x^{m+n-1} x = x^m x^n$$

$$x^{m+n} = x^m x^n,$$

and by induction, this holds for all $n \geq 1$.

$\square$