**Homework 8**

**Exercise 3** Let $G = \mathbb{Z}_8 \times \mathbb{Z}_2$. Find subgroups $H$ and $K$ of $G$, such that $H$ is isomorphic to $K$ and $G/H$ is not isomorphic to $G/K$.

*Proof.* Set $H = \{(0,0), (2,1), (4,0), (6,1)\}$ and $K = \{(0,0), (2,0), (4,0), (6,0)\}$. $H$ and $K$ are isomorphic subgroups of $G$ since they are cyclic groups of order 4. (Why?) Observe that

$$G/H = \{H, (1,0) + H, (2,0) + H, (3,0) + H\}$$

and

$$G/K = \{K, (1,0) + K, (0,1) + K, (1,1) + K\}$$

Observe that $G/H$ is cyclic and $G/K$ is not since every element of $G/K$ has order 2. Therefore $G/H$ and $G/K$ are not isomorphic. □

**Exercise 4** If $G$ is a group, let $\text{Aut}(G)$ denote the set of automorphisms of $G$. Show that $\text{Aut}(G)$ is a subgroup of $(\mathcal{S}_G, \circ)$.

*Proof.* First observe that $\text{Aut}(G)$ is a subset of $\mathcal{S}_G$, since every automorphism of $G$ is by definition bijective. So, in order to prove that it is a subgroup of $G$ it suffices to prove that the composition of two automorphisms of $G$ is an automorphism of $G$ (the operation is closed) and the inverse of an automorphism of $G$ is again an automorphism $G$. (Hint: The composition of bijective maps is bijective and the composition of homomorphisms is again a homomorphism.) □

**Exercise 8** Let $G = (\mathbb{C}^*, \cdot)$ and $H$ be the subgroup $H = \{a + bi : a^2 + b^2 = 1\}$. Prove that $G/H$ is isomorphic to $(\mathbb{R}^+, \cdot)$.

*Proof.* Define $\phi : \mathbb{C}^* \to \mathbb{R}^+$ as follows: $\phi(z) = |z| = \sqrt{x^2 + y^2}$, if we write $z = x + iy$ for some $x,y \in \mathbb{R}$. Observe that $\phi$ is a group homomorphism. It is also surjective, since for every $x \in \mathbb{R}^+, \phi(x) = x$. Prove that the kernel of $\phi$ is equal with $H$. ($z \in \ker(\phi)$ iff $|z| = 1$) Thus, by the Fundamental Theorem we have that $G/H = G/\ker(\phi)$ is isomorphic to $\phi(G) = \mathbb{R}^+$. □

**Exercise 1** Let $G$ and $H$ be finite groups. Let $\phi : G \to H$ be a surjective homomorphism. Prove that $|H|$ divides $|G|$.

*Proof.* By the Fundamental Theorem we have that $G/\ker(\phi)$ is isomorphic to $\phi(G) = H$, so $|G/\ker(\phi)| = |H|$. However, $G$ is finite, so $|G/\ker(\phi)| = \frac{|G|}{|\ker(\phi)|}$ and thus $|H| \cdot |\ker(\phi)| = |G|$. Namely, $|H|$ divides $|G|$. □
**Exercise 2** Let $\phi : G \to K$ be a surjective homomorphism and $J \triangleleft K$. Then there exists a normal subgroup $H$ of $G$ such that $G/H$ is isomorphic to $K/J$.

**Proof.** Consider the map $\pi : K \to K/J, k \mapsto kJ$. This map is a surjective homomorphism. Therefore, the map $\pi \circ \phi : G \to K/J$ is a surjective homomorphism and by the Fundamental Theorem $G/\ker(\pi \circ \phi)$ is isomorphic to $K/J$. Obviously $\ker(\pi \circ \phi)$ is the subgroup we are looking for. Note, $H = \phi^{-1}(J)$.

**Exercise 3** Find up to isomorphism all the abelian groups of order 324.

**Proof.** $324 = 2^2 \cdot 3^4$, so there exist $2 \cdot 5 = 10$ distinct (up to isomorphism) abelian groups of order 324. By the Fundamental Theorem of finitely generated abelian groups there exist two abelian groups of order 4, $Z_2 \times Z_2, Z_4$, and 5 abelian groups of order 81, $Z_{81}, Z_9 \times Z_9, Z_3 \times Z_{27}, Z_3 \times Z_3 \times Z_9, Z_3 \times Z_3 \times Z_3 \times Z_3$. Again by the Fundamental Theorem of finitely generated abelian groups we have the 10 distinct (up to isomorphism) abelian groups of order 324.

**Exercise 4** Let $G$ be an abelian group of order $p^n$, where $p$ is a prime number. Prove that the only subgroup that contains all the elements of maximal order is $G$ itself. An element $x \in G$ is an element of maximal order if $o(x) \geq o(y)$ for every $y \in G$.

**Proof.** Let $G$ be group of order $p^n$. Then by the Fundamental Theorem of finitely generated abelian groups, $G = Z_{p^{n_1}} \times Z_{p^{n_2}} \times \ldots \times Z_{p^{n_k}}$ where $n_1 + n_2 + n_3 + \ldots + n_k = n$ and $n_1 \leq n_2 \leq \ldots \leq n_k$.

Let $H$ be a subgroup that contains all the elements of maximal order.

Observe that the generator 1 of $Z_{p^{n_k}}$ is an element of maximal order (its order is $p^n$. Indeed, if $g$ is and element of $G$, then $g = (g_1, g_2, \ldots, g_k)$, where $g_i$ belongs in $Z_{p^{n_i}}$ for all $1 \leq i \leq k$. Observe that $p^{n_k} = (0, 0, 0, \ldots, 0)$ = $e_G$. Thus the order of $g$ is less or equal to $p^{n_k}$.

Consider now the following elements of $G$:

$$(0, 0, \ldots, 0, 1)$$
$$(0, 0, \ldots, 1, 1)$$
$$(0, \ldots, 1, 1, 1)$$
$$\vdots$$
$$(1, 1, \ldots, 1, 1)$$

These elements have order $p^{n_k}$, so there are elements of maximal order and thus they are contained in $H$. Finally, observe that these elements generate $G$. (Hint: Prove that the elements $(1,0,\ldots,0)(0,1,\ldots,0), \ldots, (0,0,\ldots,1)$ belong to the subgroup of $H$ generated by the elements above.) Hence, $G$ is contained in $H$ and thus $H=G$. QED.

**Homework 10**

**Exercise 1** Consider $(\mathbb{Q}, \oplus, \odot)$, where $\oplus$ is the addition given by $a \oplus b = a + b - 1$ and $\odot$ the multiplication given by $a \odot b = a + b - ab$. Is $(\mathbb{Q}, \oplus, \odot)$ a field.
**Proof.** Verify that \((\mathbb{Q}, \oplus, \odot)\) is a commutative ring. Observe also that the zero element of this ring is the number 1 and the unitary of this ring is the number 0. \((0_{\mathbb{Q}} = 1 \text{ and } 1_{\mathbb{Q}} = 0)\)

\((\mathbb{Q}, \oplus, \odot)\) has no non-zero divisors. Indeed, if \(a \odot b = 1 = 0_{\mathbb{Q}}\) for some \(a, b \in \mathbb{Q}\), then \(a + b - ab = 1\) and so \((1 - a)(b - 1) = 0\). Thus \(a = 1 = 0_{\mathbb{Q}}\) or \(b = 1 = 0_{\mathbb{Q}}\), which means that there exist no non-zero divisors.

Finally, we observe that every non-zero element of \((\mathbb{Q}, \oplus, \odot)\) has a multiplicative inverse. Indeed, if \(a \in \mathbb{Q}\) and \(a \neq 1 = 0_{\mathbb{Q}}\) we have that \(a \odot \frac{a}{1-a} = 0 = 1_{\mathbb{Q}}\). Therefore, \((\mathbb{Q}, \oplus, \odot)\) is a field.

**Exercise 3** Let \(R\) be a ring with unity, which is also Boolean (every element of \(R\) is an idempotent). Prove that \(r = -r\) for every \(r \in R\) and that \(R\) is commutative.

**Proof.** Let \(r\) be an element of \(R\). Then \(r+r\) is an idempotent, so \((r+r)^2 = r + r\). However, \((r + r)^2 = 4r^2 = 4r\). Hence, \(2r = 0\) and thus \(r = -r\).

\(R\) is commutative. Indeed, if \(x, y \in R\) then \((x+y)^2 = x + y\) and thus \(xy + yx = 0\). But \(yx = -yx\), so \(xy = yx\). \(x\) and \(y\) were arbitrary, so \(R\) is commutative.

**Exercise 5** Let \(F\) be the set of \(2 \times 2\) matrices of real numbers of the form \(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\). Prove that \(F\) forms a field under the usual addition and multiplication.

**Proof.** First observe that \(F\) is a non empty subset of the ring of \(2 \times 2\) matrices with real entries\((M_2(\mathbb{R}))\). It suffices to prove that \(F\) is a commutative subring of this set, which has no non-zero zero divisors and every element has a multiplicative inverse in \(F\).

**Subring:** Let \(A, B \in F\). Verify that the matrices \(A-B\) and \(AB\) belong in \(F\).

**Commutative:** Verify that \(A \cdot B = B \cdot A\) for every \(A, B \in F\).

**No non-zero zero divisors:** Let \(A, B\) be non-zero elements of \(F\) such that \(A \cdot B = 0\). Then by Linear Algebra \(0 = \det(A \cdot B) = \det A \cdot \det B\). So \(\det A = 0\) or \(\det B = 0\). Contradiction, since every non-zero element of \(F\) is an invertible matrix. \((\text{Note that } \det \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a^2 + b^2.\)\)

**Invertibility:** Let \(A \in F\) non-zero. Then, \(A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\) for some \(a, b \in \mathbb{R}\). Observe that the matrix \(B = \frac{1}{a^2 + b^2} \begin{pmatrix} a & -b \\ b & a \end{pmatrix}\) is the multiplicative inverse of \(A\) and that \(B\) is an element of \(F\).

**Exercise 2** Let \(R\) be a ring with unity. Assume that for all \(x\) and \(y\) in \(R\) we have \((xy)^2 = x^2y^2\). Prove that \(R\) is commutative.

**Proof.** Let \(R\) as above. Then for all \(x, y \in R\) we have \((xy)(xy) = (xy)^2 = x^2y^2\) and so \(x(yx - xy)y = 0\) \((\ast)\).

Let \(x, y \in R\). Then since equality \((\ast)\) holds for every pair of elements in \(R\), we have that it holds for the pair \((1 + x, y)\). Namely, \((x + 1)(y(x + 1) - (x + 1)y) = 0\). Equivalently, \((x + 1)(yx - xy)y = 0\) \((1)\).

We observe that \(0 = 0 - 0 = (1 - (\ast)) = (x + 1)(yx - xy)y - x(yx - xy)y = (yx - xy)y\). Namely, \((yx - xy)y = 0\). Since \(x, y\) were arbitrary, we actually proved that for all \(x, y\) in
Let \((yx - xy)y = 0\) (**). Clearly for given \(x\) and \(y\) (**) holds for the pair \((x,y+1)\). Thus 
\(((y+1)x - x(y+1))(y+1) = 0\) and so 
\((yx - xy)(y+1) = 0\) (2).

Finally, if \(x, y \in R\), we observe that 
\(0 = 0 - 0 = (2) - (**) = (yx - xy)(y+1) - (yx - xy)y = (yx - xy)\) and so \(xy = yx\). Namely, \(R\) is a commutative ring.

Exercise 3 (b) Prove that the ring \(S = \{q \in \mathbb{Q} : q = \frac{a}{b}, a, b \in \mathbb{Z} \text{ and } b \text{ is odd}\}\) has a unique maximal ideal.

Proof. Consider the set \(I = \{\frac{2k}{b} : k \in \mathbb{Z} \text{ and } b \text{ is odd}\}\). Obviously, \(I\) is a non-empty proper subset of \(S\). It is easy to verify that \(I\) is an ideal of \(S\).

Claim 1: \(I\) is a maximal ideal of \(S\).

Let \(J\) be a proper ideal of \(S\) which contains \(I\). Suppose that there exist \(x \in J\) that does not belong in \(I\). Then \(x = \frac{a}{b}\) for some non-zero odd integers \(a\) and \(b\). Observe that \(\frac{b}{a} \in S\) and thus 
\[1 = \frac{b}{a} \cdot \frac{a}{b} \in J.\]
Hence \(J = S\). Therefore, \(I\) is a maximal ideal.

Claim 2: \(I\) is the unique maximal ideal of \(S\).

Hint: Prove that if \(J\) is an ideal of \(S\), then it contains only elements of the form \(\frac{2k}{b}\) where \(k, b \in \mathbb{Z}\) and \(b\) is odd. Use the same argument as above.

Exercise 4 Let \(R\) be a commutative ring with unity \(1 \neq 0\).

(a) Prove that \(R\) is an integral domain if and only if \(\{0\}\) is a prime ideal in \(R\).

(b) Prove that \(R\) is a field if and only if \(\{0\}\) is a maximal ideal in \(R\).

Proof. (a) Let \(R\) be a integral domain and \(a, b\) be elements of \(R\) such that \(ab \in \{0\}\) \((ab = 0)\). Then since \(R\) is an integral domain we have that \(a = 0\) or \(b = 0\). Namely, \(a \in \{0\}\) or \(b \in \{0\}\), which means that \(\{0\}\) is a prime ideal.

Similarly for the other direction.

(b) Let \(R\) be a field. Lets assume that \(\{0\}\) is not maximal. Then there exists a proper ideal \(I\) of \(R\) that contains \(\{0\}\) and \(I \neq \{0\}\). Then there exists \(x \in I\) such that \(x \neq 0\). However \(F\) is a field and thus \(x\) is invertible. Hence \(1 = xx^{-1} \in I\), which means that \(I = R\) (Why?). Contradiction, since \(I\) is proper. Therefore, \(\{0\}\) is a maximal ideal.

Similarly, for the other direction.

Exercise 5 Let \(I\) be an ideal in the commutative ring \(R\). Define 
\[\text{rad}(I) = \{r \in R : \exists n \in \mathbb{N} : r^n \in I \}.\]

Prove that \(\text{rad}(I)\) is an ideal with \(I \subset \text{rad}(I)\).

Proof. First, \(\text{rad}(I)\) is non-empty, since \(0 \in \text{rad}(I)\). Clearly, \(I \subset \text{rad}(I)\) by the way \(\text{rad}(I)\) was defined.

\(\text{rad}(I)\) is an ideal: Let \(x, y \in \text{rad}(I)\). Then there exist \(n, m \in \mathbb{N}\) such that \(x^n, y^m \in I\). \(R\) is commutative, so 
\[(x - y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k(-y)^{n+m-k} = \sum_{k=0}^{n} \binom{n+m}{k} x^k(-y)^{n+m-k} + \sum_{k=n+1}^{n+m} \binom{n+m}{k} x^k(-y)^{n+m-k} \]
\[= \sum_{k=0}^{n} \binom{n+m}{k} x^k(-y)^{m(-y)^{-k}} + \sum_{k=n+1}^{n+m} \binom{n+m}{k} x^n x^{k-n}(-y)^{n+m-k}.\]
By the above equality, it follows that \((x - y)^{n+m} \in I\). Thus, \(x - y \in \text{rad}(I)\).

Now if \(x \in R\) and \(y \in \text{rad}(I)\), there exists \(m \in \mathbb{N}\) such that \(y^m \in I\). \(R\) is commutative, so \((yx)^m = (xy)^m = x^m y^m \in I\). \(I\) is an ideal. Therefore, \(xy\) and \(yx\) belong in \(\text{rad}(I)\) and thus \(\text{rad}(I)\) is an ideal.

\(\Box\)

**Exercise 6** Let \(R\) be a commutative ring and \(I \subset R\) a prime ideal. Prove that \(\text{rad}(I) = I\).

**Proof.** In Exercise 5, we saw that \(I \subset \text{rad}(I)\) for every ideal \(I\) of \(R\).

Let’s assume that \(I\) is prime ideal of \(R\) and \(x\) is an element of \(\text{rad}(I)\). Then there exists \(n \in \mathbb{N}\) such that \(x^n \in I\). If \(n = 1\) done \((x \in I)\). If \(n > 1\) then \(x \cdot x^{n-1} = x^n \in I\). However \(I\) is a prime ideal, so \(x \in I\) or \(x^{n-1} \in I\). If \(x \in I\) done. If \(x^{n-1} \in I\) we apply the same argument as before and we finally have that \(x \in I\). \(x\) was arbitrary, so \(\text{rad}(I) \subset I\) and thus we have equality. \(\Box\)