Homework #7. Due Thursday, March 24th

Reading:
1. For this assignment: Online lectures 13-15, [Pinter, §9-11] and [Gilbert, §3.4, 3.5].
2. For next week’s classes: Online lectures 15 and 16, [Pinter, §9, 14] and [Gilbert, §3.5, 3.6]. Also read the definition of direct product (see a note ‘Direct sums and products’ on last year’s webpage as well as Section G in the exercise after § 4 in Pinter).

Problems:

Problem 1: Recall that for a ring $R$ with 1 we denote by $R^\times$ the group of invertible elements of $R$ with respect to multiplication. For each of the following groups $G$, determine whether it is cyclic or not. If it is cyclic, find ALL generators (note: to prove that a group is cyclic it suffices to find one generator).

(i) $G = \mathbb{Z}_7^\times$, (ii) $G = \mathbb{Z}_9^\times$, (iii) $G = \mathbb{Z}_{12}^\times$.

Problem 2: Let $x$ be an element of a group $G$, let $n = o(x)$, and assume that $n < \infty$. Prove that

$$o(x^k) = \frac{n}{gcd(n,k)}$$

for every $k \in \mathbb{Z}$ (this is a slight reformulation of Theorem 14.1(v) from online Lecture 14). You are allowed to use Theorem 14.1(iv) proved in online notes (but obviously not Theorem 14.1(v)).

Problem 3: (practice) Theorem 14.1 is applicable to any finite cyclic group $G$ and any generator $x$ of $G$. If $G = (\mathbb{Z}_n, +)$ for some $n$, we can use $x = [1]$ as a generator, in which case all assertions of the Theorem can be restated directly in terms of $n$. For instance, part (i) would say: “Every subgroup of $\mathbb{Z}_n$ is cyclic and is equal to $\langle [d] \rangle$ where $d$ is a positive divisor of $n$”. Restate other parts of Theorem 14.1 in a similar way.

Problem 4: Use restatement of Theorem 14.1 from Problem 3 to do the following:

(a) List all generators of $(\mathbb{Z}_{12}, +)$ and $(\mathbb{Z}_{15}, +)$
(b) List all subgroups of $(\mathbb{Z}_{12}, +)$ and $(\mathbb{Z}_{15}, +)$ (without repetitions)

Problem 5: (practice) Prove that the relation $\cong$ of “being isomorphic” is an equivalence relation (Claim 15.1 from online Lecture 15).

Hint: To prove that $\cong$ is symmetric, show that if $\varphi : G \to G'$ is an isomorphism, then the inverse map $\varphi^{-1} : G' \to G$ is also an isomorphism. Since the inverse of a bijection is a bijection, you only need to show that $\varphi^{-1}(uv) = \varphi^{-1}(u)\varphi^{-1}(v)$ for all $u, v \in G'$. To prove this, take any $u, v \in G'$,
and let \( x = \varphi^{-1}(u) \), \( y = \varphi^{-1}(v) \). Then \( \varphi(x) = u \) and \( \varphi(y) = v \); at this point you can use the fact that \( \varphi \) is a isomorphism.

**Problem 6:**

(a) Let \( G = (\mathbb{Z}_6, +) \) and \( G' = (\mathbb{Z}_7^\times, \cdot) \). Prove that \( G' \cong G \) and find an explicit isomorphism \( \varphi : G \rightarrow G' \). **Hint:** Use Theorem 15.2 from online notes.

(b) (practice) Use map \( \varphi \) from (a) to show (explicitly) that the multiplication tables of \( G \) and \( G' \) can be obtained from each other by relabeling of elements.

**Problem 7:** (practice)

(a) Let \( G = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbb{R} \right\} \). Prove that \( G \) is a subgroup of \( GL_2(\mathbb{R}) \).

(b) Let \( G \) be the group from part (a). Find an isomorphism \( \varphi \) from \((\mathbb{R}, +)\) to \( G \) (and prove that \( \varphi \) is an isomorphism).

**Problem 8:** Let \( G \) be a group from Problem 2 in Homework #6: \( G = \mathbb{R} \setminus \{-1\} \) as a set, and the operation \( * \) on \( G \) is defined by \( x * y = xy + x + y \). Prove that \( (G, *) \) is isomorphic to \((\mathbb{R} \setminus \{0\}, \cdot)\) and find an explicit isomorphism between those groups.

**Problem 9:** Let \( \varphi : G \rightarrow G' \) be an isomorphism, and let \( g \in G \).

(a) Prove by induction that \( \varphi(g^n) = \varphi(g)^n \) for every \( n \in \mathbb{N} \).

(b) Prove that if \( n \in \mathbb{N} \), then \( g^n = e_G \) if and only if \( \varphi(g)^n = e_{G'} \) (where \( e_G \) is the identity element of \( G \) and \( e_{G'} \) is the identity element of \( G' \)). **Hint:** Use (a) and the fact that an isomorphism must send identity element to identity element (this will be proved in class next week).

(c) Use (b) to prove that \( o(g) = o(\varphi(g)) \) (Proposition 15.3 from online notes). Thus isomorphisms preserve orders of elements.

**Problem 10:** Let \( G \) be a group and \( g, h \in G \).

(a) Prove that the elements \( ghg^{-1} \) and \( h \) have the same order by direct computation.

(b) Now prove that \( ghg^{-1} \) and \( h \) have the same order without any computations by using Problem 9(c) and Example 3 from Lecture 15.

(c) Prove that \( gh \) and \( hg \) have the same order. **Hint:** Use (a) (or (b)).

**Hint for (a):** Let \( n = o(h) \), so that \( h^n = e \). First show that \( (ghg^{-1})^n = e \) as well (if you do not see how to do this, start with \( n = 2 \), see the pattern, then generalize). Note that the equality \( (ghg^{-1})^n = e \) DOES NOT mean that \( o(ghg^{-1}) = n \). It only means that \( o(ghg^{-1}) \leq n = o(h) \) as there could exist \( m < n \) such that \( (ghg^{-1})^m = e \) as well. Show that the latter is impossible by contradicting the assumption \( n = o(h) \).

**Problem 11:** Let \( D_8 \) be the octic group (the group of isometries of a square – for the definition see online Lecture 10 or the end of Chapter 7 in Pinter;
note that Pinter calls this group $D_4$ and $Q_8$ the quaternion group (see the definition on wikipedia).

(a) Find the order of each element in both $D_8$ and $Q_8$.
(b) Prove that $D_8$ and $Q_8$ are not isomorphic. **Hint:** Use Problem 9(c).