Homework #6. Due Thursday, October 14th

Reading:

For this homework assignment: Sections 3.3 and 3.4 (up to page 167)
Before the class next Thursday: Sections 3.5 and 3.4 (pp. 168-171). Also review the notion of a bijective mapping (1.2).

To hand in:

Problem 1:

(a) Prove that a group G is abelian (= commutative) if and only if $(xy)^2 = x^2y^2$ for all $x, y \in G$.

(b) Let G be a group such that $x^{-1} = x$ for all $x \in G$. Prove that G is abelian. **Note:** This can be deduced from (a) or proved independently.

Warning: To prove that a group G is abelian, you need to show that $xy = yx$ for ALL $x, y \in G$ (you cannot pick x and y that you like).

Problem 2: Let G be a group and H and K the subgroups of G.

(a) Prove that the intersection $H \cap K$ is a subgroup of G.

(b) Prove that the union $H \cup K$ is a subgroup of G if and only if $H \subseteq K$ or $K \subseteq H$. **Hint:** The backward ("$\Leftarrow$") direction is easy. For the forward ("$\Rightarrow$") direction do a proof by contrapositive: assume that K does not contain H and H does not contain K. This means that there exist $x, y \in G$ such that $x \in H$, but $x \notin K$, and $y \in K$, but $y \notin H$. Now prove by contradiction that xy does not belong to H or K. Why does this finish the proof?

(c) (practice) Let A be some set (possibly infinite), and let $\{H_\alpha\}_{\alpha \in A}$ be any collection of subgroups of G indexed by elements of A. Prove that the intersection of all these subgroups $\cap_{\alpha \in A} H_\alpha$ is a subgroup of G.

Problem 3:

(a) Recall that if G is a group and $a \in G$, the centralizer $C(a)$ is the set of all elements of G which commute with a, that is,

$$C(a) = \{x \in G : xa = ax\}.$$

In Lecture 12 (September 30) we started proving that $C(a)$ is a subgroup of G. Finish that proof (it remains to show that $C(a)$ is closed under inversion).

(b) Given a group G, let $Z(G)$ be the set of all $x \in G$ which commute with any element of G, that is,

$$Z(G) = \{x \in G : xg = gx \text{ for all } g \in G.\}$$

The set $Z(G)$ is called the *center of* G. Prove that $Z(G)$ is a subgroup of G without doing any computations. **Hint:** use results proved earlier in this homework.

Problem 4: Let F be a field, and recall from Homework#5 that for any integer $n \geq 2$, we denote by $GL_n(F)$ the group of all **invertible** $n \times n$ matrices with entries in F (with respect to multiplication).

(a) (practice) It is a well-known fact that if A and B are any $n \times n$ matrices over some commutative ring, then $\det(AB) = \det(A)\det(B)$. Verify this formula (by direct computation) for $n = 2$.

(b) Let $SL_2(F) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in F \text{ and } ad - bc = 1 \right\}$, that is, $SL_2(F)$ is the set of all 2×2 matrices with entries in F and determinant equal to 1. Use (a) to prove that $SL_2(F)$ is a subgroup of $GL_2(F)$.

Problem 5:

(a) Problem 3.3.14 (a) and (c), page 161. Note: the group G defined in this problem is $GL_2(\mathbb{R})$.

(b) Solve Problem 3.3.14(b) without any computations using Problems 3(a), 4(b) and 5(a) in this homework. **Hint:** What is the meaning of the expression $a^2 + b^2$ in 3.2.14(b)(c)?

(c) (bonus) Do you see a connection between subgroups in 3.2.14(b)(c) and complex numbers? If yes, explain.

Problem 6:

(a) Let A be a set, and let $S(A)$ be the set of all **bijective** functions $f : A \to A$. Recall that $S(A)$ is a group with respect to composition (we discussed this group in class on Thursday, September 23). Fix $a \in A$, and let $H_a = \{f \in S(A) : f(a) = a\}$, that is, H_a is the set of all functions from $S(A)$ which send a to a. Prove that H_a is a subgroup of $S(A)$.

(b) Now let $A = \{1, 2, 3, 4\}$ and $a = 3$. Describe explicitly all elements of the subgroup $H_3 = H_a$ (you can use "two line notation" to list elements of H_3).

Problem 7: Recall that for a ring R we denote by R^* 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) $G = \mathbb{Z}_7^*$, (ii) $G = \mathbb{Z}_9^*$, (iii) $G = \mathbb{Z}_{12}^*$.

Problem 8: Let $n > 1$ be an integer, and let $G = (\mathbb{Z}_n, +)$, that is, $G = \mathbb{Z}_n$, and the group operation is addition. If d is a positive **divisor** of n, let $e = \frac{n}{d}$, and define $G_d = \{[0], [d], [2d], \ldots, [(e-1)d]\}$ (note that $[ed] = [n] = [0]$)

(a) (practice) Prove that G_d is equal to $\langle [d] \rangle$, the cyclic subgroup generated by $[d]$ (in particular, this shows that G_d is a subgroup of G). We will prove shortly that any subgroup of $G = \mathbb{Z}_n$ is equal to G_d for some d dividing n. Note that if $d = 1$, then $G_d = G$, and if $d = n$, then $G_d = \{[0]\}$, the trivial subgroup.

(b) Now let $n = 12$. For each $a = 1, 2, \ldots, 11$ compute the cyclic subgroup $\langle [a] \rangle$ and find d (depending on a) such that $d \mid n$ and $\langle [a] \rangle = G_d$ (in the above notations). Note that if $a \mid n$, then $d = a$, but if $a \nmid n$, then d is something else. **Reminder:** The group operation in this example is addition, so $\langle [a] \rangle = \{n[a] : n \in \mathbb{Z}\} = \{[0], \pm[a], \pm 2[a], \ldots\}$.

(c) Now let n be arbitrary and $a \in \mathbb{Z}$. According to the statement in part (a), the cyclic subgroup $\langle [a] \rangle$ of G is equal to G_d for some d, depending on n and a. Based on your computation in part (b), make a conjecture about how d depends on n and a.

(d) (optional) Prove your conjecture from part (c).

Problem 9 (optional): Let $G = (\mathbb{Z}, +)$, integers with respect to addition, and let H be a subgroup of G. Prove that $H = n\mathbb{Z}$ for some $n \in \mathbb{Z}$ (recall that $n\mathbb{Z} = \{0, \pm n, \pm 2n, \ldots\}$ is the set of all integer multiples of n). The sketch of proof is given below.

Since H is a subgroup, H must contain the identity element (0 in this case). If H consists of 0 alone, then $H = 0 \cdot \mathbb{Z}$, and the assertion of the theorem holds. Otherwise, we can assume that there exists a nonzero element $z \in H$.

(a) Prove that H contains at least one positive integer y. **Hint:** if $z > 0$, we can set $y = z$; if $z < 0$, do something else.

(b) Prove that H contains $m\mathbb{Z}$ for any $m \in H$.

(c) Let n be the smallest positive element of H (why does such n exist?). Prove that $H = n\mathbb{Z}$. **Hint:** assume not. Since H contains $n\mathbb{Z}$ by part (b), the only way H may not equal $n\mathbb{Z}$ is if there exists $x \in H$ such that $x \notin n\mathbb{Z}$. Use division with remainder to obtain contradiction with the choice of n.

Problem 10 (optional):

(a) Prove the formula for the inverse of a product of several elements in a group: if G is a group and $g_1, g_2, \ldots, g_k \in G$, then

$$(g_1 g_2 \ldots g_k)^{-1} = g_k^{-1} g_{k-1}^{-1} \ldots g_1^{-1}. \qquad (***)$$

Hint: You can imitate the proof of the formula $(xy)^{-1} = y^{-1}x^{-1}$ established in Theorem 3.4(e), or you can prove (***) by induction on k (the base case $k = 2$ is precisely the statement of Theorem 3.4(e)). If you are not sure how to set up the induction step, look at how we proved the generalized Euclid's lemma using the regular Euclid's lemma (done some time in week 2 or 3).

(b) Now let G be a group and a, b some elements of G. Define $\langle a, b \rangle$ to be the smallest subgroup of G which contains both a and b. Prove that $\langle a, b \rangle$ is equal to the set

$$S = \{g \in G : g = g_1 g_2 \dots g_k \text{ for some } k \geq 1 \text{ where each } g_i \text{ is equal to } a, b, a^{-1} \text{ or } b^{-1}.\}$$

Note that your proof must consist of two parts

(i) Show that if H is any subgroup of G containing a and b, then H must contain all elements of the set S (this is very easy)

(ii) The set S is a subgroup. This is where part (a) of this problem becomes relevant.