Homework #6. Due Thursday, October 13th, in class

Reading:

1. For this assignment: Section 3.2, beginning of Section 2.3 (pages 71-73) + online Lectures 12.

2. For next week's class: second part of Section 3.2 (starting from page 108), Section 3.5 (up to the middle of page 138) and the beginning of Section 3.4 (in this order) and online Lecture 13 and 14.

Problems:

Problem 1: 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 Problem 6 in HW#5 or proved independently.

Problem 2: Let G be a group and let $H = \{x \in G : x^2 = e\}$, the set of all elements of G whose square is the identity element.

(a) Assume that G is abelian. Prove that H is a subgroup of G. Clearly indicate where you use that G is abelian. **Note:** we did part of this problem in class, but you should present the entire solution.

(b) Give an example of a non-abelian group G such that H is not a subgroup (and prove your answer). **Hint:** you have seen such a group before.

Problem 3: Let G be a group and H and K 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 4:

(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,

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

Prove that $C(a)$ is a subgroup. Note that the proof is started in online Lecture 12. 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 every 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 Problem 3.

Problem 5: Let F be a field and let $n \geq 2$ be an integer. Recall that $GL_n(F)$ is the group of all **invertible** $n \times n$ matrices with entries in F (with respect to multiplication). Also recall that a matrix A with entries in F is invertible $\iff$ $\det(A) \neq 0$.

(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 6: Again let F be a field and $G = GL_2(F)$. For each of the following sets H prove that H is a subgroup of G and determine whether H is abelian or not.

(a) $H = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in F \right\}$

(b) $H = \{A \in G : A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \text{ for some } a, b \in F\} = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a, b \in F, a \neq 0 \right\}$

(c)

$$H = \{A \in G : A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \text{ for some } a, b \in F\} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in F, a^2 + b^2 \neq 0 \right\}$$

Problem 7:

(a) Let A be a set, and let $Sym(A)$ be the set of all **bijective** functions $f : A \to A$. Recall that $Sym(A)$ is a group with respect to composition (we briefly discussed this group in Lecture 10). Fix $a \in A$, and let $H_a = \{f \in Sym(A) : f(a) = a\}$, 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).

Note: The group $Sym(A)$ is discussed in detail in Section 2.3 in the book (but you would not find any group-theoretic terminology there since groups are not introduced in the book until Chapter 3).

Problem 8: 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 9 (practice): 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.

Bonus: Let R be an arbitrary ring and consider R as a group with respect to addition.

(a) Let $S = \{r_1, \ldots, r_k\}$ be a finite subset of R, and let H be the set of all linear combinations of elements of S with integer coefficients, that is,

$$H = \{x \in R : x = n_1 r_1 + \ldots + n_k r_k \text{ for some } n_1, \ldots, n_k \in \mathbb{Z}\}.$$

Prove that H is a subgroup of $(R, +)$ and that if H' is any subgroup of $(R, +)$ containing S, then $H' \supseteq H$ (thus, H is the smallest subgroup of $(R, +)$ containing S). The subgroup H is called *the subgroup generated by* S and is denoted by $\langle S \rangle$. Note that in the case when $S = \{r_1\}$ has just one element the subgroup $\langle S \rangle = \langle r_1 \rangle$ is precisely the cyclic subgroup generated by r_1.

(b) Now assume that $R = \mathbb{Q}$, the rationals. Prove that there is no finite set S such that $\langle S \rangle = \mathbb{Q}$. This property is expressed by saying that the group $(\mathbb{Q}, +)$ is not finitely generated.