Homework #6. Due on Thursday, March 17th, in class

Reading:

1. For this assignment: Online lectures 10-12, [Gilbert, §3.1-3.3] and [Pinter, §3-5].
2. For next week's classes: Online lectures 13 and 14, [Gilbert, §3.4, 3.5] and [Pinter, §9-11].

Problems:

Problem 1 (practice): In each of the following examples determine whether the given set G is a group with respect to a given operation. If G is a group, prove why (that is, verify all the axioms); if G is not a group, state at least one axiom which does not hold and explain why.

(i) $G = (\mathbb{R} \setminus \mathbb{Q}, +)$, the set of all irrational numbers with addition
(ii) $G = (\mathbb{Q}_{>0}, \cdot)$, the set of all rational numbers with multiplication

Problem 2: Let $G = \mathbb{R} \setminus \{-1\}$ be the set of real numbers different from -1, and define the binary operation $*$ on G by $x * y = x + y + xy$. Prove that $(G, *)$ is a group, find its identity element and explicit formula for the inverse of x. **Warning:** None of the four axioms in this example is obvious.

Problem 3: Let R be a ring with 1 (not necessarily commutative), and let $R^\times$ be the set of invertible elements of R, that is,

$$R^\times = \{a \in R : \text{ there exists } b \in R \text{ such that } ab = ba = 1\}.$$

Prove that $R^\times$ is closed with respect to multiplication (that is, if $x, y \in R^\times$, then $xy \in R^\times$). As mentioned in class, this is the main thing one needs to check to show that $R^\times$ is a group with respect to multiplication.

Problem 4 (practice): Compute the multiplication tables for the groups $\mathbb{Z}_5^\times, \mathbb{Z}_8^\times$ and $\mathbb{Z}_{10}^\times$ (here the superscript $\times$ has the same meaning as in Problem 2). Recall that invertible elements of $\mathbb{Z}_n$ are described in Theorem 9.1.

Problem 5 (practice): Let G be a group.

(a) Prove that for any $a, b \in G$ the equation $ax = b$ has exactly one solution $x \in G$. Do the same for the equation $xa = b$.
(b) Deduce from (b) that every row and column of the multiplication table of G contains exactly one element of G (Sudoku puzzle property).

Problem 6: Let F be a field and $n \geq 2$ an integer. Recall from Lecture 10 that $GL_n(F)$ denotes the set of all **invertible** $n \times n$ matrices with coefficients in F. The set $GL_n(F)$ is a group with respect to matrix multiplication (the the identity element of $GL_n(F)$ is the identity matrix, and the inverse of $A \in GL_n(F)$ is the inverse matrix in the usual sense). In order to determine whether a $n \times n$ matrix A lies in $GL_n(F)$ one can use the following result from linear algebra:

Theorem: *Let F be a field and let $n \geq 2$ be an integer. Then an $n \times n$ matrix $A \in Mat_n(F)$ is invertible if and only if $\det(A) \neq 0$.*

Also recall that the determinant of a 2×2 matrix is given by the formula

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc.$$

Thus, $GL_2(F) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in F \text{ and } ad - bc \neq 0. \right\}$

(a) Prove the following formula for inverses in $GL_2(F)$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Recall that if $\lambda \in F$ is a scalar, then by definition $\lambda \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{pmatrix}$. Note that the proof can be shortened using Theorem 11.1.

(b) Let $F = \mathbb{Z}_7$ and $A = \begin{pmatrix} [1] & [2] \\ [3] & [4] \end{pmatrix}$. Find A^{-1} (and simplify your answer). Answer the same question for $F = \mathbb{Z}_5$.

Problem 7: A group G is called *abelian* (=commutative) if $xy = yx$ for ALL $x, y \in G$.

(a) Prove that a group G is abelian $\iff$ $(xy)^2 = x^2y^2$ 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 8: 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.

(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 in class.

Problem 9: 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 10:

(a) 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:** The facts that $C(a)$ contains e and is closed under inversion are proved in online Lecture 12; thus it only 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 9(c).

Problem 11: Let F be a field and let $n \geq 2$ be an integer.

(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 12: (bonus) A subset S of a group G is called a *subsemigroup* if S is non-empty and S is closed under the group operation (that is, if $x \in S$ and $y \in S$, then $xy \in S$).

(a) Prove that if S is a finite subsemigroup, then S is automatically a subgroup of G (that is, S also contains e and is closed under inversion). In particular, any subsemigroup of a finite group must be a subgroup. **Hint:** Consider the part of the multiplication table of G with rows and columns labeled by elements of S (it is an $|S|\times|S|$ "subtable"; you can actually assume that this subtable is located in the left upper corner of the multiplication table of G by choosing a suitable order of elements of G). Since S is a subsemigroup, every entry of this subtable must lie in S as well. First use this fact and the Sudoku property to show that S must contain e (for this you just need to look at a single row of the subtable). Once you know that $e \in S$, use a similar argument to show that S is closed under inversion.

(b) Give an example of a group G and a subsemigroup S of G which is not a subgroup.