Homework #5. Due on Thursday, October 17th, 11:59pm on Canvas

Reading:

1. For this assignment: Online lecture 10 and 11. From Hungerford: 4.3, 7.1 and 7.2

2. For next week's class: Online lecture 12 and beginning of Lecture 13. From Hungerford: 7.3.

Online lectures are currently posted on the Spring 2016 webpage

`https://m-ershov.github.io/3354_Spring2016/`

Problems:

Preface to problem 1: Let F be a field. Recall that we defined irreducible polynomials in $F[x]$ as follows. Let $f \in F[x]$.

(i) First assume that f is monic. Then we say that f is *irreducible* if $f \neq 1$ and the only monic divisors of f in $F[x]$ are 1 and f.

(ii) In general we say that f is irreducible if $f \neq 0$ and the polynomial $\frac{f}{LC(f)}$ (which must be monic) is irreducible. Here $LC(f)$ is the leading coefficient of f.

Note that the definition immediately implies that constant polynomials are never irreducible, while polynomials of degree 1 are always irreducible.

Problem 1:

(a) Let F be an arbitrary field and let $f(x) \in F[x]$ with $\deg(f) = 2$ or 3. Prove that $f(x)$ is NOT irreducible $\iff$ $f(x) = (x-a)g(x)$ for some $g(x) \in F[x]$ and $a \in F$. Do not assume any results about irreducibility (you can freely use any general facts about fields as well as previously established properties of the degree function).

(b) Give an example showing that the assertion of part (a) is false for polynomials of degree 4 (at least for some field F).

(c) Let p be a prime (so that $\mathbb{Z}_p$ is a field). Find the number of irreducible monic polynomials of degree 2 in $\mathbb{Z}_p[x]$. **Hint:** First use (a) to find the number of monic polynomials of degree 2 which are reducible (that is, not irreducible).

(d) List explicitly all irreducible monic polynomials of degree 2 in $\mathbb{Z}_3[x]$. **Hint:** This should follow from your proof in (c).

Problem 2: 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.

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

Note: For (b) use the following definition of $\mathbb{Q}_{>0}$: a rational number lies in $\mathbb{Q}_{>0}$ if it can be written as $\frac{a}{b}$ for some $a, b \in \mathbb{Z}_{>0}$ (but do not assume any other facts about inequalities in $\mathbb{Q}$).

Problem 3: 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 an explicit formula for the inverse of x. **Warning:** None of the four axioms in this example is obvious.

Problem 4: 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 5: Compute the multiplication tables for the groups $\mathbb{Z}_7^{\times}, \mathbb{Z}_8^{\times}$ and $\mathbb{Z}_{10}^{\times}$ (here the superscript $\times$ has the same meaning as in Problem 4).

In Problem 6 and 7 below we use multiplicative notation in groups.

Problem 6: In Lecture 12 on Mon, October 7th, we started analyzing the possible structure of the multiplication tables for groups of order 4. Using the Sudoku property, we proved that if G is a group of order 4 and G contains an element x such that $x^2 \neq e$, then $G = \{e, x, x^2, x^3\}$, and the multiplication table is as follows:

	e	x	x^2	x^3
e	e	x	x^2	x^3
x	x	x^2	x^3	e
x^2	x^2	x^3	e	x
x^3	x^3	e	x	x^2

(here the entries in the first column and the first row are the row and column labels, respectively).

Thus, it remains to consider groups G of order 4 such that $g^2 = e$ for all $g \in G$. Let G be such a group, and let $x \neq y$ be any distinct non-identity elements of G. Prove that $G = \{e, x, y, xy\}$ and compute its multiplication table with full justification. The answer should be determined uniquely.

Problem 7: A group G is called *abelian* (=commutative) if $xy = yx$ for ALL $x, y \in G$. Prove that a group G is abelian $\iff$ $(xy)^2 = x^2y^2$ for all $x, y \in G$.

Note/warning: By definition $g^2 = g * g$ where $*$ is the group operation. 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 F be a field. Recall from Lecture 10 that $GL_2(F)$ denotes the set of all **invertible** 2×2 matrices with coefficients in F. The set $GL_2(F)$ is a group with respect to matrix multiplication (the identity element of $GL_2(F)$ is the identity matrix, and the inverse of $A \in GL_2(F)$ is the inverse matrix in the usual sense). In order to determine whether a 2×2 matrix A lies in $GL_2(F)$ 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 $\lambda \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{pmatrix}$ **Hint:** Computation will be very short if use a suitable part of 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 $F = \mathbb{Z}_5$.