Final Exam Math 370 F 2020 (Take-Home)

Instructions: You may consult any written source in notes, books, or on the internet, but all work must be your own. Create a pdf of your solutions and upload it to canvas by 6p.m. EST on Tuesday, December 22. If you upload your final after Dec. 18, please also email a copy of the pdf to jhaglund@math.upenn.edu.

1. (10 points. This is problem 3 on p. 367 in Herstein.) Show that any finite subring of a division ring is a division ring.

2. (10 points. This is problem 6 on p. 360 in Herstein.) If F is a finite field, by the quaternions over F we shall mean the set of all

$$\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k,$$

where $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in F$ and where addition and multiplication are carried out as in the real quaternions (i.e. $i^2 = j^2 = k^2 = ijk = -1$, etc.). Prove that the quaternions over a finite field *do not* form a division ring.

3. (10 points) Prove that a group of order $n = 2p$, p prime, is either cyclic or dihedral.

4. (10 points) Let K be a finite field. Prove that the product of the nonzero elements of K is -1.

5. (10 points). The polynomials $f(x) = x^3+x+1, g(x) = x^3+x^2+1$ are irreducible in $\mathbb{Z}_2[x]$. Give an explicit isomorphism between the finite fields $\mathbb{Z}_2/(f(x))$ and $\mathbb{Z}_2/(g(x))$. *Hint:* see the example in the file on canvas of class lecture notes titled "Math370Week14".

6. (10 points). Prove that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean Domain. *Hint:* One way to proceed is to try and modify the proof of Theorem 3.8.1 on p. 150 of Herstein, that the Gaussian Integers $\mathbb{Z}[i]$ are a Euclidean Domain.

7. (10 points). Prove that any group of order p^2q is not simple, where p, q are distinct primes.

8. (10 points). Let $\epsilon = \pm 1$, and let $a, b \in \{0, 1\}$ be binary variables. Define a set G_2 of eight 2×2 matrices $\epsilon(a|b)$ given by

$$\epsilon(a|b) = \epsilon \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{a} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^{b}.$$

a) Prove that

$$[\epsilon(a|b)][\epsilon(a|b)] = [\epsilon(a|b)](a \oplus a'|b \oplus b'),$$

where $\oplus$ denotes binary addition, and that G_2 is a group with respect to matrix multiplication. (G_2 is a way to represent the dihedral group D_4 although you do not need to prove that).

b) Prove there is only one subgroup F of G_2 generated by an element of order 4.

The next problems involve Kronecker products of matrices, which are important in representation theory. Given a $p \times p$ matrix $X = [x_{i,j}]$ and a $q \times q$ matrix $Y = [y_{i,j}]$, the *Kronecker product* $X \otimes Y$ is defined by

$$X \otimes Y = \begin{pmatrix} x_{11}Y & \cdots\cdots & x_{1p}Y \\ \vdots & & \vdots \\ x_{p1}Y & \cdots\cdots & x_{pp}Y \end{pmatrix}.$$

Given a second $p \times p$ matrix $X' = [x'_{ij}]$ and a second $q \times q$ matrix $Y' = [y'_{ij}]$, it is not hard to see that

$$(X \otimes Y)(X' \otimes Y') = (XX') \otimes (YY').$$

In general,

$$[X_1 \otimes X_2 \otimes \cdots \otimes X_m]\,[Y_1 \otimes Y_2 \otimes \cdots \otimes Y_m] = X_1Y_1 \otimes \cdots \otimes X_mY_m.$$

9. (20 points). Let $\epsilon = \pm 1$ and for $i = 0, 1, \ldots m-1$, let $a_i b_i \in \{0, 1\}$ be binary variables. Define a set G_{2^m} of 2^{2m+1} matrices $\epsilon(a_{m-1} \cdots a_0|b_{m-1} \cdots b_0)$ of size 2^m, where

$$\epsilon(a_{m-1} \cdots a_0|b_{m-1} \cdots b_0) = \epsilon \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{a_{m-1}} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^{b_{m-1}} \right] \otimes \cdots \otimes \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{a_0} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^{b_0} \right].$$

a) Identify

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

as matrices $\epsilon(a_1a_0|b_1b_0)$ in G_4.

b) Prove that

$$[\epsilon(a|b)][\epsilon'(a'|b')] = (-1)^{ab'^T + a'b^T}[\epsilon'(a'|b')][\epsilon(a|b)],$$

(where x^T denotes the transpose of the row vector x) and that G_{2^m} is a group with respect to matrix multiplication.

c) Prove that every non-identity element of G_{2^m} has order $1, 2$ or 4.

d) Let

$$\mathbf{1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \mathbf{i} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \mathbf{j} = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \mathbf{k} = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Verify that $Q_8 = \{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$ is a group of order 8.