Ve203 Discrete Mathematics (Fall 2016)

Assigment 3: Groups, Fields, Numbers

Date Due: 4:00 PM, Thursday, the 13th of October 2016

JOINT INSTITUTE
交大密西根学院

This assignment has a total of **(40 Marks)**.

Exercise 3.1 Roots of Unity

For this exercise, you may use everything you know about complex numbers from calculus.

i) Show that the set $S = \{z \in \mathbb{C} \colon |z| = 1\}$ is a group $(S, \cdot)$ with the group operation being the usual multiplication of complex numbers.

   (2 Marks)

ii) Show that for any $n \in \mathbb{N} \setminus \{0\}$ the set $S(n) = \{z \in \mathbb{C} \colon z^n = 1\}$ is a group with the usual multiplication of complex numbers.

   (2 Marks)

Exercise 3.2 Matrix Groups

For this exercise, you may use everything you know about matrices and real numbers from linear algebra or calculus. The set of $n \times n$ matrices with real coefficients is denoted by $\mathrm{Mat}(n \times n; \mathbb{R})$.

i) The matrix representing a rotation of $\mathbb{R}^2$ by the angle φ is given by

$$A(\varphi) = \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix}.$$

   Show that the set $S = \{A(\varphi) \colon \varphi \in \mathbb{R}\}$ is a group, with the group operation being the usual matrix multiplication.

   (2 Marks)

ii) Show that the following sets of matrices are groups (with group operation being matrix multiplication):

   (a) The *special linear group* $\mathrm{SL}(n, \mathbb{R}) := \{A \in \mathrm{Mat}(n \times n, \mathbb{R}) \colon \det A = 1\}$.
   (b) The *orthogonal group* $\mathrm{O}(n, \mathbb{R}) := \{A \in \mathrm{GL}(n, \mathbb{R}) \colon A^T = A^{-1}\}$.
   (c) The *special orthogonal group* $\mathrm{SO}(n, \mathbb{R}) := \{A \in \mathrm{O}(n, \mathbb{R}) \colon \det A = 1\}$.

   (3 Marks)

Exercise 3.3

Let

$$m \sim n \qquad :\Leftrightarrow \qquad 2 \mid (n - m), \qquad\qquad m, n \in \mathbb{Z}.$$

i) Show that $\sim$ is an equivalence relation.

   (1 Mark)

ii) What partition $\mathbb{Z}_2 := \mathbb{Z}/\sim$ is induced by $\sim$?

   (1 Mark)

iii) Define addition and multiplication on $\mathbb{Z}_2$ by the addition and multiplication of class representatives, i.e.,

$$[m] + [n] := [m + n], \qquad\qquad [m] \cdot [n] := [m \cdot n].$$

   Show that these operations are well-defined, i.e., independent of the representatives m and n of each class.

   (2 Marks)

iv) Show that $(\mathbb{Z}_2, +, \cdot)$ is a field.

   (2 Marks)

Remark: Everything that you may have learned about vector fields over the real numbers or complex numbers remains valid for vector spaces over general fields, such as the one introduced here.

Exercise 3.4
Prove Corollary 1.6.11 of the lecture:

> Let $a, b \in \mathbb{Z}$ with $|a| + |b| \neq 0$. Then
>
> $$T(a,b) = \{n \in \mathbb{Z} \colon n = ax + by,\ x, y \in \mathbb{Z}\}$$
>
> is the set of all integer multiples of $\gcd(a,b)$.

(2 Marks)

Exercise 3.5
Use the Division Algorithm to show that for any $n \in \mathbb{N}$ there exists a $k \in \mathbb{N}$ such that either $n^2 = 3k$ or $n^2 = 3k + 1$.
(3 Marks)

Exercise 3.6
Let $a \in \mathbb{Z}$ and $n \in \mathbb{N}$. Prove that $\gcd(a, a+n)$ divides n. Deduce that a and $a+1$ are always relatively prime.
(3 Marks)

Exercise 3.7
Find all $x, y \in \mathbb{Z}$ such that

i) $56x + 72y = 40$,

   (2 Marks)

ii) $84x - 439y = 156$.

   (2 Marks)

Exercise 3.8

i) Suppose $a, b \in \mathbb{N} \setminus \{0\}$ with $\gcd(a,b) = 1$ and let $c \in \mathbb{Z}$. Show that there exist infinitely many solutions $x, y \in \mathbb{N}$ of the Diophantine equation $ax - by = c$.

   (3 Marks)

ii) Find $x, y \in \mathbb{N}$ such that $158x - 57y = 7$.

   (2 Marks)

Exercise 3.9
Consider the set S of all positive integers of the form $3k+1$: $S = \{n \in \mathbb{N} \colon n = 3k+1,\ k \in \mathbb{N}\}$. An integer in S is said to be prime if it cannot be factored into two smaller integers, each of which belongs to S. (Thus, 10 and 25 are prime, while 16 and 28 are not.)

i) Prove that any member of S is either prime or a product of primes.

   (2 Marks)

ii) Give an example to show that it is possible for an element of S to be factored into primes in more than one way.

   (1 Mark)

Exercise 3.10
Let D be the set of all the primes of the form $4 \cdot n + 3$ for $n \in \mathbb{N}$. We suppose D to be finite and define $d = 4 \cdot (3 \cdot 7 \cdots p) - 1$, where p is the largest prime in D.

i) Prove that no prime of the form $4 \cdot k + 3$ divides d.

   (1 Mark)

ii) Prove that d is not divisible by $4 \cdot k + 1$.

   (2 Marks)

iii) Conclude that there is an infinite number of primes of the form $4 \cdot n + 3$.

(2 Marks)

*N*ote: The general version of this result is called Dirichlet's theorem and states that if a and b are non-zero coprime natural numbers then there are an infinite number of primes of the form $an + b$ for $n \in \mathbb{N}$.