MATH 111, Assignment 1 Solutions

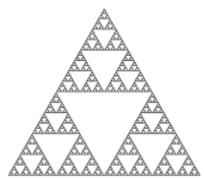
Name: Dillon Allen **Date:** August 26, 2021
Group Name:N/A

1. Typeset the following text using LaTeX.

Many graphs contain substructures that may give information about their 'host' graph; One such substructure is a cycle.

Definition 1. *A sequence of distinct vertices* $x_1, x_2, \ldots, x_k$*, for all* $i = 1, \ldots k$*, and edges* $e_1, e_2, \ldots, e_k$*, such that each edge* $e_i = x_i x_{i+1}$ *is called a path. If we allow* x_1 *and* x_{k+1} *to be the same vertex, then the path is said to be a cycle.*

Example 1. *In* K_7*, consider the sequence of edges,* x_1x_2, x_2x_3, x_3x_1*, whcih forms a 3-cycle that can be seen as the highlighted triangle in Figure 1.*



Lemmma 1. *All cycles contained in the Heawood graph must be of even length.*

Proof. We provide a proof by contradiction, let x_i be a vertex of C_{14} and assume that the Heawood graph contains a cycle of odd length, denoted by $C = x_1 x_2 \ldots x_k x_1$. Since C is an odd-length cycle, then k must be odd. Since the Heawood graph is bipartite, then all vertices can be partitioned into two disjoint and pairwise non-adjacent sets U, V. Since x_i and x_{i+1} are adjacent, without loss of generality, suppose that $x_i \in U$ and $x_{i+1} \in V$, for all i odd. Hence $\{x_1, x_3, \ldots, x_k\} \subseteq U$ and $\{x_2, x_4, \ldots, x_{k-1}\} \subseteq V$. Note that x_k, x_1 are adjacent in C, but x_1 and x_k are both in U, contradicting that U is pairwise non-adjacent. Thus the Heawood graph does not contain a cycle of odd length. $\square$

2. Type the following text into LaTeX (problem 2).

With this lemma, we can now prove the following two theorems. Since in our study we only deal with finite fields, it is enough to prove the Frobenius map is an automorphism if F is finite.

Theorem 1. *Let p be prime and F a field such that $char(F) = p$. Then,*

$$\phi : F \to F : x \mapsto x^p$$

is an automorphism.

Proof. Using the Binomial Theorem, we have that $(a+b)^p = a^p + b^p$ and so

$$\phi(a+b) = \phi(a) + \phi(b)$$

Since F is a field, then all elements in F commute, which implies that $(ab)^p = b^p a^p = a^p b^p$. Hence, this gives us that $\phi(ab) = \phi(a)\phi(b)$. Therefore, ϕ is a homomorphism of fields. Suppose F is finite. Now, let $x \in F$ and suppose $x \in Ker(\phi)$. Then, we can see that

$$\begin{aligned} x \in Ker(\phi) &\iff \phi(x) = 0_F \\ &\iff x^p = 0_F \\ &\iff x = 0_F, \end{aligned}$$

where the last equation follows from F not containing any zero divisors. Thus, since F is finite and ϕ is injective then by the 2-out-of-3 property, ϕ is bijective. $\square$

Theorem 2. *Every element in F_q is a solution of the equation $x^q = x$.*

Proof. We have the $|F_q| = q = p^n$, for some prime p, and $n \in \mathbb{N}$. Suppose that $x \in F_q$. We will consider the following two cases.

(Case 1) Suppose that $x = 0_{F_q}$. Then, it is easy to see that $x^{p^n} = x$.

(Case 2) Suppose that $x \neq 0_{F_q}$. Then, $x \in F_q^*$. Since F_q is a finite field, then F_q^* is the multiplicative group with $|F_q^*| = q - 1 = p^n - 1$. Since F_q^* is a finite group, then $x^{|F_q^*|} = 1_{F_q}$; and thus, $x^{p^n-1} = 1_{F_q}$. By multiplying both sides by x, we get $x^{p^n} = x$. Therefore, $x^q = x$. $\square$

Now, we embark on our study of field extensions by first introducing some basic definitions and results.

Definition 2. *If K is a field containing a subfield F, then K is a field extension of F which will be denoted as K/F.*