MATH 122 PSET 9 DUE 12/3 BY THE END OF THE DAY

The total number of points for all problems is 50.

I remind you that using AI to give you answers to or help you answer homework problems is just as much cheating and unethical and honor code violating as asking a person to do that. I trust you will hold yourself to the highest ethical standards!

1. Problem 1

Let F be a finite field.

Remark 1.1. Please feel free to assume that $F = \mathbb{Z}/p\mathbb{Z}$ if that feels simpler!

The goal of this problem is to show that the group $(F^\times, \cdot)$ is cyclic.

a) (5 points) Set $n := |F^\times|$. Prove that to show that $(F^\times, \cdot)$ is cyclic it's enough to find an element $x \in F^\times$ such that the order of x is n.

b) (5 points) For $k|n$ let $f(k)$ be the number of elements of $(F^\times, \cdot)$ that have order k. By a) our goal is to check that $f(n) > 0$. Show that if $a \in F^\times$ has order k, then the only roots of the polynomial $x^k - 1$ are $1, a, \ldots, a^{k-1}$.

Hint: use that the number of roots of a polynomial is at most its degree.

c) (5 points) Conclude from b) that $f(k) \leqslant \varphi(k)$.

Hint: use that the number of elements of order k in $\mathbb{Z}/k\mathbb{Z}$ is equal to $\varphi(k)$.

d) (5 points) Combining part c) above with Problem 4 f) of PSet 8 show that $\sum_{k|n} f(k) \leqslant n$.

e) (5 points) Conclude from d) that we must have an equality $f(k) = \varphi(k)$, in particular, $f(n) = \varphi(n) > 0$. This finishes the argument.

2. Problem 2

The goal of this problem is to prove that if D is a division ring and V is a *finitely generated* module over D, then V must be *isomorphic* to $\underbrace{D \times D \times \ldots \times D}_{n}$ for some $n \in \mathbb{Z}_{\geqslant 0}$.

a) (5 points) First of all recall that we equip $\underbrace{D \times D \times \ldots \times D}_{n}$ with a module structure over D defined as follows:

$$(a_1, \ldots, a_n)+(b_1, \ldots, b_n) = (a_1+b_1, \ldots, a_n+b_n),\ c\cdot(a_1, \ldots, a_n) = (ca_1, \ldots, ca_n). \quad (2.1)$$

Show that (2.1) indeed defines the D-module structure on $\underbrace{D \times D \times \ldots \times D}_{n}$.

b) (10 points) A subset $\{v_1, \ldots, v_n\} \subset V$ is called a *basis* if for every $v \in V$ there exist *unique* $a_1, \ldots, a_n \in F$ such that

$$v = \sum_{i=1}^{n} a_i v_i.$$

Prove that every finitely generated vector space contains a basis. You can do this as follows. Pick any collection $v_1, \ldots, v_n$ of generators of V such that n is *minimal possible* (i.e., if you delete one of v_i's the rest of them, will *not* generate V). If they do not form a basis then there exist $a_1, \ldots, a_n$ such that not all of them are zero and such that:

$$a_1 v_1 + a_2 v_2 + \ldots + a_n v_n = 0.$$

Without loosing the generality we can assume that $a_n \neq 0$ (otherwise reorder v_i's). We conclude that

$$v_n = -\frac{a_1 v_1 + \ldots + a_{n-1} v_{n-1}}{a_n} \text{ (here we use that } D \text{ is a division ring).} \quad (2.2)$$

Deduce from (2.2) that $v_1, \ldots, v_{n-1}$ must be generators (because $v_1, \ldots, v_n$ are). This contradicts the assumption on n.

c) (10 points) Pick any basis $\{v_1, \ldots, v_n\}$ in V. Show that the map:

$$D \times D \times \ldots \times D \to V,\ (a_1, a_2, \ldots, a_n) \mapsto a_1 v_1 + \ldots + a_n v_n \in V$$

is an isomorphism of vector spaces.