PSET11

Student: Ryan Baldwin, rbaldwi2@swarthmore.edu

Professor: Dr. Hsu

Collaborators:

Peer Reviewers:

Due Date: April 27, 2025

Chapter 11: 7.1 Prove that a domain of finite order is a field.

Proof. Let R have characteristic p for some prime p and let $a \in R$. Because the ring is finite, a has finite order under multiplication. Let k and l be two integers such that $a^k = a^l$.

Without loss of generality, assume $k > l$. Then we can we can subtract a^l from both sides to get $a^k - a^l = 1$. Factoring out by a^l, we have $a^l(a^{k-l} - 1) = 0$. Since R is a domain, either $a^l = 0$ or $a^{k-l} - 1 = 0$. The first case is impossible since a is nonzero. Thus, we have $a^{k-l} = 1$. This means that a has a multiplicative inverse, and hence R is a field. □

Chapter 11: 7.3 Is there a domain that contains exactly 15 elements?

Proof. Since a domain of finite order must be a field (per Artin Chapter 11: 7.1), the number of elements in a finite domain must be a power of a prime, (i.e., of the form p^n for some prime p and positive integer n.).

Since 15 can be decomposed into $3 \cdot 5$, we can see that 15 is not a prime power. Thus, there cannot be a domain of finite order with exactly 15 elements as the order of a domain must be a prime power. □

Chapter 12: 1.5 Let a and b be relatively prime integers. Prove that there are integers m and n such that $a^m + b^n \equiv 1 \mod ab$.

Proof. Since a and b are relatively prime, , then there are integers solutions r and s such that $ar + bs = 1$. Raising this expression to the xyth power, we see that $(ar + bs)^{xy} = 1^{xy} = 1$.

Notice that when we expand the binomial $(ar+bs)^{xy}$ and reduce modulo ab, all terms that are multiples of ab will reduce to 0. The only terms that will not reduce to 0 are those that do not contain a multiple of ab.

Hence,

$$(ra + sb)^{xy} \equiv (ra)^{xy} + (sb)^{xy} \mod ab \equiv 1 \mod ab.$$

Furthermore, after distributing the mnth power, we see that

$$r^{xy}a^{xy} + s^{xy}b^{xy} \equiv 1 \mod ab.$$

Because there exists integer solutions (r, s) that satisfy the pair (a, b) such that $ar + bs = 1$, then (a, b) must conversely be a solution to (r, s) in $ra + sb = 1$. Thus, r is coprime to b and s is coprime to a. This implies that there must exist an integer xy such that $r^{xy} \equiv 1 \mod b$ and $s^{xy} \equiv 1 \mod a$. Equivalently, we say that $r^{xy} = 1 + kb$ and $s^{xy} = 1 + la$ for some integers k and l.

Thus, we can write $r^{xy}a^{xy} + s^{xy}b^{xy} \equiv 1 \mod ab$ as

$$(1 + kb)a^{xy} + (1 + la)b^{xy} \equiv 1 \mod ab.$$

Distributing and reducing modulo ab, we have

$$a^{xy} + b^{xy} \equiv 1 \mod ab.$$

Since xy is an integer, we can say, more generally, that there exist integers m and n such that $a^m + b^n \equiv 1 \mod ab$.

□