Math 561/661 | **Fall 2018**

Homework 5 | **Drew Armstrong**

---

1. Quotient Rings. Let $(R,+,\times,0,1)$ be a *commutative ring*. Technically: This means that (1) $(R,+,0)$ is an abelian group, (2) $(R,\times,1)$ is a commutative monoid (abelian group without inverses), and (3) for all $a,b,c\in R$ we have $a(b+c)=ab+ac$.

(a) Let $I\subseteq R$ be an additive subgroup and recall that "addition of cosets" is well-defined:

$$(a+I)+(b+I)=(a+b)+I.$$

Thus we obtain the quotient group $(R/I,+,0+I)$. Now suppose that for all $a\in R$ and $b\in I$ we have $ab\in I$. (Jargon: We say that $I\subseteq R$ is an *ideal*.) In this case prove that the following "multiplication of cosets" is well-defined:

$$(a+I)(b+I)=(ab)+I.$$

It follows that $(R/I,+,\times,0+I,1+I)$ is a ring, called the *quotient ring*. [You do not need to check all the details.]

(b) Apply part (a) to show that $\mathbb{Z}/n\mathbb{Z}$ is a ring.

2. The Fermat-Euler-Lagrange Theorem, Part II. Let $(R,+,\times,0,1)$ be a ring and let $R^\times\subseteq R$ denote the subset of elements that have multiplicative inverses. We call $(R^\times,\times,1)$ the *group of units*.

(a) For all $n\in\mathbb{Z}$ prove that $(\mathbb{Z}/n\mathbb{Z})^\times=\{a+n\mathbb{Z}:\gcd(a,n)=1\}$. [Hint: If $\gcd(a,n)=1$ then we have $a\mathbb{Z}+n\mathbb{Z}=1\mathbb{Z}$, hence there exist integers $x,y\in\mathbb{Z}$ with $ax+ny=1$. This is sometimes called *Bézout's Identity*.]

(b) **Euler's Totient Theorem.** Euler's totient function is defined by $\phi(n):=\#(\mathbb{Z}/n\mathbb{Z})^\times$. For all $a\in\mathbb{Z}$ with $\gcd(a,n)=1$ prove that

$$a^{\phi(n)}=1 \mod n.$$

(c) **Fermat's Little Theorem.** If $p\in\mathbb{Z}$ is prime and $p\nmid a$ prove that

$$a^{p-1}=1 \mod p.$$

3. Chinese Remainder Theorem. In this problem I will use the shorthand notation $[a]_n:=a+n\mathbb{Z}$. Now fix some $m,n\in\mathbb{Z}$ with $\gcd(m,n)=1$ and consider the function

$$\begin{array}{rccc}\varphi: & \mathbb{Z}/mn\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}\\ & [a]_{mn} & \mapsto & ([a]_m,[a]_n).\end{array}$$

(a) Prove that φ is **well-defined**. That is, for all $a,a'\in\mathbb{Z}$ prove that

$$[a]_{mn}=[a']_{mn} \quad \text{implies} \quad [a]_m=[a']_m \text{ and } [a]_n=[a']_n.$$

(b) For all $c\in\mathbb{Z}$ prove that $m|c$ and $n|c$ together imply $(mn)|c$. [Hint: There exist $x,y\in\mathbb{Z}$ such that $mx+ny=1$.] Use this conclude that φ is **injective**.

(c) Prove that φ is **surjective**. [Big Hint: Given $([a]_m,[b]_n)$ we want to find $c\in\mathbb{Z}$ such that $[a]_m=[c]_m$ and $[b]_n=[c]_n$. Try $c:=any+bmx$.]

(d) Prove that φ restricts to a bijection

$$\varphi:(\mathbb{Z}/mn\mathbb{Z})^\times\longleftrightarrow(\mathbb{Z}/m\mathbb{Z})^\times\times(\mathbb{Z}/n\mathbb{Z})^\times.$$

[Hint: Use the fact that $\gcd(k,\ell)=1$ if and only if there exist integers $x,y\in\mathbb{Z}$ such that $kx+\ell y=1$.] It follows that Euler's totient is multiplicative: $\phi(mn)=\phi(m)\phi(n)$.

4. Automorphisms of a Cyclic Group. For all integers $n \in \mathbb{Z}$ prove that

$$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

[Hint: Show that any automorphism $\varphi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ has the form $\varphi_a([k]_n) := [ak]_n$ for some integer $a \in \mathbb{Z}$ satisfying $\gcd(a, n) = 1$.]

5. Matrix Representation of Isometries. Consider the following set of matrices:

$$G = \left\{ \left(\begin{array}{ccc|c} & A & & \mathbf{u} \\ \hline 0 & \cdots & 0 & 1 \end{array} \right) : A \in O(n) \text{ and } \mathbf{u} \in \mathbb{R}^n \right\} \subseteq \mathrm{Mat}_{n+1}(\mathbb{R}).$$

(a) Prove that $G \subseteq \mathrm{Mat}_{n+1}(\mathbb{R})$ is a subgroup. [Hint: Block multiplication.]

(b) Use results from class to prove that G is isomorphic to the group $\mathrm{Isom}(\mathbb{R}^n)$ of isometries of n-dimensional Euclidean space.

6. Second and Third Isomorphism Theorems.

(a) Let $H, K \subseteq G$ be subgroups with $K \trianglelefteq G$ normal. We already know that $HK \subseteq G$ is a subgroup. Prove that $K \trianglelefteq HK$ is a normal subgroup and the map $h \mapsto hK$ defines a surjective group homomorphism $H \to (HK)/K$ with kernel $H \cap K$. It follows that

$$\frac{H}{H \cap K} \cong \frac{HK}{K}.$$

(b) Now consider another normal subgroup $N \trianglelefteq G$ such that $N \subseteq K$. Prove that $N \trianglelefteq K$ is normal and that the map $gN \mapsto gK$ defines a surjective group homomorphism $G/N \to G/K$ with kernel K/N. It follows that

$$\frac{G/N}{K/N} \cong \frac{G}{K}.$$

7. Dimension of a Vector Space, Part II. Let V be a vector space over a field $\mathbb{F}$.

(a) Let $\mathbf{u}_1, \ldots, \mathbf{u}_n \in V$ be a basis and consider the subspaces $V_k := \mathbb{F}(\mathbf{u}_1, \ldots, \mathbf{u}_k) \subseteq V$. Prove for all $0 \le k < n$ that there is no subspace U satisfying

$$V_k \subsetneq U \subsetneq V_{k+1}.$$

(b) Conversely, suppose that we have a maximal chain of subspaces

$$\{\mathbf{0}\} = V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_n = V.$$

Prove by induction that V_k has a basis of size k, hence $\dim(V_k) = k$. Parts (a) and (b) together show that **dimension** equals the **length** of a maximal chain of subspaces

(c) If $U \subseteq V$ is a subspace you may assume that the quotient group V/U is a vector space. Prove that $\dim(V/U) = m$ if and only if there exists a maximal chain of subspaces

$$U = V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_m = V.$$

[Hint: You may assume that the Correspondence Theorem and the First Isomorphism Theorem still hold after replacing the word "subgroup" with "subspace."[1]]

(d) Prove that $\dim(V) = \dim(U) + \dim(V/U)$. [Hint: Combine (a), (b) and (c).]

(e) **Rank-Nullity Theorem.** For any linear function $\varphi : V \to W$ prove that

$$\dim(V) = \dim(\ker \varphi) + \dim(\mathrm{im}\, \varphi).$$

[1] For that matter, the Second and Third Isomorphism Theorems also hold.