**School of Mathematical and Computational Sciences**
Abstract Algebra

Prof. Pablo Rosero
& Christian Chávez
Problem Set 3

# Cyclic Groups, Normality, Quotients and the Isomorphism Theorems

(Lessons 6, 7, and 8)

## 1. Workout guide

Let $A$ be a ring with unit. Show that if $u$ is invertible in $A$ then so is $-u$. Prove that ${}_p$ is a field iff $p$ is prime. **Hint:** Prove first that ${}_p$ is a integral domian iff $p$ is prime, then use Proposition **??**. Prove point iii) of **??**. The direct product of the rings $A$ and $B$ is the cartesian product $A \times B$ endowed with the operations defined by

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2),$$
$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2, y_1 y_2).$$

Prove that $A \times B$ is a ring with these operations. Prove that if $A$ and $B$ are Abelian, then so is its direct product. Describe the divisors of zero of $A \times B$. Describe the invertible elements of $A \times B$. Assume that $A$ and $B$ are non trivial rings. Explain why $A \times B$ can not be an integral domain. Let $I$ be any nonempty index set and let $\{A_i\}_{i \in I}$ an indexed family of rings. Prove that $\prod_{i \in I} A_i$ is a ring under componentwise addition and multiplication. If $I =^+ \cup \{0\}$, prove that $\coprod_{i \in I} A_i$ under componentwise addition and multiplication. Prove that $A[x]$ is a ring. Let $(A, +, \cdot)$ be a ring. Prove that for any $a, b, c \in A$,

$$a(b - c) = ab - ac, \quad (b - c)a = ba - ca.$$

Assume that $a, b \in A$ are such that $ab = -ba$. Prove that

$$(a + b)^2 = (a - b)^2 = a^2 + b^2.$$

Assume that $A$ is an integral domain. Prove that

$$\forall a, b \in A : \quad a^2 = b^2 \Rightarrow (a = b \vee a = -b);$$
$$\forall x \in A : \quad x = x^{-1} \Rightarrow x \in \{-1, 1\}.$$

Prove that if $(A, +)$ is a cyclic group, then $A$ is a commutative ring. Let $A$ a non-void set equipped with internal operations $+$ and $\cdot$. Assume that $(A, +)$ is a group, $(A, \cdot)$ is a semigroup, and that

$$\forall a, b, c \in A : \quad a \cdot (b + c) = a \cdot b + a \cdot c \ \wedge \ (b + c) \cdot a = b \cdot a + c \cdot a;$$

$$\exists 1 \in A, \forall x \in A : \quad x \cdot 1 = 1 \cdot x = 1.$$

Prove that $A$ is a ring with unit. Let $(A,+,\cdot)$ be a nontrivial ring with unit and $a,b,c\in A$. Prove that if $a$ is invertible, then

$$ab = ac \;\Rightarrow\; b = c,$$

and that $a$ has only one multiplicative inverse. Prove that if $a^2=0$, then $a+1$ and $a-1$ are invertible. Prove that if $a$ and $b$ are invertible, then $ab$ is invertible. Prove that $(A^\times,\cdot)$ is a group. Let $(F,+,\cdot)$ be a field with $|F|=m\in\mathbb{N}$. Prove that

$$\forall x\in F\setminus\{0\}: \quad x^{m-1}=1. \tag{1}$$

Let $A$ be a commutative ring and $a,b\in A$. Prove that if $ab$ is invertible, then $a$ and $b$ are both invertible. Let $(A,+,\cdot)$ be a nontrivial ring and $a,b,c\in A$. Prove that if $a\notin\{-1,1\}$ and $a^2=1$, then $a+1$ and $a-1$ are zero divisors Prove that if $ab$ is a divisor of zero, then either $a$ or $b$ is a zero divisor. Prove that in a nontrivial commutative ring with unit, a zero divisor cannot be invertible. Consider $A=(,\oplus,\odot)$ where

$$a\oplus b = a+b-1, \quad a\odot b = ab-(a+b)+2.$$

Prove that $A$ is a commutative ring with unit. Indicate the zero element, the unit, and the negative of an arbitrary $a$. Is $A$ an integral domain? Consider $A=(\times,\oplus,\odot)$ where

$$(a,b)\oplus(c,d)=(a+c,b+d), \quad (a,b)\odot(c,d)=(ac-bd,ad+bc).$$

Prove that $A$ is a commutative ring with unit. Indicate the zero element, the unit element, and the negative of an arbitrary $a$. Prove that $A$ is a field and indicate the multiplicative inverse of an arbitrary nonzero element. Consider Example **??** and $A=Q(\sqrt{2})$. Prove that $A$ is a commutative ring with unit. Indicate the zero element, the unit, and the negative of an arbitrary $a=x+y\sqrt{2}$. Prove that $A$ is a field. Verify that  satisfies all the axioms of a commutative ring with unit. Indicate the zero element and invertible elements. Describe the zero divisors in . Explain why  is neither a field nor an integral domain. Let $\Omega\neq\emptyset$ be a set and consider $A=(,\Delta,\cap)$. Prove that $A$ is a commutative ring with unit. Describe the zero divisors and the invertible elements of $A$. Explain why $A$ is not an integral domain. Give the tables for additiona and multiplication of $A$ for $\Omega=\{a,b,c\}$. The set of *quaternions*, , can be seen as the elements of [2]() with the form

$$\alpha=\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi\end{pmatrix}, \quad a,b,c,d\in . \tag{2}$$

Prove that  endowed with the usual addition and multiplication of matrices is a non-commutative ring with unit. Prove that $\alpha$ as given in (**??**) can be written, in *standard notation*, as

$$\alpha = a\mathbf{1}+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}, \tag{3}$$

where

$$\mathbf{1}=\begin{pmatrix}1&0\\0&1\end{pmatrix}, \quad \mathbf{i}=\begin{pmatrix}i&0\\0&-i\end{pmatrix}, \quad \mathbf{j}=\begin{pmatrix}0&1\\-1&0\end{pmatrix}, \quad \mathbf{k}=\begin{pmatrix}0&i\\i&0\end{pmatrix}.$$

Prove that

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{1}; \tag{4}$$

$$\mathbf{ij} = -\mathbf{ji} = \mathbf{k}, \quad \mathbf{jk} = -\mathbf{kj} = \mathbf{i}, \quad \mathbf{ki} = -\mathbf{ik} = \mathbf{j}. \tag{5}$$

The *conjugate* and *norm* of the quaternion $\alpha = a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ are, respectively,

$$\overline{\alpha} = a\mathbf{1} - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}, \tag{6}$$

$$\|\alpha\| = \sqrt{a^2 + b^2 + c^2 + d^2}. \tag{7}$$

Prove that

$$\alpha\overline{\alpha} = \overline{\alpha}\alpha = \|\alpha\|^2\mathbf{1}.$$

Prove that  is a *skew field* i.e., it's a (not necessarily commutative) ring with unit in which every nonzero element has a multiplication inverse.  Let $G$ be an additive Abelian group. An endomorphism on $G$ is a homomorphism from $G$ into $G$. Prove that $\mathrm{End}(G)$, the set of endomorphisms on $G$ becomes a ring with unit when it's endowed with addition and the composition product.  Let $(A, +, \cdot)$ be a ring. An element $a \in A$ is said to be *nilpotent* if

$$\exists n \in \mathbb{N} : \quad a^n = 0.$$

Prove that if $A$ has a unit element and $a \in A$ is nilpotent, then both $a + 1$ and $a - 1$ are invertible. Prove that if $A$ is commutative and $a \in A$ is nilpotent, then $xa$ is nilpotent, for all $x \in A$. Prove that if $A$ is commutative and $a, b \in A$ are nilpotent, then $a + b$ is nilpotent.