Math 210A: Algebra, Homework 9

Ian Coley

December 3, 2013

Problem 1.
Determine all subrings of \( \mathbb{Z} \).

Solution.
Let \( R \subset \mathbb{Z} \) be a subring. Then we must have \( 1 \in R \). Since \( R \) is closed under addition, we have \( 1 + \ldots + 1 = n \in R \). Since \( R \) is closed under taking additive inverse, \( -n \in R \) for every \( n \). Therefore we must have \( R = \mathbb{Z} \). \( \square \)

Problem 2.
Determine all subrings of \( \mathbb{Z} \times \mathbb{Z} \).

Solution.
By the above reasoning, in any subring \( R \subset \mathbb{Z} \times \mathbb{Z} \), we must have all elements of the form \( (n, n) \). This is one such subring. Suppose now that any other \( (m, n) \in R \). Then \( (m, n) + (n, -n) = (m - n, 0) \) is in \( R \), so it suffices to examine what elements of the form \( (k, 0) \) (or equivalently \( (0, k) \)) are in \( R \). Since \( R \) is closed under addition, the element \( (0, k) \) yields \( (0, n \cdot k) \) (and \( (n \cdot k, 0) \)) for any \( n \in \mathbb{Z} \). Therefore we can obtain any element of the form \( (m, n) \) where \( m \equiv n \mod k \). If we include the case where \( k = 1 \) (which yields the subring \( \mathbb{Z} \times \mathbb{Z} \)), this gives us every subring of \( \mathbb{Z} \times \mathbb{Z} \). \( \square \)

Problem 3.
Determine all ideals of \( \mathbb{Z} \times \ldots \times \mathbb{Z} \) \( n \) times.

Solution.
First, since \( \mathbb{Z} \) is a principal ideal domain, we know that every ideal is of the form \( m\mathbb{Z} \). We claim that every ideal of \( \mathbb{Z}^n \) is of the form

\[
m_1\mathbb{Z} \times \ldots \times m_n\mathbb{Z}
\]

for some integers \( m_1, \ldots, m_n \). First, it is clear that every \( \prod m_i\mathbb{Z} \) is an ideal in \( \mathbb{Z}^n \). Conversely, suppose that \( J \subset \mathbb{Z}^n \) is an ideal. Let \( \pi_1, \ldots, \pi_n \) be the canonical projections onto the components of \( \mathbb{Z}^n \). By the last homework assignment, the image of an ideal is an ideal under surjection, so \( \pi_i(J) \subset \mathbb{Z} \) is an ideal for each \( i \). Then consider the map

\[
\pi : J \rightarrow \pi_1(J) \times \ldots \times \pi_n(J)
\]

defined in the obvious way. This map is an isomorphism by the Chinese Remainder Theorem, so we are done. \( \square \)
Problem 4.
Give an example of a commutative ring \( R \) and two distinct ideals \( I \) and \( J \) of \( R \) such that \( I \cap J \neq IJ \).

Solution.
Let \( R = \mathbb{Z} \), \( I = 2\mathbb{Z} \), and \( J = 4\mathbb{Z} \). Then \( I \cap J = 4\mathbb{Z} \), but \( IJ = 8\mathbb{Z} \), which are not equal. \( \square \)

Problem 5.
Determine all finite rings of 2 and 3 elements.

Solution.
Let \( R \) be a ring with 2 elements. Then these elements must be 0 and 1, where \( 1 + 1 = 0 \). This ring is unique up to isomorphism since 0 and 1 have unique roles in any ring.

Now let \( R \) be a ring with 3 elements, \( R = \{0, 1, r\} \). Since \( R \) has an underlying abelian group structure, it must be isomorphic to \( \mathbb{Z}/3\mathbb{Z} \), so we may write \( R = \{0, 1, 2\} \) where \( 1+1 = 2 \) and \( 2+1 = 0 \). Since we know how to multiply by 0 and 1, we need only show how to multiply by 2. We have
\[
2 \cdot r = (1 + 1) \cdot r = r + r
\]
for any \( r \in R \), so there is only one way to multiply by 2, given by the abelian group structure of \( R \) isomorphic to \( \mathbb{Z}/3\mathbb{Z} \). Therefore there is only one ring with three elements up to isomorphism. \( \square \)

Problem 6.
Let \( R \) be a commutative ring, \( r \in R \). Prove that there is a unique ring homomorphism \( f : \mathbb{Z}[X] \to R \) such that \( f(X) = r \). Show that the image of \( f \) is the smallest subring of \( R \) that contains \( r \).

Solution.
We claim the ring homomorphism required is completely defined by \( f(X) = r \). Since we must have \( f(1) = 1_R \), we have \( f(n) = n \cdot f(1) = \underbrace{1_R + \cdots + 1_R}_{n \text{ times}} \). We also have \( f(-n) = -f(n) \), \( f \) restricted to \( \mathbb{Z} \) is without choice for any ring homomorphism. In our case, given any polynomial \( g = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X] \), we have
\[
f(g) = \sum_{i=0}^{n} f(a_i X^i) = \sum_{i=0}^{n} f(a_i) \cdot f(X)^i = \sum_{i=0}^{n} \underbrace{r^i + \cdots + r^i}_{a_i \text{ times}},
\]
since \( f \) is uniquely defined on \( \mathbb{Z} \) and \( X \) and respects multiplication.

The smallest subring containing \( r \) must be closed under addition and multiplication and contain 0 and 1. The image of any ring homomorphism must contain 0 and 1, so that condition is settled. Further, the above construction shows that precisely any sum of any powers of \( r \) is in the image of \( f \). Further, this homomorphism is clearly unique, so we are done. \( \square \)

Problem 7.
Let \( R \) be an integral domain such that \( R[X] \) is a principal ideal domain. Prove that \( R \) is a field.
Solution.
Let \( r \in R \) be a nonzero element. Then \((r, X) \subset R[X]\) is an ideal, so we must have \((r, X) = (f)\) for some polynomial \( f \). Further, there exist polynomials \( p, q \) such that \( fp = r \) and \( fq = X \). Since \( R \) is an integral domain, \( R[X] \) has the property that \( \text{deg} fg = \max\{\text{deg} f, \text{deg} g\} \). Therefore since \( \text{deg} r = 0 \), we must have \( \text{deg} f = 0 \) so \( p = b \) and \( f = a \) are constant functions. Additionally, \( q = c + dX \) is a linear function. Therefore
\[
X = fq = a(c + dX) = ac + adX
\]
so we have \( ad = 1 \). Therefore \((f) = (a) = R[X]\), the entire ring. Therefore there exist \( \alpha, \beta \in R[X] \) such that
\[
\alpha r + \beta X = 1.
\]
Again by the properties of degree, we must have \( \beta = 0 \) so \( \alpha r = 1 \). Therefore \( r \) is invertible.

Therefore \( R \) is a commutative division ring, so it is a field.

Problem 8.
Prove that for every nonzero commutative ring, the ring \( R[X] \) has infinitely many prime ideals.

Solution.
We follow Euclid’s proof. By Zorn’s Lemma, there exists some prime ideal \( p \) of \( R[X] \). Proceeding by induction, suppose that we have \( n \) prime ideals, \( p_1, \ldots, p_n \). Let \( a_i \in p_i \) for each \( i \), and choose these such that the product \( a_1 \cdots a_n \neq -1 \) and that \( X \) appears at least once in the product. This is always possible via the replacement \( a_1X \) for \( a_1 \).

Let \( a = a_1 \cdots a_n + 1_R \neq 0 \). We claim that \( a \notin p_i \) for every \( i \). Suppose \( a \in p_1 \). Then since \( a_1 \mid a_1 \cdots a_n \), we have \( a_1 \cdots a_n \in p_1 \). Therefore we must have \( 1_R \in p_1 \) as well, which is a contradiction since \( p_1 \) is a prime ideal. Therefore there must be another prime ideal \( p \) containing \( a \), since \( a \) is not invertible. Therefore by induction, there are infinitely many primes.

Problem 9.
Let \( B \subset A \) be a subgroup of an abelian group \( A \). Prove that the set
\[
I = \{ f \in \text{End} A : f(A) \subset B \}
\]
is a right ideal in the ring \( \text{End} A \).

Solution.
Let \( f, g \in I \) and \( h \in \text{End} A \). First, note that \((f + g)(A) = f(A) + g(A)\), where both \( f(A), g(A) \subset B \). Since \( B \) is closed under addition, we have \( f(A) + g(A) \subset B \), so \( f + g \in I \). Further \((f \circ h)(A) = f(h(A))\). Since \( h \) is an endomorphism of \( A \), we have \( h(A) \subset A \), so \( f(h(A)) \subset f(A) \subset B \), hence \( f \circ h \in I \). Therefore \( I \) is a right ideal of \( \text{End} A \).

Problem 10.
The Jacobson radical of a commutative ring \( R \) is the ideal \( \text{Rad} R \) that is the intersection of all maximal ideals in \( R \). Show that \( x \in \text{Rad} R \) if and only if \( 1 - xy \in R^x \) for all \( y \in R \).
Solution.
First, let $x \in \text{Rad } R$ and suppose that $1 - xy$ is not invertible. Then $1 - xy \in \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. Then since $x \in \text{Rad } R \subset \mathfrak{m}$, we have $xy \in \mathfrak{m}$. Therefore $(1 - xy) + xy = 1 \in \mathfrak{m}$, which is a contradiction. Therefore every $1 - xy$ must be invertible.

Conversely, suppose that $x \notin \text{Rad } R$. Then $x \notin \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. Then $R = \mathfrak{m} + Rx$, so we have $1 = m + xy$ for some $y \in R$, $m \in \mathfrak{m}$. Then $m = 1 - xy$ cannot be invertible since $\mathfrak{m} \neq R$. Since we have proved the contrapositive of the converse, we are done.