Math 125 Modern Algebra
Second Test Answers
November 2017

Scale. 90–104 A. 70–89 B. 50-69 C. Median 91.

1. [20; 10 points each part] Recall that a commutative ring satisfies the cancellation law if whenever \( xy = xz \) and \( x \neq 0 \), then \( y = z \). Recall that a commutative ring has no zero-divisors if whenever \( xy = 0 \), then either \( x = 0 \) or \( y = 0 \).

In parts a and b you’ll prove the following theorem: A commutative ring satisfies the cancellation law if and only if it has no zero-divisors.

a. Prove that if a commutative ring \( R \) satisfies the cancellation law, then it has no zero-divisors.

There are, of course, many proofs. Here’s one.

Proof. Suppose the ring satisfies the cancellation law. Let \( x \) be a nonzero element in the ring. If \( xy = 0 \), then \( xy = x0 \), so by that cancellation law, \( y = 0 \). Thus the ring has no zero-divisors. Q.E.D.

b. Prove that if a commutative ring \( R \) has no zero-divisors, then it satisfies the cancellation law.

Proof. Suppose that the ring has no zero-divisors. We’ll show it satisfies the cancellation law. If \( x \neq 0 \) and \( xy = xz \), then \( x(y - z) = 0 \), and since \( x \) is not a zero divisor, therefore \( y - z = 0 \), so \( y = z \). Thus the ring satisfies the cancellation law. Q.E.D.

2. [16] The Chinese Remainder Theorem states that if \( k \) and \( m \) are relatively prime and \( n = km \), then \( \mathbb{Z}_n \cong \mathbb{Z}_k \times \mathbb{Z}_m \) where an element \([x]_n\) corresponds to the pair \(( [x]_k, [x]_m \)\). In other words, the pair of simultaneous congruences

\[
\begin{align*}
x &\equiv a \pmod{k} \\
x &\equiv b \pmod{m}
\end{align*}
\]

has a unique solution for \( x \) modulo \( n \).

Solve this pair of simultaneous congruences

\[
\begin{align*}
x &\equiv 5 \pmod{20} \\
x &\equiv 20 \pmod{21}
\end{align*}
\]

for \( x \) modulo \( 20 \cdot 21 = 420 \). Use whatever method you like, but show your work.

Here’s Brahmagupta’s method using modern algebra. We’re looking for an \( x \) such that

\[
x = 20s + 5 = 21t + 20.
\]

So we need \( s \) and \( t \) so that

\[
20s = 21t + 15.
\]

Rewrite the equation as \( 20s = 20t + t + 15 \), then \( 20(s - t) = t + 15 \), and introduce another variable \( u = s - t \) so the equation becomes \( 20u = t + 15 \). That’s the first step in the extended Euclidean algorithm. You could continue in this way, but you can also find a solution to \( 20u = t + 15 \) by inspection, namely \( u = 1 \) and \( t = 5 \). Therefore \( x = 21t + 20 = 21 \cdot 5 + 20 = 125 \).

There are many variants of Brahmagupta’s algorithm. There’s also Qin Jiushao’s algorithm which works fine.

Also, since the numbers are fairly small, you could actually just search for a solution. Since \( x \equiv 5 (\pmod{20}) \), therefore the candidates for \( x \) are 5, 25, 45, 65, 85, 105, 125, etc. Of these, the first one that satisfies \( x \equiv 20 (\pmod{21}) \) is 125.

3. [16] Recall that we defined a Boolean ring as a ring in which every element is idempotent \( x^2 = x \), and we proved that Boolean rings are commutative and that \( x + x = 0 \) holds in a Boolean ring.

Boolean rings correspond to Boolean algebras where multiplication \( x \cdot y \) in the Boolean ring corresponds to intersection \( x \cap y \) in a Boolean algebra, and \( x + y + xy \) in the Boolean ring corresponds to union \( x \cup y \) in a Boolean algebra.

Since in a Boolean algebra, union distributes over intersection \( x \cup (y \cap z) = (x \cup y) \cap (x \cup z) \), therefore the corresponding equation in Boolean rings must also hold. That corresponding equation is

\[
x + yz + xyz = (x + y + xy)(x + z + xz).
\]

Using those facts about Boolean rings mentioned in the first paragraph above, prove that that equation holds in all Boolean rings.

Expanding the right side of the equation, we get

\[
(x + y + xy)(x + z + xz) = x^2 + xz + x^2z + xy + yz + xyz + x^2y + xy + x^2y + yz
\]

but \( x^2 = x \) so that

\[
x + xz + xz + xy + yz + xyz + xy + xyz + xz + xz + xz + xz = x + yz + xyz
\]

There are several pairs of identical terms, so they cancel making that

\[
x + yz + xyz
\]

which is the left side of the equation.

4. [16] Determine the kernel of the ring homomorphism \( f : \mathbb{Z}_{20} \to \mathbb{Z}_5 \) where \( f([x]_{20}) = [x]_5 \). It is enough to list the elements in the kernel.

What elements of \( \mathbb{Z}_{20} \) are sent to \([0]_5 \) in \( \mathbb{Z}_5 \)? Any multiple of 5 is 0 in \( \mathbb{Z}_5 \), so the elements \([0]_{20}, [5]_{20}, [10]_{20}, \text{ and } [15]_{20}\) are in the kernel of \( f \).

Typically, we don’t write elements of \( \mathbb{Z}_n \) so formally as congruence classes, so an answer of 0, 5, 10, and 15 is fine.
5. Let \( R \) be the polynomial ring \( \mathbb{Q}[x] \), and let \( I \) be the principal ideal \((x^2 - 3)\) generated by the polynomial \( x^2 - 3 \). In other words, the elements of \( I \) are polynomials of the form \((x^2 - 3)f(x)\) where \( f(x) \) is any polynomial in \( R \).

Describe in your own words the quotient ring \( R/I = \mathbb{Q}[x]/(x^2 - 3) \). Is it a field?

It’s the rational number field with \( \sqrt{3} \) adjoined, usually written \( \mathbb{Q}[\sqrt{3}] \) or \( \mathbb{Q}(\sqrt{3}) \). It’s a field since \( x^2 - 3 \) has no roots in \( \mathbb{Q} \).

Note that \( \mathbb{Q}[x]/(x^2 - 4) \) is not a field, so any argument that \( \mathbb{Q}[x]/(x^2 - 3) \) is a field must explicitly consider the polynomial \( x^2 - 3 \).

6. [20; 4 points each part] True/false. For each sentence write the whole word “true” or the whole word “false”. If it’s not clear whether it should be considered true or false, you may explain in a sentence if you prefer.

a. The natural numbers \( \mathbb{N} = \{0, 1, 2, \ldots\} \) is a ring. False. It doesn’t have negation.

b. Every integral domain is a subring of a field. True. We showed that every integral domain can be extended to its field of fractions.

c. The product of two fields is a field. False. It never is. For example, \((1, 0)\) doesn’t have a reciprocal.

d. If a ring is a finite integral domain, then it is a field. True. There are no finite integral domains that aren’t fields.

e. A morphism \( f : A \rightarrow B \) in a category is defined to be an isomorphism if there exists another morphism \( g : B \rightarrow A \), called its inverse, such that \( f \circ g = 1_A \). False. It is necessary that \( f \circ g = 1_B \) and \( g \circ f = 1_A \).