MATH 100B: Homework #3

Due on Feb 1, 2024 at 12:00pm

Professor McKernan

Section A02 6:00PM - 6:50PM
Section Leader: Castellano-Macías

Source Consulted: Textbook, Lecture, Discussion, Office Hour

Ray Tsai
A16848188

Problem 1

If a, b are integers and $3 \nmid a$ or $3 \nmid b$, show that $3 \nmid (a^2 + b^2)$.

Proof. Suppose that $3 \nmid a$. Then, $a \mod 3$ is either 1 or 2, so $a^2 \equiv 1 \mod 3$. Similarly, if $3 \nmid b$ then $b^2 \equiv 1 \mod 3$. Otherwise, $3 \nmid b$ and so $b^2 \equiv 0 \mod 3$. This implies that $a^2 + b^2 \mod 3$ is either 2 or 1, so 3 does not divide $a^2 + b^2$. □

Problem 2

Show that in Example 2, R/M is a field having nine elements.

Proof. Since M is a maximum ideal, R/M is a field. Note that $M = \langle 3 \rangle$. Let $r = a+bi+M \in R/M$. Suppose that $a \equiv m \mod 3$ and $b \equiv n \mod 3$. Then, $r = m+3l+(n+3k)i+M = m+ni+3(l+ki)+M = m+ni+M$. This implies that r can only have $3 \cdot 3 = 9$ possibilities, and thus $|R/M| = 9$. □

Problem 3

In Example 4, show that R/M is a field having 25 elements.

Proof. Since $M = \langle 5 \rangle$, M is an ideal. We show that M is a maximal ideal. Suppose that $N \supset M$, $N \neq M$ is an ideal. There exists $a + b\sqrt{2} \in N \backslash M$. Consider $t = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$. Since N is an ideal in R, t is an integer in N. Note that for all $x \nmid 5$, $x^2 \mod 5$ is either 1 or 4. Since $a + b\sqrt{2} \notin M$, we may assume $a \nmid 5$. Then, we know $a^2 \mod 5$ can be either 1 or 4, and $b^2 \mod 5$ can be either 0, 1, or 4. Notice that there are no possible combinations of a, b that allow $t = a^2 - 2b^2 \equiv 0 \mod 5$, so $t \nmid 5$. Since $\gcd(t, 5) = 1$, we know $ut + 5w = 1$, for some $u, w \in \mathbb{Z}$. However, since N, M are both ideals, $ut \in N$ and $5w \in M \subset N$, and thus $ut + 5w = 1 \in N$. This immediately follows that $N = R$, so M is a maximal ideal, and thus R/M is a field.

Let $r = a + b\sqrt{2} + M \in R/M$. Suppose that $a \equiv m \mod 5$ and $b \equiv n \mod 5$. Then, $r = m + 5l + (n + 5k)\sqrt{2} + M = m + ni + 5(l + k\sqrt{2}) + M = m + n\sqrt{2} + M$. This implies that r can only have $5 \cdot 5 = 25$ possibilities, and thus $|R/M| = 25$. □

Problem 4

Using Example 2 as a model, construct a field having 49 elements.

Proof. Consider $M = \langle 7 \rangle$. M is an ideal. We show that M is a maximal ideal. Suppose that $N \supset M$, $N \neq M$ is an ideal. There exists $a + bi \in N \backslash M$. Consider $t = (a + bi)(a - bi) = a^2 + b^2$. Since N is an ideal in R, t is an integer in N. Note that for all $x \nmid 7$, $x^2 \mod 7$ is either 1, 2, or 4. Since $a + bi \notin M$, we may assume $a \nmid 7$. Then, we know $a^2 \mod 7$ can be either 1, 2, or 4, and $b^2 \mod 7$ can be either 0, 1, 2, or 4. Notice that there are no possible combinations of a, b that allow $t = a^2 + b^2 \equiv 0 \mod 7$, so $t \nmid 7$. Since $\gcd(t, 7) = 1$, we know $ut + 7w = 1$, for some $u, w \in \mathbb{Z}$. However, since N, M are both ideals, $ut \in N$ and $7w \in M \subset N$, and thus $ut + 7w = 1 \in N$. This immediately follows that $N = R$, so M is a maximal ideal, and thus R/M is a field.

Let $r = a+bi+M \in R/M$. Suppose that $a \equiv m \mod 7$ and $b \equiv n \mod 7$. Then, $r = m+7l+(n+7k)i+M = m + ni + 7(l + ki) + M = m + ni + M$. This implies that r can only have $7 \cdot 7 = 49$ possibilities, and thus $|R/M| = 49$. □

Problem 5

Let R be a ring and let I be an ideal of R, not equal to the whole of R. Suppose that every element not in I is a unit. Prove that I is the unique maximal ideal in R.

Proof. Suppose that $N \supset I$, $N \neq I$ is an ideal. Then, there exists $n \in N$ such that n is invertible, which makes $N = R$. Thus, I is a maximal ideal. We now show that I is the unique maximal ideal. Let I' be a maximal ideal. Since $I' \neq R$, all elements in I' are not invertible. However, since every element not in I is a unit and $I \neq R$, I contains all the non-invertible elements, and thus $I \supseteq I'$. This immediately follows that I' is a maximal ideal, so $I = I'$. □

Problem 6

Let $\varphi : R \to S$ be a ring homomorphism and suppose that J is a prime ideal of S.

(i) Prove that $I = \varphi^{-1}(J)$ is a prime ideal of R.

Proof. Define $\psi : S \to S/J$ as the natural projection. We know Ker $\psi \circ \varphi = \varphi^{-1}(\psi^{-1}(0)) = \varphi^{-1}(J) = I$. Suppose $a, b \in R$ such that $ab \in I$. Since S/J is an integral domain, $\psi \circ \varphi(ab) = \psi \circ \varphi(a)\psi \circ \varphi(b) = 0$ implies that $\psi \circ \varphi(a)$ or $\psi \circ \varphi(b)$ is 0. This immediately follows that a or b is in I, so I is a prime ideal. □

(ii) Give an example of an ideal J that is maximal such that I is not maximal.

Proof. Consider homomorphism $\mathbb{Z} \hookrightarrow \mathbb{Q}$. Since $\mathbb{Q}$ is a field, $\{0\}$ is a maximal ideal. However, the zero ideal is not a maximal ideal of $\mathbb{Z}$. □

Problem 7

Prove that every prime element of an integral domain is irreducible. Let R be a commutative ring.

Proof. Suppose that $p = ab$ is a prime. Hence, we may assume that $a \in \langle p \rangle$, or, $a = kp$ for some $k \in \mathbb{R}$. We then get $p = ab = kbp$, Since R is an integral domain, $kb = 1$ and the result now follows. $\square$

Problem 8

Our aim is to prove a very strong form of the Chinese Remainder Theorem. First we need some definitions. Let I and J be two ideals. We say that I and J are coprime if $I + J = R$.

(a) Show that I and J are coprime if and only if there is an $i \in I$ and a $j \in J$ such that $i + j = 1$.

Proof. Suppose that I and J are coprime. Then, $1 \in I + J = R$, so there exists $i \in I$ and $j \in J$ such that $i + j = 1$. Conversely, suppose that there is an $i \in I$ and a $j \in J$ such that $i + j = 1$. Consider $(i + j)r$ for some $r \in R$. Since I, J are ideals, $ir \in I$ and $jr \in J$. However, this implies that $r = (i + j)r = ir + jr \in I + J$, so $I + J = R$. □

(b) Show that if I and J are coprime then $IJ = I \cap J$.

Proof. Let $ij \in IJ$, for $i \in I$ and $j \in J$. Since I and J are both ideals, $ij \in I$ and $ij \in J$, so $ij \in I \cap J$. Conversely, suppose that $r = i + j \in I \cap J$. Since I, J are groups under addition, $i + j \in I$ and $i + j \in J$ implies that $i, j \in I \cap J$. From part (a), we know that there exists $i' \in I, j' \in J$, such that $i' + j' = 1$. Then we get $r = (i + j)(i' + j') = i'(i + j) + (i + j)j'$. However, since $i + j \in I \cap J$, we get that $i'(i + j) + (i + j)j' = i'j_r + i_r j' \in IJ$, for $i_r = j_r = i + j$. Therefore, $IJ = I \cap J$. □

Problem 9

Suppose that $I_1, I_2, \ldots, I_k$ are ideals of R. We say these ideals are pairwise coprime, if for all $i \neq j$, I_i and I_j are coprime. If $I_1, I_2, \ldots, I_k$ are pairwise coprime, show that the product I of the ideals $I_1, I_2, \ldots, I_k$ is equal to the intersection, that is

$$\prod_{i=1}^{k} I_i = \bigcap_{i=1}^{k} I_i.$$

Proof. We proceed by induction on k. The base case is trivial. Suppose $k > 1$. By induction, we know $\prod_{i=1}^{k-1} I_i = \bigcap_{i=1}^{k-1} I_i$. Note that $\bigcap_{i=1}^{k-1} I_i$ is an additive subgroup. Let $r \in R$ and $i \in \bigcap_{i=1}^{k-1} I_i$. Since $I_1, I_2, \ldots, I_k$ are all ideals, $ri \in \bigcap_{i=1}^{k-1} I_i$, and so the intersection is also an ideal. Thus, it suffices to show that I_k and $\prod_{i=1}^{k-1} I_i$ are coprime, by the result we obtained from the previous problem. Since $I_1, I_2, \ldots, I_k$ are pairwise coprime, for each pair of ideals, say I_m, I_n, there exists $i_m \in I_m$ and $i_n \in I_n$ such that $i_m + i_n = 1$, which we denote as $1_{m,n}$. We know

$$\prod_{m<n\leq k} 1_{m,n} = \prod_{m<n\leq k} (i_m + i_n) = 1.$$

Note that in the expansion of $\prod_{m<n\leq k}(i_m + i_n)$, each term is the product of elements from at least $k-1$ distinct ideals I_i, for $1 \leq i \leq k$. Since I_k is an ideal, each term that is divided by an element from I_k is in I_k, and thus there exists $i'_k \in I_k$ that is the sum of those terms. On the other hand, the rest of the terms are products of elements from each of I_i, for $1 \leq i < k$, and thus the sum of those terms is in $\prod_{i=1}^{k-1} I_i$, we denote as i_Π. Therefore, we get $1 = i'_k + i_\Pi \in I_k + \prod_{i=1}^{k} I_i$. This immediately follows that $I_k + \prod_{i=1}^{k} I_i = R$, and we are done. □

Problem 10

Let R_i denote the quotient R/I_i. Define a map,

$$\phi : R \longrightarrow \bigoplus_{i=1}^{k} R_i,$$

by $\phi(a) = (a + I_1, a + I_2, \ldots, a + I_k)$

(a) Show that ϕ is a ring homomorphism.

Proof. ϕ is obviously well defined. Suppose that $a, b \in R$. Then,

$$\begin{aligned}\phi(a+b) &= (a+b+I_1, a+b+I_2, \ldots, a+b+I_k)\\ &= (a+I_1, a+I_2, \ldots, a+I_k) + (b+I_1, b+I_2, \ldots, b+I_k)\\ &= \phi(a) + \phi(b),\end{aligned}$$

$$\begin{aligned}\phi(ab) &= (ab+I_1, ab+I_2, \ldots, ab+I_k)\\ &= (a+I_1, a+I_2, \ldots, a+I_k)(b+I_1, b+I_2, \ldots, b+I_k)\\ &= \phi(a)\phi(b),\end{aligned}$$

and most importantly, $\phi(1) = (1 + I_1, 1 + I_2, \ldots, 1 + I_k)$. Thus, ϕ is a homomorphism. □

(b) Show that ϕ is surjective if and only if the ideals $I_1, I_2, \ldots, I_k$ are pairwise coprime.

Proof. idk bro. □

(c) Show that ϕ is injective if and only if I, the intersection of the ideals $I_1, I_2, \ldots, I_k$, is equal to the zero ideal.

Proof. Suppose that ϕ is injective. Then, we know for all $a, b \in R$, $a \neq b$ implies $(a + I_1, a + I_2, \ldots, a + I_k) \neq (b + I_1, b + I_2, \ldots, b + I_k)$. That is, there exists I_i that does not contain $a - b$. However, for all nonzero $r \in R$, $r = m - n \neq 0$, for some $m, n \in R$, so $r \notin \bigcap_{i=1}^{k} I_i$. Since the intersection of groups is still a group, $I = \bigcap_{i=1}^{k} I_i$ can only be $\{0\}$.

We now assume the converse. Suppose that $(a + I_1, a + I_2, \ldots, a + I_k) = (b + I_1, b + I_2, \ldots, b + I_k)$, for some $a, b \in R$. Then, $a - b \in \bigcap_{i=1}^{k} I_i = \{0\}$, so $a = b$. The result then follows. □

Problem 11

Deduce the Chinese Remainder Theorem, which states that if $I_1, I_2, \ldots, I_k$ are pairwise coprime and the product I is the zero ideal, then R is isomorphic to $\bigoplus_{i=1}^{k} R_i$. Show how to deduce the other versions of the Chinese Remainder Theorem, which are stated as exercises in the book.

Proof. By the previous problem, the conditions given here makes the natural mapping $\phi : R \longrightarrow \bigoplus_{i=1}^{k} R_i$ an isomorphism, and thus $R \simeq \bigoplus_{i=1}^{k} R_i$.

We now deduce the other version of the Chinese Remainder Theorem. Let $m, n \in \mathbb{Z}$ such that $\gcd(m, n) = 1$. Consider $I_m = \langle m \rangle, I_n = \langle n \rangle$, for some coprime $m, n \in \mathbb{Z}$. That is, let I_m be the set of multiples of m and I_n be the set of multiples of n. We know that $I_m \cap I_n = I_{mn}$, the set of multiples of mn. Since m, n are coprime, $um + vn = 1$, for some $u, v \in \mathbb{Z}$. However, since $1 = um + vn \in I_m + I_n$, we know I_m and I_n are coprime. Since $I_m \cap I_n = I_{mn}$, we get $\mathbb{Z}/(I_m \cap I_n) = \mathbb{Z}_{mn} \simeq \mathbb{Z}_m \oplus \mathbb{Z}_n$. □