Math 308
3-4-1994

Solutions to Problem Set 2.

1. Let G be an abelian group. A subset $\{x_a\}_{a \in A} \subset G$ is **independent** if

$$b_1 x_{a_1} + \cdots + b_n x_{a_n} = 0, \qquad b_k \in \mathbb{Z}, \quad a_k \in A, \quad n \geq 1$$

implies $b_1 x_{a_1} = \cdots = b_n x_{a_n} = 0$. In words, if a finite linear combination of elements of $\{x_a\}_{a \in A}$ with integer coefficients is 0, then all the terms in the combination are 0.

Note that the set $\{x_a\}_{a \in A}$ need not be finite, or even countable.

For example, the elements $(1, 0)$ and $(0, 1)$ form an independent set in $\mathbb{Z} \oplus \mathbb{Z}$. On the other hand, the set $\{(2, 2), (-1, 3), (10, -6)\}$ is not independent in $\mathbb{Z} \oplus \mathbb{Z}$, since

$$3 \cdot (2, 2) + (-4) \cdot (-1, 3) + (-1) \cdot (10, -6) = (0, 0).$$

A subset that is not independent is **dependent**.

(a) Show that any subset of $(\mathbb{Q}, +)$ containing more than one element but not containing 0 is dependent.

Let S be a subset of $(\mathbb{Q}, +)$ containing more than one element but not containing 0. Let $\dfrac{a}{b}$, $\dfrac{c}{d}$ be distinct elements of S. Then

$$cb \cdot \frac{a}{b} + (-ad) \cdot \frac{c}{d} = ac - ac = 0.$$

But $cb \cdot \dfrac{a}{b} \neq 0$ and $(-ad) \cdot \dfrac{c}{d} \neq 0$. Hence, S is dependent. □

(b) Prove or disprove: The subset $\{(1, 1), (1, -1)$ of $\mathbb{Z} \oplus \mathbb{Z}$ is independent.

Suppose

$$m \cdot (1, 1) + n \cdot (1, -1) = (0, 0).$$

Equating corresponding components yields $m + n = 0$ and $m - n = 0$, so $m = n = 0$. Therefore, $m \cdot (1, 1) = n \cdot (1, -1) = (0, 0)$, so the set $\{(1, 1), (1, -1)$ is independent. □

(c) Let G be an abelian group. An independent subset of G is a **maximal independent set** if it is not properly contained in any other independent subset of G.

Prove that every independent set in an abelian group is contained in a maximal independent set.

Let S be an independent subset of the abelian group G. Let $\mathcal{A}$ be the set of independent subsets of G which contain S. Order $\mathcal{A}$ by set inclusion. Since $S \in \mathcal{A}$, $\mathcal{A} \neq \emptyset$.

Let $\mathcal{B}$ be a chain in $\mathcal{A}$. I will show $\mathcal{B}$ has an upper bound in $\mathcal{A}$. Let

$$T = \bigcup_{U \in \mathcal{B}} U.$$

Clearly, T contains S, since each $U \in \mathcal{B}$ contains S. I claim that T is independent. Suppose then that

$$b_1 x_1 + \cdots + b_n x_n = 0, \qquad b_k \in \mathbb{Z}, \quad x_k \in T.$$

Suppose $x_k \in U_k \in \mathcal{B}$. Since $\mathcal{B}$ is a chain, one of $U_1, \ldots, U_n$ contains all the others. Suppose that U_m contains U_k for $k = 1, \ldots, n$. Then

$$b_1 x_1 + \cdots + b_n x_n = 0, \qquad b_k \in \mathbb{Z}, \quad x_k \in U_m.$$

By independence of U_m, $b_k x_k = 0$ for all k. Hence, T is independent.

Now T is an independent set containing S, and T contains every element of $\mathcal{B}$. Hence, T is an upper bound for $\mathcal{B}$. By Zorn's lemma, $\mathcal{A}$ has maximal elements. Such a maximal element will be a maximal independent set containing S. $\square$

[page 228]

1. Show that the correspondence $x \mapsto 5x$ from $\mathbb{Z}_5$ to $\mathbb{Z}_{10}$ is not well defined (that is, the correspondence is not a function).

This question should be interpreted as follows: There are integers x and y such that $x = y \bmod 5$ but $5x \neq 5y \bmod 10$. For example, take $x = 0$ and $y = 5$. Now $5 = 0 \bmod 5$, but $25 \neq 0 \bmod 10$. $\square$

---

4. Let $\mathbb{Z}_3[i] = \{a + bi \mid a, b \in \mathbb{Z}_3\}$. Show that $\mathbb{Z}_3[i]$ is isomorphic to $\mathbb{Z}_3[x]/\langle x^2+1\rangle$.

Define $\phi : \mathbb{Z}_3[x] \to \mathbb{Z}_3[i]$ by

$$\phi(f) = f(i).$$

It's easy to check that ϕ is a ring map (indeed, any evaluation map is a ring map).

$$\phi(a + bx) = a + bi,$$

so ϕ is surjective.

$\phi(x^2+1) = i^2 + 1 = 0$, so $\langle x^2+1\rangle \subset \ker\phi$.

Let $f(x) \in \mathbb{Z}_3[x]$. By the Division Algorithm, there are polynomials $q(x)$, $r(x)$, with $\deg r(x) < \deg f(x)$, such that

$$f(x) = (x^2+1)\cdot q(x) + r(x).$$

Since $\deg f = 2$ and $\deg r < \deg f$, $r(x) = a + bx$ for some a and b. Therefore, every element of $\mathbb{Z}_3[x]$ has the form $a + bx + (x^2+1)\cdot q(x)$.

Now suppose $f(x) \in \ker\phi$. Write

$$f(x) = a + bx + (x^2+1)\cdot q(x).$$

Then

$$0 = \phi(f) = \phi\left(a + bx + (x^2+1)\cdot q(x)\right) = a + bi + 0\cdot q(i) = a + bi.$$

It follows that $a = 0$ and $b = 0$, so $f(x) = (x^2+1)\cdot q(x) \in \langle x^2+1\rangle$. Therefore, $\ker\phi \subset \langle x^2+1\rangle$, so $\ker\phi = \langle x^2+1\rangle$.

By the First Isomorphism Theorem,

$$\frac{\mathbb{Z}_3[x]}{\langle x^2+1\rangle} = \frac{\mathbb{Z}_3[x]}{\ker\phi} \approx \operatorname{im}\phi = \mathbb{Z}_3[i]. \ \square$$

---

34. Show that if m and n are distinct positive integers, then $m\mathbb{Z}$ is not ring isomorphic to $n\mathbb{Z}$.

Suppose $\phi : m\mathbb{Z} \approx n\mathbb{Z}$. I'll show $m = n$.

Since ϕ is an isomorphism of the additive groups of $m\mathbb{Z}$ and $n\mathbb{Z}$, and since these additive groups are cyclic, ϕ must map a generator of $m\mathbb{Z}$ to $n\mathbb{Z}$. The generators of $m\mathbb{Z}$ are $\pm m$ and the generators of $n\mathbb{Z}$ are $\pm n$. Hence, $\phi(m) = n$ or $\phi(m) = -n$.

If $\phi(m) = n$, then since ϕ is a map of abelian groups,

$$\phi(m\cdot m) = m\cdot\phi(m) = mn.$$

But since ϕ is a ring map,

$$\phi(m \cdot m) = \phi(m) \cdot \phi(m) = n^2.$$

Therefore, $mn = n^2$, so $m = n$.
If $\phi(m) = -n$, then since ϕ is a map of abelian groups,

$$\phi(m \cdot m) = m \cdot \phi(m) = -mn.$$

But since ϕ is a ring map,

$$\phi(m \cdot m) = \phi(m) \cdot \phi(m) = n^2.$$

Therefore, $-mn = n^2$, so $-m = n$, a contradiction since m and n are *positive* integers.
Hence, the only possibility is $m = n$. □

[page 239]

1. Let $f(x) = 4x^3 + 2x^2 + x + 3$ and $g(x) = 3x^4 + 3x^3 + 3x^2 + x + 4$ where $f(x), g(x) \in \mathbb{Z}_5[x]$. Compute $f(x) + g(x)$ and $f(x) \cdot g(x)$.

$$f(x) + g(x) = 3x^4 + 2x^3 + 2x + 2.$$

$$f(x) \cdot g(x) = 2x^7 + 3x^6 + x^5 + 2x^4 + 3x^2 + 2x + 2. \ \square$$

---

12. Let $f(x) = 5x^4 + 3x^3 + 1$ and $g(x) = 3x^2 + 2x + 1$ in $\mathbb{Z}_7[x]$. Determine the quotient and remainder upon dividing $f(x)$ by $g(x)$.

$$5x^4 + 3x^3 + 1 = (4x^2 + 3x + 6) \cdot (3x^2 + 2x + 1) + (6x + 2). \ \square$$

---

17. Prove that the ideal $\langle x \rangle$ in $\mathbb{Z}[x]$ is prime but not maximal.

Define $\phi : \mathbb{Z}[x] \to \mathbb{Z}$ by

$$\phi(f) = f(0).$$

ϕ is a ring map; if $n \in \mathbb{Z}$, then $\phi(n) = n$, so ϕ is surjective.
Since $\phi(x) = 0$, $\langle x \rangle \subset \ker \phi$.
Suppose $\phi(f) = 0$. Then the constant term in $f(x)$ must be 0, so f is divisible by x: $f(x) \in \langle x \rangle$. Therefore, $\langle x \rangle = \ker \phi$.
By the First Isomorphism Theorem,

$$\frac{\mathbb{Z}[x]}{\langle x \rangle} = \frac{\mathbb{Z}[x]}{\ker \phi} \approx \operatorname{im} \phi = \mathbb{Z}.$$

Since $\mathbb{Z}$ is a domain, $\langle x \rangle$ is prime; since $\mathbb{Z}$ is not a field, $\langle x \rangle$ is not maximal. □

---

18. Prove that the ideal $\langle x \rangle$ in $\mathbb{Q}[x]$ is maximal.

Define $\phi : \mathbb{Q}[x] \to \mathbb{Q}$ by

$$\phi(f) = f(0).$$

By an argument similar to that given in Problem 17, ϕ induces an isomorphism

$$\frac{\mathbb{Q}[x]}{\langle x\rangle} = \frac{\mathbb{Q}[x]}{\ker\phi} \approx \operatorname{im}\phi = \mathbb{Q}.$$

Since $\mathbb{Q}$ is a field, $\langle x\rangle$ is maximal. $\square$

---

20. Let F be an infinite field and let $f(x), g(x) \in F[x]$. If $f(a) = g(a)$ for infinitely many elements a of F, show that $f(x) = g(x)$.

This is the same as showing that if $h(a) = 0$ for infinitely many elements a of F, then $h(x) = 0$.

Now $h(a) = 0$ implies that $x - a \mid h(x)$. By Corollary 3, page 238, $h(x)$ has at most $\deg h$ roots if $\deg h > 0$. Since h has infinitely many roots, $\deg h \leq 0$. $\deg h = 0$ implies h is a nonzero constant, which has no roots. Since this is ruled out, the only possibility is $h(x) = 0$. $\square$

---

30. Find infinitely many polynomials $f(x) \in \mathbb{Z}_3[x]$ such that $f(a) = 0$ for all a in $\mathbb{Z}_3$.

$x(x+1)(x+2)$ vanishes on $\mathbb{Z}_3$, so the same is true for $f(x) \cdot x(x+1)(x+2)$, where $f(x) \in \mathbb{Z}_3[x]$. $\square$