Math 308
3-8-1994

Solutions to Test 1.

If you want a problem regraded, *do not make any marks on or changes to your exam.* Write a note *on a separate piece of paper* and turn it back in with your test at the end of class. You must ask for any regrades at the time you receive your exam back.

1. (a) Find all ring maps from $\mathbb{Z}_{10}$ to $\mathbb{Z}_{30}$.

Let $\phi : \mathbb{Z}_{10} \to \mathbb{Z}_{30}$ be a ring map. ϕ is a group map of the additive groups; since $\mathbb{Z}_{10}$ is cyclic with generator 1, ϕ is determined by $\phi(1)$.

In $\mathbb{Z}_{10}$, $10 \cdot 1 = 0$, so $10 \cdot \phi(1) = 0$. Hence, the order of $\phi(1)$ divides 10, and the order of $\phi(1)$ can be 1, 2, 5, or 10.

Since $\phi(1) \in \mathbb{Z}_{30}$, the order of $\phi(1)$ divides 30. Hence, the order of $\phi(1)$ can be 1, 2, 3, 5, 6, 10, 15, or 30. Combining the two lists, I see that the order of $\phi(1)$ can be 1, 2, 5, or 10.

The only element of order 1 is 0. $\phi(1) = 0$ implies $\phi(x) = 0$ for all x. This is the zero map, which is always a ring map.

In what follows, I have to verify that certain maps are ring maps. I only need to check that $\phi(xy) = \phi(x)\phi(y)$, because the maps are already group maps by the discussion above. Note also that if ϕ is a ring map, then $\phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1)$ — and conversely, if the last equation does not hold, ϕ is not a ring map.

The only element of order 2 is 15. $\phi(1) = 15$ implies $\phi(x) = 15x \bmod 30$ for all x. ϕ is a ring map:

$$\phi(xy) = 15xy, \quad \phi(x)\phi(y) = (15x)(15y) = 225xy = 15xy.$$

The elements of order 5 are 6, 12, 18, 24.

$\phi(1) = 6$ gives $\phi(x) = 6x$ for all x. ϕ is a ring map:

$$\phi(xy) = 6xy, \quad \phi(x)\phi(y) = (6x)(6y) = 36xy = 6xy.$$

$\phi(1) = 12$ does not give a ring map:

$$\phi(1) = 12, \quad \text{but} \quad \phi(1)\phi(1) = 144 = 24.$$

$\phi(1) = 18$ does not give a ring map:

$$\phi(1) = 18, \quad \text{but} \quad \phi(1)\phi(1) = 324 = 24.$$

$\phi(1) = 24$ does not give a ring map:

$$\phi(1) = 24, \quad \text{but} \quad \phi(1)\phi(1) = 576 = 6.$$

The elements of order 10 are 3, 9, 21, and 27.

$\phi(1) = 3$ does not give a ring map:

$$\phi(1) = 3, \quad \text{but} \quad \phi(1)\phi(1) = 9.$$

$\phi(1) = 9$ does not give a ring map:

$$\phi(1) = 9, \quad \text{but} \quad \phi(1)\phi(1) = 81 = 21.$$

$\phi(1) = 21$ gives $\phi(x) = 21x$ for all x. ϕ is a ring map:

$$\phi(xy) = 21xy, \quad \phi(x)\phi(y) = (21x)(21y) = 441xy = 21xy.$$

$\phi(1) = 27$ does not give a ring map:

$$\phi(1) = 27, \quad \text{but} \quad \phi(1)\phi(1) = 729 = 9.$$

The ring maps from $\mathbb{Z}_{10}$ to $\mathbb{Z}_{30}$ are $\phi(x) = 0$, $\phi(x) = 6x$, $\phi(x) = 15x$, and $\phi(x) = 21x$. □

(b) Give an example of a commutative ring R and an ideal $I \subset R$ such that I is prime but not maximal.

$\dfrac{\mathbb{Z}[x]}{\langle x \rangle} \approx \mathbb{Z}$, which is a domain but not a field. Hence, $\langle x \rangle$ is a prime ideal, but is not maximal.

(You can show this directly: If $x \mid f(x)g(x)$, then $xp(x) = f(x)g(x)$, so $0 = 0 \cdot p(0) = f(0)g(0)$. Either $f(0) = 0$ and $x \mid f(x)$ or $g(0) = 0$ and $x \mid g(x)$. Hence, $\langle x \rangle$ is prime. It's not maximal, because it's properly contained in the proper ideal $\langle 2, x - 2 \rangle$.) □

---

2. (a) Let R be a domain. An element $r \in R$ is **prime** if $r \neq 0$, r is not a unit, and $r \mid xy$ implies $r \mid x$ or $r \mid y$. Prove that a prime element is irreducible.

Suppose r is prime, and let $r = xy$. Then $r \mid xy$, so $r \mid x$ or $r \mid y$. If $r \mid x$, then $x = ra$, so $r = ray$, $1 = ay$, and y is a unit. If $r \mid y$, then $y = rb$, so $r = rbx$, $1 = bx$, and x is a unit. Therefore, r is irreducible. □

(b) Find the general solution to the system of equations

$$\begin{array}{ccccccccccc} & & & & c & & & + & 2e & = & 3 \\ a & - & b & & & & & - & e & = & 1 \\ a & - & b & - & c & + & d & - & 2e & = & 2 \end{array}$$

Row reduce the coefficient matrix:

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 2 & 3 \\ 1 & -1 & 0 & 0 & -1 & 1 \\ 1 & -1 & -1 & 1 & -2 & 2 \end{bmatrix} \underset{r_1 \leftrightarrow r_2}{\longrightarrow} \begin{bmatrix} 1 & -1 & 0 & 0 & -1 & 1 \\ 0 & 0 & 1 & 0 & 2 & 3 \\ 1 & -1 & -1 & 1 & -2 & 2 \end{bmatrix} \underset{r_3 \to r_3 - r_1}{\longrightarrow}$$

$$\begin{bmatrix} 1 & -1 & 0 & 0 & -1 & 1 \\ 0 & 0 & 1 & 0 & 2 & 3 \\ 0 & 0 & -1 & 1 & -1 & 1 \end{bmatrix} \underset{r_3 \to r_3 + r_2}{\longrightarrow} \begin{bmatrix} 1 & -1 & 0 & 0 & -1 & 1 \\ 0 & 0 & 1 & 0 & 2 & 3 \\ 0 & 0 & 0 & 1 & 1 & 4 \end{bmatrix}$$

The equations are

$$\begin{array}{ccccccccc} a & - & b & & & - & e & = & 1 \\ & & & c & & + & 2e & = & 3 \\ & & & & d & + & e & = & 4 \end{array}$$

So the parametrized solution is

$$a = b + e + 1, \quad c = -2e + 3, \quad d = -e + 4. \ \square$$

---

3. (a) Give an example of a nonconstant polynomial with rational coefficients which has no roots in $\mathbb{Q}$ but is not irreducible over $\mathbb{Q}$.

$(x^2 + 1)^2$ has no rational roots, but is obviously reducible over $\mathbb{Q}$. □

(b) Prove or disprove: $y^4 - 4y^2 + 6y - 1$ is irreducible over $\mathbb{Q}$.

Method 1: Let $y = x + 1$. Then

$$y^4 - 4y^2 + 6y - 1 = x^4 + 4x^3 + 2x^2 + 2x + 2.$$

$x^4 + 4x^3 + 2x^2 + 2x + 2$ is irreducible by Eisenstein using the prime 2. Hence, the original polynomial is irreducible.

Method 2: Reduce mod 3 to obtain $y^4 + 2y^2 + 2$. By substitution, $y = 0$, $y = 1$, $y = 2$ are not roots, so $y^4 + 2y^2 + 2$ has no linear or cubic factors. If it factors, it must be the product of two quadratics.

Note that if a quadratic $2y^2 + ay + b$ is a factor, then $2 \cdot (2y^2 + ay + b) = y^2 + 2ay + 2b$ is also a factor (since $2^{-1} = 2$ in $\mathbb{Z}_3$). Therefore, I only need to consider quadratic factors of the form $y^2 + ay + b$. They are:

$$y^2, y^2 + 1, y^2 + 2, y^2 + y, y^2 + y + 1, y^2 + y + 2, y^2 + 2y, y^2 + 2y + 1, y^2 + 2y + 2.$$

y^2, $y^2 + y$, and $y^2 + 2y$ obviously have $y = 0$ as a root, but the quartic has no roots — so I can throw these out. $y^2 + 2$ amd $y^2 + y + 1$ have $y = 1$ as a root, and $y^2 + 2y + 1$ has $y = 2$ as a root. Throwing these out, I'm left with

$$y^2 + 1, y^2 + y + 2, y^2 + 2y + 2.$$

The product of the second and third has constant term $2 \cdot 2 = 1$, so $y^4 + 2y^2 + 2 \neq (y^2 + y + 2)(y^2 + 2y + 2)$. Finally,

$$(y^2 + 1)(y^2 + y + 2) = y^4 + y^3 + y + 2,$$

$$(y^2 + 1)(y^2 + 2y + 2) = y^4 + 2y^3 + 2y + 2.$$

Thus, $y^4 + 2y^2 + 2$ does not factor into a product of quadratics. It is irreducible mod 3, so it's irreducible over $\mathbb{Q}$. $\square$

---

4. Either prove that the set of vectors

$$\left\{ \begin{bmatrix} -1 \\ 2 \\ 4 \end{bmatrix}, \begin{bmatrix} -7 \\ 8 \\ 6 \end{bmatrix}, \begin{bmatrix} 2 \\ -1 \\ 3 \end{bmatrix} \right\}$$

is independent, or find a nontrivial linear combination of the vectors which adds up to the zero vector.

The set is dependent. Solve

$$a \cdot \begin{bmatrix} -1 \\ 2 \\ 4 \end{bmatrix} + b \cdot \begin{bmatrix} -7 \\ 8 \\ 6 \end{bmatrix} + c \cdot \begin{bmatrix} 2 \\ -1 \\ 3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

This amounts to doing the following row reduction:

$$\begin{bmatrix} -1 & -7 & 2 \\ 2 & 8 & -1 \\ 4 & 6 & 3 \end{bmatrix} \underset{r_1 \to -r_1}{\to} \begin{bmatrix} 1 & 7 & -2 \\ 2 & 8 & -1 \\ 4 & 6 & 3 \end{bmatrix} \underset{r_2 \to r_2 - 2r_1}{\to}$$

$$\begin{bmatrix} 1 & 7 & -2 \\ 0 & -6 & 3 \\ 4 & 6 & 3 \end{bmatrix} \underset{r_3 \to r_3 - 4r_1}{\to} \begin{bmatrix} 1 & 7 & -2 \\ 0 & -6 & 3 \\ 0 & -22 & 11 \end{bmatrix} \underset{r_2 \to -r_2/6}{\to}$$

$$\begin{bmatrix} 1 & 7 & -2 \\ 0 & 1 & -1/2 \\ 0 & -22 & 11 \end{bmatrix} \underset{r_3 \to r_3 + 22 r_2}{\to} \begin{bmatrix} 1 & 7 & -2 \\ 0 & 1 & -1/2 \\ 0 & 0 & 0 \end{bmatrix} \underset{r_1 \to r_1 - 7 r_2}{\to} \begin{bmatrix} 1 & 0 & 3/2 \\ 0 & 1 & -1/2 \\ 0 & 0 & 0 \end{bmatrix}$$

The parametrized solution is

$$a = -\frac{3}{2}c, \quad b = \frac{1}{2}c.$$

So (e.g.) setting $c = 2$, I get $a = -3$ and $b = 1$. Thus,

$$(-3) \cdot \begin{bmatrix} -1 \\ 2 \\ 4 \end{bmatrix} + \begin{bmatrix} -7 \\ 8 \\ 6 \end{bmatrix} + 2 \cdot \begin{bmatrix} 2 \\ -1 \\ 3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}. \ \Box$$

---

5. Let

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

$\mathbb{Q}[\sqrt{2}]$ is a subring of $\mathbb{R}$. (You may take this for granted.) Prove that

$$\frac{\mathbb{Q}[x]}{\langle x^2 - 2 \rangle} \approx \mathbb{Q}[\sqrt{2}].$$

Use this fact to prove that $\mathbb{Q}[\sqrt{2}]$ is a field.

Define $\phi : \mathbb{Q}[x] \to \mathbb{Q}[\sqrt{2}]$ by

$$\phi[f(x)] = f(\sqrt{2}).$$

ϕ is a ring map; ϕ is surjective, since

$$\phi(a + bx) = a + b\sqrt{2} \quad \text{for} \quad a, b \in \mathbb{Q}.$$

$\phi(x^2 - 2) = 2 - 2 = 0$, so $\langle x^2 - 2 \rangle \subset \ker \phi$. For the opposite inclusion, first observe that if $f(x) \in \mathbb{Q}[x]$, the Division Algorithm gives

$$f(x) = (x^2 - 2)q(x) + r(x).$$

Here $\deg r < \deg(x^2 - 2) = 2$, so $r(x) = a + bx$.

Now suppose $f \in \ker \phi$. Then with q and r as above,

$$0 = \phi(f) = f(\sqrt{2}) = 0 \cdot q(\sqrt{2}) + r(\sqrt{2}) = a + b\sqrt{2}.$$

Since $a, b \in \mathbb{Q}$, $a = b = 0$. This means $r(x) = a + bx = 0$, so $f(x) = (x^2 - 2)q(x) \in \langle x^2 - 2 \rangle$. It follows that $\ker \phi \subset \langle x^2 - 2 \rangle$, so in fact $\ker \phi = \langle x^2 - 2 \rangle$.

By the First Isomorphism Theorem,

$$\frac{\mathbb{Q}[x]}{\langle x^2 - 2 \rangle} = \frac{\mathbb{Q}[x]}{\ker \phi} \approx \operatorname{im} \phi \mathbb{Q}[\sqrt{2}].$$

Finally, $x^2 - 2$ is irreducible over $\mathbb{Q}$, so $\langle x^2 - 2 \rangle$ is maximal. Hence, $\dfrac{\mathbb{Q}[x]}{\langle x^2 - 2 \rangle}$ is a field, so $\mathbb{Q}[\sqrt{2}]$ is a field. $\Box$

"Perseverance is not a long race; it is many short races one after another." - Walter Elliot

