

Math 351 (Section 03)
Exam #2 Answer Key
November 2006

1. (20 points) Circle “True” if the statement is always true, “Possible” if the statement is true for some examples but false for others, or “False” if the statement is never true. **Then justify your choice!**

(a) Let R be a finite integral domain.

TRUE / **POSSIBLE** / **FALSE**: R has no irreducible elements.

All finite integral domains are fields. Since every element of a field is either zero or a unit, fields have no irreducible elements. (Remember that by definition irreducibles are non-zero non-units.)

(b) Let R be a unique factorization domain.

TRUE / **POSSIBLE** / **FALSE**: R is a Euclidean domain.

We know that every Euclidean domain is a PID, and every PID is a UFD. But the converses of these statements do not hold!

For example, \mathbb{Z} is both a Euclidean domain and a UFD. However, $\mathbb{Z}[x]$ is a UFD, but not a PID (and hence not a Euclidean domain).

(c) Let R be an integral domain, and let $p \in R$ such that (p) is a prime ideal of R .

TRUE / **POSSIBLE** / **FALSE**: p is a prime in R .

For example, (0) is a prime ideal in \mathbb{Z} , but primes are non-zero by definition. On the other hand, $(2) = 2\mathbb{Z}$ is a prime ideal in \mathbb{Z} and 2 is a prime.

In general, if p generates a prime ideal, we know that $(p) \neq R$. Thus p is not a unit. Also, if p divides ab for some $a, b \in R$. We have that $ab \in (p)$. Thus either $a \in (p)$ or $b \in (p)$. Therefore, either p divides a or p divides b .

So if p is not zero, then p is prime in R . However, 0 generates a prime ideal in every integral domain R .

(d) Consider the quotient ring $R = \mathbb{Z}[x]/(x^2 + 1)$.

TRUE / **POSSIBLE** / **FALSE**: R has the ascending chain condition.

R and $\mathbb{Z}[i]$ are isomorphic (use the map $\phi : \mathbb{Z}[x] \rightarrow \mathbb{Z}[i]$ defined by $\phi(f(x)) = f(i)$ and apply the first isomorphism theorem). Now since $\mathbb{Z}[i]$ is a Euclidean domain, it is also a PID and hence a UFD. Thus R is a unique factorization domain. We proved in class that every UFD has the ascending chain condition for principal ideals (actually since R is a PID, we have the ACC for *all* ideals).

(e) Let R be a finite integral domain.

TRUE / **POSSIBLE** / **FALSE**: The field of quotients of R is bigger than R .

Finite integral domains are fields. Let \mathbb{F} be the field of quotients of R . Since R is already a field, we have that $R \cong \mathbb{F}$. Thus they have the exact same size.

2. (12 points) Euclidean domains.

- (a) Give the definition of a “Euclidean domain”.

See the handout from class or your textbook.

- (b) Fix a non-negative integer
- c
- . Let
- R
- be a Euclidean domain such that
- $\delta(x) = c$
- for all
- $x \in R$
- ,
- $x \neq 0$
- . Prove that
- R
- is a field.

Suppose $x \in R$ and $x \neq 0$. To find an inverse for x we need to divide 1 by x . We know that there exists some $q, r \in R$ such that $1 = xq + r$ where either $r = 0$ or $\delta(r) < \delta(x)$. But notice that if $r \neq 0$, then $c = \delta(r) < \delta(x) = c$. This is impossible. Therefore, we must have that $r = 0$. Thus $1 = xq$. Therefore, $x^{-1} = q$. So R is a field.

A pointless note: Notice that the converse of this statement is also true. Suppose that \mathbb{F} is a field and δ makes it into a Euclidean domain. We proved in class that $\delta(x) = \delta(1)$ for all units x in our Euclidean domain. Thus since all non-zero elements are units we must have $\delta(x) = \delta(1)$ for all non-zero elements in \mathbb{F} . Thus δ is a constant function!

- (c) Let
- R
- be a Euclidean domain. Show that
- $\delta(x) \geq \delta(1)$
- for all nonzero
- $x \in R$
- .

Suppose that $x \in R$ and $x \neq 0$. Then $x = x1$. Therefore, $\delta(x) = \delta(x1) \geq \delta(1)$.

3. (10 points) An ideal question.

- (a) Is there a homomorphism whose domain is
- $\mathbb{Z}[x]$
- and kernel is
- $(x^2 - 4)$
- ? If so, find one. If not, explain why.

Yes. Use the projection homomorphism $\pi : \mathbb{Z}[x] \rightarrow \mathbb{Z}[x]/(x^2 - 4)$ defined by $\pi(f(x)) = f(x) + (x^2 - 4)$. The kernel of π is exactly $(x^2 - 4)$.

- (b) Is there a homomorphism whose domain is
- $M(\mathbb{R}) = \mathbb{R}^{2 \times 2}$
- and kernel is

$$D = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{R} \right\}?$$

If so, find one. If not, explain why.

No. D is not the kernel of any homomorphism because D is not an ideal of $\mathbb{R}^{2 \times 2}$. To see this notice that $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in D$, but $I_2 \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \notin D$.

4. (12 points) Fielding questions.

- (a) Construct a field with 9 elements.

Notice that if $R = \mathbb{Z}_3[x]/(f(x))$ where $f(x)$ has degree k , then $|R| = 3^k$. Thus to construct a field with 9 = 3^2 elements. We need to find an irreducible polynomial in $\mathbb{Z}_3[x]$ of degree 2.

Since there are only 9 monic polynomials of degree 2 in $\mathbb{Z}_3[x]$ and degree 2 polynomials are irreducible iff they have no roots, we can list all of the polynomials and start checking roots. Notice that $x^2 + 1$ is irreducible in $\mathbb{Z}_3[x]$. (There are two other irreducible monics of degree 2 in $\mathbb{Z}_3[x]$. Namely, $x^2 + x + 2$ and $x^2 + 2x + 2$.)

So we have that $\mathbb{Z}_3[x]/(x^2 + 1)$ is a field with 9 = 3^2 elements.

- (b) Consider
- $f(y) = y^3 + y \in \mathbb{Z}_3[y]$
- . Find all of the roots of
- $f(y)$
- in your field of 9 elements.

The field constructed in part (a) has the following elements: $[0], [1], [2], [x], [x + 1], [x + 2], [2x], [2x + 1]$, and $[2x + 2]$. Just start plugging these into $f(y)$ to find its roots.

Notice that $[0]^3 + [0] = [0]$, $[x]^3 + [x] = [x(x^2 + 1)] = [0]$, and $[2x]^3 + [2x] = [2x(x^2 + 1)] = [0]$. Thus the roots of $y^3 + y$ are $[0] = 0 + (x^2 + 1)$, $[x] = x + (x^2 + 1)$, and $[2x] = 2x + (x^2 + 1)$.

5. (12 points) Let $I = (x^2 - 4)$ be a principal ideal in $\mathbb{Q}[x]$.

(a) Is $x^2 + x + I$ a unit in $\mathbb{Q}[x]/I$? If not, explain why. If so, find its inverse.

$x^2 - 4 = (x + 2)(x - 2)$. But ± 2 are not roots of $x^2 + x$. Therefore, $x^2 + x$ and $x^2 - 4$ are relatively prime. So **YES**, $x^2 + x + I$ is a unit in $\mathbb{Q}[x]/I$.

Notice $x^2 + x = (x^2 - 4) + (x + 4)$. Thus $x^2 + x + I = x + 4 + I$. To find the inverse we need to find $u(x)$ and $v(x)$ so that $u(x)(x + 4) + v(x)(x^2 - 4) = 1$. We can accomplish this using the Euclidean algorithm for polynomials.

Dividing $x^2 - 4$ by $x + 4$ yields: $x^2 - 4 = (x - 4)(x + 4) + 12$. Thus

$$\frac{1}{12}(x^2 - 4) + \left(-\frac{1}{12}x + \frac{1}{3}\right)(x + 4) = 1. \text{ Therefore,}$$

$$(x^2 + x + I)^{-1} = (x + 4 + I)^{-1} = -\frac{1}{12}x + \frac{1}{3} + I.$$

(b) Does $\mathbb{Q}[x]/I$ have any zero divisors? If not, explain why. If so, find one.

Yes. $x^2 - 4 = (x + 2)(x - 2)$. Thus $(x + 2 + I)(x - 2 + I) = x^2 - 4 + I = 0 + I$. $x + 2 + I$ and $x - 2 + I$ are not equal to $0 + I$. Thus $x + 2 + I$ is a zero divisor in $\mathbb{Q}[x]/I$.

(c) I is not a maximal ideal of $\mathbb{Q}[x]$. Use part (b) to explain why. Also, find an ideal J of $\mathbb{Q}[x]$ so that $I \subsetneq J \subsetneq \mathbb{Q}[x]$.

We know that $\mathbb{Q}[x]$ is a Euclidean domain and thus a PID. In a PID, I is a maximal ideal iff $\mathbb{Q}[x]/I$ is a field. By part (b), $\mathbb{Q}[x]/I$ is not a field (it has zero divisors). Therefore, I cannot be maximal.

We can see I is not maximal directly by noticing that $J = (x + 2)$ properly contains $I = (x^2 - 4)$ yet $J \neq \mathbb{Q}[x]$.

6. (12 points) The Third Isomorphism Theorem – Let I and J be ideals of R where $J \subseteq I$.

(a) Show that I/J is an ideal of R/J directly (i.e. **Do not find a homomorphism whose kernel is I/J**).

Notice that $0 + J \in I/J$ since $0 \in I$. Thus it is non-empty. Suppose that $a + J, b + J \in I/J$, so $a, b \in I$. But I is an ideal, thus $a - b \in I$. Therefore, $(a + J) - (b + J) = (a - b) + J \in I/J$. Finally, consider $r + J \in R/J$. Then $(r + J)(a + J) = ra + J$ and $(a + J)(r + J) = ar + J$. But $r \in R$ and $a \in I$ imply that $ar, ra \in I$ since I is an ideal. Thus $(r + J)(a + J), (a + J)(r + J) \in I/J$. Therefore, I/J is an ideal of R/J .

(b) Oh horrors! A quotient of quotients!

Show that $(R/J)/(I/J)$ is isomorphic to R/I . *Hint:* Use the first isomorphism theorem.

Consider the map $\phi : R/J \rightarrow R/I$ defined by $\phi(a + J) = a + I$. First we must check that ϕ is well defined. Suppose that $a + J = b + J$. This implies that $a - b \in J \subseteq I$. Thus $a + I = b + I$. Hence, ϕ is well defined. Next, let $a + I \in R/I$ (so $a \in R$). Then $\phi(a + J) = a + I$. Therefore, ϕ is onto. Notice that $\phi((a + J) + (b + J)) = \phi((a + b) + J) = (a + b) + I = (a + I) + (b + I) = \phi(a + J) + \phi(b + J)$ and $\phi((a + J)(b + J)) = \phi(ab + J) = ab + I = (a + I)(b + I) = \phi(a + J)\phi(b + J)$. Thus ϕ is a homomorphism. Finally, suppose that $a + J$ is in the kernel of ϕ . So $\phi(a + J) = a + I = 0 + I$. Thus $a \in I$ which means that $a + J \in I/J$. Conversely, if $a + J \in I/J$, then $\phi(a + J) = a + I = 0 + I$ (since $a \in I$). Thus $a + J$ is in the kernel of ϕ . Thus $\text{Ker}(\phi) = I/J$. Now apply the first isomorphism theorem and get $(R/J)/(I/J) \cong R/I$.

7. (12 points) Isomorphic or not isomorphic?(a) Is $\mathbb{Z}[x]$ isomorphic to $\mathbb{Z}[i]$? Why or why not?

No. Notice that $\mathbb{Z}[x]$ is not a PID (the ideal $(x, 2)$ is not principal in $\mathbb{Z}[x]$) while $\mathbb{Z}[i]$ is a PID (since it's a Euclidean domain). Therefore, they cannot be isomorphic.

(b) Is $\mathbb{Q}[x]/(x+2)$ isomorphic to \mathbb{Q} ? Why or why not?

Yes. Consider the map $\phi : \mathbb{Q}[x] \rightarrow \mathbb{Q}$ defined by $\phi(f(x)) = f(-2)$. $\phi(f(x) + g(x)) = \phi((f+g)(x)) = (f+g)(-2) = f(-2) + g(-2) = \phi(f(x)) + \phi(g(x))$ and $\phi(f(x)g(x)) = \phi((fg)(x)) = (fg)(-2) = f(-2)g(-2) = \phi(f(x))\phi(g(x))$. Also, if $f(x) = c$, then $\phi(f(x)) = f(-2) = c$. Thus ϕ is a surjective homomorphism. Finally, $\phi(f(x)) = f(-2) = 0$ iff $x+2$ is a factor of $f(x)$ iff $f(x) \in (x+2)$. Thus the kernel of ϕ is $(x+2)$. Therefore, by the first isomorphism theorem $\mathbb{Q}[x]/(x+2) \cong \mathbb{Q}$.

(c) Is \mathbb{Z} isomorphic to $\mathbb{Q}[x]/(f(x))$ for some $f(x) \in \mathbb{Q}[x]$? Why or why not?

No. If $f(x) = 0$, then $\mathbb{Q}[x]/(0) \cong \mathbb{Q}[x]$. But $\mathbb{Q}[x]$ has infinitely many units and \mathbb{Z} has only two. If $f(x) \neq 0$, then we know that every element of $\mathbb{Q}[x]/(f(x))$ is either zero, a zero divisor, or a unit. Since \mathbb{Z} has many elements which are neither zero, zero divisors or units (for example 2, 3, ...), it is impossible for \mathbb{Z} to be isomorphic to $\mathbb{Q}[x]/(f(x))$.

8. (10 points) Fields of quotients.(a) Show that $\mathbb{Q}[\sqrt{-5}]$ is a field.

Notice that $\mathbb{Q}[\sqrt{-5}] \subseteq \mathbb{C}$. $1 = 1 + 0\sqrt{-5} \in \mathbb{Q}[\sqrt{-5}]$. Let $a + b\sqrt{-5}, c + d\sqrt{-5} \in \mathbb{Q}[\sqrt{-5}]$. Then $(a + b\sqrt{-5}) - (c + d\sqrt{-5}) = (a - c) + (b - d)\sqrt{-5} \in \mathbb{Q}[\sqrt{-5}]$. Finally, let $a + b\sqrt{-5}, c + d\sqrt{-5} \in \mathbb{Q}[\sqrt{-5}]$ with $c + d\sqrt{-5} \neq 0$. This implies that $c - d\sqrt{-5} \neq 0$. Therefore, since \mathbb{C} has no zero divisors, we have that $(c + d\sqrt{-5})(c - d\sqrt{-5}) = c^2 + 5d^2 \neq 0$. Now notice:

$$\frac{a + b\sqrt{-5}}{c + d\sqrt{-5}} \frac{c - d\sqrt{-5}}{c - d\sqrt{-5}} = \frac{(ac + 5bd) + (bc - ad)\sqrt{-5}}{c^2 + 5d^2} = \frac{(ac + 5bd)}{c^2 + 5d^2} + \frac{(bc - ad)}{c^2 + 5d^2}\sqrt{-5} \in \mathbb{Q}[\sqrt{-5}]$$

since $\frac{(ac + 5bd)}{c^2 + 5d^2}$ and $\frac{(bc - ad)}{c^2 + 5d^2}$ are rational (because $a, b, c,$ and d are rational).

Therefore, $\mathbb{Q}[\sqrt{-5}]$ is a subfield of \mathbb{C} (and thus it's a field).

(b) Prove that $\mathbb{Q}[\sqrt{-5}]$ is the field of quotients of $\mathbb{Z}[\sqrt{-5}]$.

Let \mathbb{F} be the field of quotients of $\mathbb{Z}[\sqrt{-5}]$.

We have shown that $\mathbb{Q}[\sqrt{-5}]$ is a field. Notice $\mathbb{Z}[\sqrt{-5}] \subseteq \mathbb{Q}[\sqrt{-5}]$. Thus $\mathbb{Q}[\sqrt{-5}]$ must contain a subfield (call it \mathbb{E}) which is isomorphic to \mathbb{F} .

Let $a + b\sqrt{-5} \in \mathbb{Q}[\sqrt{-5}]$. We know that $a = \frac{a_1}{a_2}$ where $a_1, a_2 \in \mathbb{Z}$ and $a_2 \neq 0$. Also,

$b = \frac{b_1}{b_2}$ where $b_1, b_2 \in \mathbb{Z}$ and $b_2 \neq 0$. Consider the following:

$$a + b\sqrt{-5} = \frac{a_1}{a_2} + \frac{b_1}{b_2}\sqrt{-5} = \frac{a_1b_2}{a_2b_2} + \frac{b_1a_2}{a_2b_2}\sqrt{-5} = \frac{1}{a_2b_2} ((a_1b_2) + (b_1a_2)\sqrt{-5})$$

$a_2b_2 \in \mathbb{Z} \subseteq \mathbb{Z}[\sqrt{-5}]$ and $(a_1b_2) + (b_1a_2)\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$. Thus $(a_2b_2)^{-1} \in \mathbb{E}$ and thus $a + b\sqrt{-5} = (a_2b_2)^{-1}((a_1b_2) + (b_1a_2)\sqrt{-5}) \in \mathbb{E}$.

Therefore, $\mathbb{Q}[\sqrt{-5}] \subseteq \mathbb{E}$. Thus $\mathbb{Q}[\sqrt{-5}] = \mathbb{E} \cong \mathbb{F}$.