

# Math 415B Midterm 2 Practice Problems (Posted)

Max von Hippel

April 15, 2019

## Question 1

Let  $R, S$  be commutative unital rings and  $\phi : R \rightarrow S$  an *onto* ring homomorphism. Let  $I \triangleleft S$  be an ideal.

(a) NTS  $I$  prime in  $S \implies \phi^{-1}(I)$  prime in  $R$ .

*Proof.* Assume  $I$  is a prime ideal in  $S$ . If  $\phi^{-1}(I) = R$  then as  $R$  is unital  $1_R \in R = \phi^{-1}(I)$  so as  $\phi$  is a homomorphism  $\phi(1_R) = 1_S \in I$  but then  $I = S$  contradicting our assumption of primality. So,  $\phi^{-1}(I) \subsetneq R$ .

Let  $a, b \in \phi^{-1}(I)$  arbitrarily; then as  $\phi$  is a homomorphism  $\phi(a - b) = \phi(a) - \phi(b) \in I$  since  $I$  is an ideal containing  $\phi(a), \phi(b)$ . Let  $r \in R$  arbitrarily; then as  $\phi$  is a homomorphism,  $\phi(ra) = \phi(r)\phi(a) \in I$  since  $\phi(r) \in S$  and  $\phi(a) \in I$  and  $I$  is an ideal in  $S$ . By commutativity and the preceding logic we conclude  $\phi^{-1}(I)$  is a proper ideal of  $R$ .

Let  $h, j \in R$  be such that  $hj \in \phi^{-1}(I)$ . Then as  $\phi$  is a homomorphism,  $\phi(hj) = \phi(h)\phi(j) \in I$ ; but then as  $I$  is prime  $\phi(h) \in I$  or  $\phi(j) \in I$ , so  $\phi^{-1}(\phi(h)) \subseteq \phi^{-1}(I)$  or  $\phi^{-1}(\phi(j)) \subseteq \phi^{-1}(I)$ , so  $h \in \phi^{-1}(I)$  or  $j \in \phi^{-1}(I)$ . But  $h, j$  were arbitrary so, combined with the fact that  $\phi^{-1}(I)$  is a proper ideal of  $R$ , we conclude that  $\phi^{-1}(I)$  is a prime ideal of  $R$  and we are done.  $\square$

(b) NTS  $I$  maximal in  $S \implies \phi^{-1}(I)$  maximal in  $R$ .

*Proof.* Assume  $I$  is a maximal ideal in  $S$ . Consider the natural homomorphism  $\sigma : R \rightarrow S/I$  defined by  $r \mapsto \phi(r) + I$ . By the First Isomorphism Theorem for Rings:

$$R/\text{Ker}(\sigma) = R/\phi^{-1}(I) \cong \sigma(R)$$

Clearly:

$$\sigma(R) = \phi(R)/I$$

So then:

$$R/\phi^{-1}(I) \cong \phi(R)/I$$

$\square$

## Question 2

Show that the homomorphic image of a PID is a PID

*Proof.* Assume that  $S$  is a PID,  $R$  is a ring, and  $\phi : S \rightarrow R$  is a homomorphism. Let  $I \triangleleft \phi(S)$  be an arbitrary ideal of  $\phi(S)$ . Then  $\phi^{-1}(I)$  is an ideal of  $S$ . But  $S$  is a PID, so we can express  $\phi^{-1}(I) = \langle i \rangle$  for some  $i \in \phi^{-1}(I)$ . So, for any  $j \in \phi^{-1}(I)$ , we have that  $j = ri$  for some  $r \in R$ . Then  $\phi(j) = \phi(r)\phi(i)$  where  $\phi(i) \in \phi(\phi^{-1}(I)) \subseteq I$ ; so  $\phi(\phi^{-1}(I)) = \langle \phi(i) \rangle$ . But  $\phi$  is onto, so  $\phi(\phi^{-1}(I)) = I$ , therefore  $I = \langle \phi(i) \rangle$ . So  $I$  is principal. But  $I$  was arbitrary so every ideal of  $\phi(R)$  is principal; hence as  $\phi, R, S$  were arbitrary (with only the restrictions that  $\phi$  be a homomorphism and  $S$  a PID) we conclude in general that the homomorphic image of a PID is a PID, and we are done.  $\square$

### Question 3

Show that the polynomial  $2X + 1 \in \mathbb{Z}_4[X]$  has a multiplicative inverse in  $\mathbb{Z}_4[X]$ .

*Proof.*

$$\begin{aligned}(2X + 1)(1 - 2X) &= (1 + 2X)(1 - 2X) = 1 - 4X^2 \\ 4 + 0 &= 4 = 0 \pmod{4} \implies -4 = 0 \in \mathbb{Z}_4[X] \\ \implies 1 - 4X^2 &= 1 + 0X^2 = 1 \in \mathbb{Z}_4[X] \implies (2X + 1)^{-1} = (1 - 2X) \in \mathbb{Z}_4[X]\end{aligned}$$

□

### Question 4

Prove that the ideal  $\langle X \rangle \subseteq \mathbb{Q}[X]$  is maximal.

*Proof.* Let  $a(X) + \langle X \rangle \in \mathbb{Q}[X] + \langle X \rangle$  arbitrarily. If  $\deg(a(X)) > 0$ , then we can set  $a(X) = a_m X^m + a_{m-1} X^{m-1} + \dots + a_1 X + a_0 = X(a_m X^{m-1} + a_{m-1} X^{m-2} + \dots + a_1) + a_0$  so  $a(X) + \langle X \rangle = a_0 + \langle X \rangle$ . So,  $\deg(a(X)) = 0$ . Then  $a(X) = a_0 \in \mathbb{Q}$  is just a rational constant. If it is non-zero, then it must be of the form  $a_0 = t_0/b_0$  for some  $t_0, b_0 \in \mathbb{Z} - \{0\}$ . Then it has the multiplicative inverse  $b_0/t_0$  in  $\mathbb{Q}$ , so:

$$(a_0 + \langle X \rangle)(\frac{b_0}{t_0} + \langle X \rangle) = a_0 \frac{b_0}{t_0} + \langle X \rangle = \frac{b_0}{a_0} \frac{a_0}{b_0} + \langle X \rangle = 1 + \langle X \rangle$$

Since  $1 \notin \langle X \rangle$  given that  $\deg(1) = 0 < \deg(X) = 1$  it follows that this must be the identity in  $\mathbb{Q}[X]/\langle X \rangle$ . So then  $a(X)^{-1} = (b_0/t_0)X^0$ , so  $a(X) \in U(\mathbb{Q}[X]/\langle X \rangle)$ , so  $U(\mathbb{Q}[X]/\langle X \rangle) = \mathbb{Q}[X]/\langle X \rangle$ . Moreover,  $X$  is irreducible and therefore  $\mathbb{Q}[X]/\langle X \rangle$  has no zero divisors. So then  $\mathbb{Q}[X]/\langle X \rangle$  is a ring in which every non-zero element is a unit and there are no zero divisors, so it's a field, so  $\langle X \rangle \subseteq \mathbb{Q}[X]$  is a maximal ideal of  $\mathbb{Q}[X]$  by Theorem 14.4 and we are done. □

### Question 5

Find a polynomial with integer coefficients that has  $1/2$  and  $-1/3$  as zeros.

*Proof.*

$$\begin{aligned}(X - \frac{1}{2})2(X + \frac{1}{3})3 &= (2X - 1)(3X + 1) = 6X^2 - 3X + 2X - 1 = 6X^2 - X - 1 \\ 6(\frac{1}{2})^2 - \frac{1}{2} - 1 &= \frac{6}{4} - \frac{2}{4} - 1 = \frac{4}{4} - 1 = 0 \\ 6(\frac{-1}{3})^2 - \frac{-1}{3} - 1 &= 6(\frac{1}{9}) + \frac{3}{9} - \frac{9}{9} = \frac{6+3-9}{9} = \frac{9-9}{9} = 0\end{aligned}$$

So  $f(X) = 6X^2 - X - 1$  solves the problem. □

### Question 6

Assume that an integer  $n > 0$  can be written in the form  $n = t^2 m$ . Show that  $tmX + 1$  is a unit in  $\mathbb{Z}_n[X]$ .

*Proof.* Let  $g(X) = (n - m)tX + 1$ . Then:

$$\begin{aligned}(tmX + 1)g(X) &= (tmX + 1)(ntX - mtX + 1) = t^2 nmX^2 - t^2 m^2 X^2 + tmX + ntX - mtX + 1 \\ &= 0 - 0 + tmX + 0 - mtX + 1 = 0 + 1 = 1\end{aligned}$$

So,  $tmX + 1$  has a multiplicative inverse in  $\mathbb{Z}_n[X]$  and is therefore a unit in  $\mathbb{Z}_n[X]$ , and we are done. □

## Question 7

**Suppose that  $f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in \mathbb{Z}[X]$ . If  $r \in \mathbb{Q}$  is a rational number such that  $X - r$  divides  $f(X)$  then show that  $r$  is an integer.**

*Proof.* Assume that  $r = t/b \in \mathbb{Q}$  is a rational number such that  $X - r \mid f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in \mathbb{Z}[X]$ . Then  $f(t/b) = 0$  if we evaluate in  $\mathbb{Q}[X]$ , so:

$$\left(\frac{t}{b}\right)^n + a_{n-1}\left(\frac{t}{b}\right)^{n-1} + \dots + a_1\frac{t}{b} + a_0 = 0$$

Multiplying both sides by  $b^n$ :

$$t^n + a_{n-1}t^{n-1}b + \dots + a_1tb^{n-1} + a_0b = 0$$

Moving terms around:

$$t^n = b(-a_{n-1}t^{n-1} - \dots - a_1tb^{n-2} - a_0)$$

Then we must have that  $b \mid t^n$ . If  $\gcd(b, t) \neq 1$  then we trivially have that  $t/b \in \mathbb{Z}$  so we assume the opposite; but then combining these statements we conclude  $b = \pm 1$  so  $t/b \in \{\pm t\} \subseteq \mathbb{Z}$  and we are done. So in all cases  $r$  is an integer when  $(X - r)$  divides  $f(X)$ .  $\square$

## Question 8

**Show that  $X^3 + X^2 + X + 1$  is reducible over  $\mathbb{Q}$ .**

*Proof.* Using the Reducibility Test for degrees 2, 3, I see that  $(-1)^3 + (-1)^2 + (-1) + 1 = -1 + 1 + -1 + 1 = 0 + 0 = 0$  so  $-1$  is a root so  $X^3 + X^2 + X + 1$  is reducible and we are done.  $\square$

**Does this fact contradict the statement that if  $p > 0$  is prime then the cyclotomic polynomial  $\phi_p$  is irreducible?**

*Proof.* No because it's not a cyclotomic polynomial.  $\square$

## Question 9

**Determine which of the polynomials in  $\mathbb{Q}[X]$  are irreducible over  $\mathbb{Q}$ .**

- (i)  $X^5 + 9X^4 + 12X^2 + 6$
  - (ii)  $X^4 + X + 1$
  - (iii)  $X^4 + 3X^2 + 3$
  - (iv)  $X^5 + 5X^2 + 1$
  - (v)  $\frac{5}{2}X^5 + \frac{9}{2}X^4 + 15X^3 + \frac{3}{7}X^2 + 6X + \frac{3}{14}$
- (i):

*Proof.* Notice that  $3 \mid 9, 3 \mid 12$ , but  $3 \nmid 1$  and  $3^2 \nmid 6$ . So by Eisenstein's Criterion, as  $3 > 0$  is prime, we conclude that this is irreducible.  $\square$

(ii):

*Proof.* Consider  $f(X) = X^4 + X + 1$ . We apply the Mod 2 Irreducibility Test. Since it has no zeros in  $\mathbb{Z}_2$ , it has no degree-1 factor in  $\mathbb{Z}_2$ . So if we can factor it into two polynomials of non-zero degree, they must each be of degree 2. Our choices for factors are  $X^2, X^2 + X, X^2 + 1, X^2 + X + 1$ . Long division shows that none of these divide  $f(X)$ . So,  $f(X)$  is irreducible in  $\mathbb{Z}_2[X]$ , and therefore irreducible in  $\mathbb{Q}[X]$ .  $\square$

(iii):

*Proof.* We can use the same trick to see that  $X^4 + 3X^2 + 3$  in mod 2 is literally just  $X^4 + X^2 + 1$  which is irreducible in mod 2, so  $X^4 + 3X^2 + 3$  is irreducible in mod 2, so  $X^4 + 3X^2 + 3$  is irreducible in  $\mathbb{Q}$  and we're done.  $\square$

(iv):

*Proof.*  $X^5 + 5X^2 + 1$  in mod 2 is  $X^5 + X^2 + 1$  which is the same as (iii) so and (ii) so by identical logic to (iii) this is also irreducible over  $\mathbb{Q}$ .  $\square$

(v):

*Proof.*

$$\begin{aligned} & \frac{5}{2}X^5 + \frac{9}{2}X^4 + 15X^3 + \frac{3}{7}X^2 + 6X + \frac{3}{14} \\ &= \frac{1}{14} \left( 35X^5 + 63X^4 + 6X^2 + 84X + 3 \right) \end{aligned}$$

In mod 2, this becomes:

$$\cong X^5 + X^4 + 0 + 0 + 1 = X^5 + X^4 + 1 = f(X)$$

Notice that  $1 + 1 + 1 = 3 \cong 1 \pmod{2}$ , and  $0 + 0 + 1 = 1 \cong 1 \pmod{2}$ , so this has no roots and therefore no linear factors in mod 2. So, any factorization must be of the form  $g(X)h(X)$  with  $(\deg(g(X)), \deg(h(X))) \in \{(3, 2), (2, 3)\}$ . Our possible choices of  $g(X), h(X)$ , considering they must include a constant 1, are  $X^3 + 1, X^3 + X^2 + 1, X^3 + X^2 + X + 1, X^3 + X + 1, X^2 + 1, X^2 + X + 1$ .

$X^3 + 1$  doesn't work because it has a zero at 1 whereas  $f(X)$  does not.

$X^3 + X^2 + 1$  doesn't work because when you long-divide it you get a remainder of **not checking this, hopefully non-zero**.

$X^3 + X^2 + X + 1$  doesn't work because it has a zero at 1 whereas  $f(X)$  does not.

$X^3 + X + 1$  doesn't work because when you long divide it you get a remainder of **not checking this, hopefully non-zero**.

$X^3 + X^2 + X + 1$  doesn't work because it has a zero at 1 whereas  $f(X)$  does not.

$X^3 + X + 1$  doesn't work because when you long divide it you get a remainder of **not checking this, hopefully non-zero**.

$X^2 + 1$  doesn't work because it has a zero at 1 whereas  $f(X)$  does not.

$X^2 + X + 1$  doesn't work because when you long divide it you get a remainder of **not checking this, hopefully non-zero**.  $\square$

## Question 10

**Assume  $d \in \mathbb{Z}$  is a square-free integer. Prove that the function  $N : \mathbb{Z}[\sqrt{d}] \rightarrow \mathbb{N}_0$  defined by  $N(a + b\sqrt{d}) = |a - db^2|$  satisfies the following conditions:**

- (i)  $N(z) = 0$  if and only if  $z = 0$
- (ii)  $N(zw) = N(z)N(w)$  for all  $z, w \in \mathbb{Z}[\sqrt{d}]$
- (iii)  $z \in \mathbb{Z}[\sqrt{d}]$  is a unit if and only if  $N(z) = 1$
- (iv) if  $N(z)$  is a prime integer then  $z$  is irreducible in  $\mathbb{Z}[\sqrt{d}]$
- (i):  $N(z) = 0$  if and only if  $z = 0$

*Proof.* **TODO**  $\square$

- (ii):  $N(zw) = N(z)N(w)$  for all  $z, w \in \mathbb{Z}[\sqrt{d}]$

*Proof.* **TODO**  $\square$

(iii):  $z \in \mathbb{Z}[\sqrt{d}]$  is a unit if and only if  $N(z) = 1$

*Proof.* **TODO**

□

(iv): if  $N(z)$  is a prime integer then  $z$  is irreducible in  $\mathbb{Z}[\sqrt{2}]$

*Proof.* **TODO**

□

## Question 11

Let  $R$  be a PID and let  $f \in R$ . Prove that  $\langle f \rangle$  is a maximal ideal in  $R$  if and only if  $f$  is irreducible.

*Proof.* **TODO**

□

## Question 12

Find  $q, r \in \mathbb{Z}[i]$  such that  $3 - 4i = (2 + 5i)q + r$  and  $d(r) < d(2 + 5i)$ .

*Proof.* **TODO**

□