

**Problem 1:**

Let  $R$  be a UFD and  $P$  be a prime ideal.

Let  $P$  fail to be principal. Let  $a \in P$ .

Now,  $a$  has a prime factorization,  $p_1^{\alpha_1} \dots p_n^{\alpha_n}$ .

Then one of the  $p_i^{\alpha_i}$  is in  $P$ ;  $a \in P$ , so  $p_1^{\alpha_1} \in P$  or  $p_2^{\alpha_2} \dots p_n^{\alpha_n} \in P$ . If  $p_2^{\alpha_2} \dots p_n^{\alpha_n} \in P$ , then  $p_2^{\alpha_2} \in P$  or  $p_3^{\alpha_3} \dots p_n^{\alpha_n} \in P$ . We can iterate this process, so one of the  $p_i^{\alpha_i}$  is in  $P$ .

So  $p_i \in P$ , by applying the same method.

So  $(p_i) \subset P$ . Because  $p_i$  is prime,  $(p_i)$  is prime (and nonzero). But it's not  $P$ , as  $P$  is not principal.

So  $P$  has a proper, nonzero prime ideal.

**Problem 2:**

Let  $k$  be a field and  $n \geq 2$ .

If  $\text{char}(k) = 2$ ,  $x_1^2 + x_2^2 \dots x_n^2 - 1$  is equal to  $(x_1 + x_2 + \dots + x_n - 1)^2$  (when you multiply it out, every term has a factor of 2 except the  $x_i^2$  and  $-1$  terms) and so  $x_1^2 + x_2^2 \dots x_n^2 - 1$  is reducible.

Now, if  $\text{char}(k) \neq 2$ , then  $x_1^2 + x_2^2 - 1$  is irreducible in  $k[x_1, x_2]$ ;  $x_1^2 + x_2^2 - 1$  is a monic polynomial of degree 2 in  $k[x_1][x_2] = k[x_1, x_2]$ . So if it factors, it factors into a product of degree 1 polynomials; so it factors into something of the form  $(x_2 + s)(x_2 + r)$ , with  $r$  and  $s$  both in  $k[x_1]$ . But the only way for this to happen is if  $s = -r$ . That is,  $1 - x_1^2$  must be a perfect square. However, its unique prime factorization is  $(x_1 + 1)(x_1 - 1)$ ; it is not a perfect square.

We proceed by induction:

Let  $x_1^2 + x_2^2 \dots x_{n-1}^2 - 1$  be irreducible in  $k[x_1, x_2 \dots x_{n-1}]$ , and set this equal to  $p$ . It is clear that  $x_n^2 + p$  is a monic polynomial of degree 2 in  $k[x_1, x_2 \dots x_{n-1}][x_n] = k[x_1, x_2 \dots x_n]$ . So if it factors, it factors into a product of degree 1 polynomials; so it factors into something of the form  $(x_n + s)(x_n + r)$ , with  $r$  and  $s$  both in  $k[x_1, x_2 \dots x_{n-1}]$ . But this would mean that  $p = rs$  for some  $r, s \in k[x_1, x_2 \dots x_{n-1}]$ , so  $p$  would be reducible.

So if  $x_1^2 + x_2^2 \dots x_{n-1}^2 - 1$  is irreducible in  $k[x_1, x_2 \dots x_{n-1}]$ , then  $x_1^2 + x_2^2 \dots x_n^2 - 1$  is irreducible in  $k[x_1, x_2 \dots x_n]$ .

So we have our result.

**Problem 3:**

By the reduction criterion,  $x^4 + 3x^3 + 3x^2 - 5$  is irreducible in  $\mathbb{Z}[x]$  if it is irreducible in  $\mathbb{Z}/(7)[x]$ .

Now, if  $x^4 + 3x^3 + 3x^2 - 5 = x^4 + 3x^3 + 3x^2 + 2$  is reducible, it either has a root or it can be written as a product of two monic order 2 polynomials.

But  $p(x) = x^4 + 3x^3 + 3x^2 + 2$  has no roots;

$$p(0) = 2$$

$$p(1) = 2$$

$$p(2) = 5$$

$$p(3) = 2$$

$$p(4) = 1$$

$$p(5) = 6$$

$$p(6) = 3$$

So if  $p$  is reducible, then  $p$  can be written as a product of two monic order 2 polynomials. That is,

$$\begin{aligned} x^4 + 3x^3 + 3x^2 + 2 &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + (a + c)x^3 + (b + d + ac)x^2 + (ad + bc)x + bd \end{aligned}$$

This means that

$$a + c = 3$$

$$b + d + ac = 3$$

$$ad + bc = 0$$

$$bd = 2$$

The first equation can be reduced to  $c = 3 - a$ , which yields

$$b + d + 3a - a^2 = 3 \quad (\alpha)$$

$$ad + 3b - ba = 0 \quad (\beta)$$

$$bd = 2 \quad (\gamma)$$

Now,  $(\gamma)$  only 6 solutions; we are working in a field, so for any given  $b$  there is a unique solution of that equation for  $d$ . Also,  $b = 0$  fails.

So we have that the only six valid solutions for  $b$  and  $d$  are:

$$b = 1, d = 2$$

$$b = 2, d = 1$$

$$b = 3, d = 3$$

$$b = 4, d = 4$$

$$b = 5, d = 6$$

$$b = 6, d = 5$$

The middle two fail, for any value of  $a$ ; because  $ad = ba$ ,  $(\beta)$  gives us  $3b = 0$ , which fails for any nonzero  $b$ . We are left with

$$b = 1, d = 2$$

$$b = 2, d = 1$$

$$b = 5, d = 6$$

$$b = 6, d = 5$$

A rearrangement of  $(\alpha)$  gives us  $a(3 - a) = 3 - b - d$ .

For the first two cases,  $b + d = 3$ , so we have that  $a = 3$  or  $a = 0$ . If  $a = 0$ , then  $(\beta)$  reduces to  $3b = 0$ , which fails for any nonzero  $b$ . If  $a = 3$ , then  $(\beta)$  reduces to  $3d = 0$  which fails for any nonzero  $d$ .

For the last two cases,  $b + d = 30 = 2$ . This means that  $(\alpha)$  gives us that  $a(3 - a) = 1$ . But this is unsatisfiable; if  $q = a(3 - a)$ , then:

$$q(0) = 0$$

$$q(1) = 2$$

$$q(2) = 2$$

$$q(3) = 0$$

$$q(4) = 3$$

$$q(5) = 4$$

$$q(6) = 3$$

That is, every possible solution for  $(\gamma)$  modulo 7 fails to satisfy the system of equations. That is, we cannot reduce  $x^4 + 3x^3 + 3x^2 + 2$  modulo 7.

So by the reduction criterion,  $x^4 + 3x^3 + 3x^2 - 5$  is irreducible in  $\mathbb{Z}[x]$ . So  $x^4 + 3x^3 + 3x^2 - 5$  is irreducible in  $\mathbb{Q}[x]$ .

**Problem 4:**

Let  $R = \mathbb{Z}[\sqrt{-5}]$ , and  $K = \text{Quot}(R)$ .

Consider  $3x^2 + 4x + 3$ . By the quadratic formula, if this polynomial has roots, they are  $\frac{-2}{3} \pm \frac{\sqrt{-5}}{3}$ . A factorization of  $3x^2 + 4x + 3$  is given by  $3(x + \frac{2}{3} + \frac{\sqrt{-5}}{3})(x + \frac{2}{3} - \frac{\sqrt{-5}}{3})$ . So the polynomial is reducible in  $K[x]$ .

Now, in  $R[x]$ ,  $3x^2 + 4x + 3$  cannot have a constant factored out of it. As it is a degree 2 polynomial, this means that it factors only as a product of two degree 1 polynomials. So any factorization of that polynomial must be of the form  $(rx + r'(2 + \sqrt{-5}))(sx + s'(2 - \sqrt{-5}))$ , with  $r', s' \in \mathbb{Z}[\sqrt{-5}]$  and  $r = 3r'$ ,  $s = 3s'$ . Yet, this means that the leading coefficient of the polynomial is a multiple of 9, which 3 isn't. So the polynomial is irreducible in  $R[x]$ .

**Problem 5:**

Note: I'm playing fast and loose with notation. I recognize this, but feel that it's still clear in context what is meant.

Let  $R$  be a UFD and  $P$  be a prime ideal of  $R[x]$  with  $P \cap R = 0$ . Define  $K = \text{quot}(R)$ .

We can view  $P$  as a subset of  $K[x]$ . Consider  $(P) \subset K[x]$ . We see that  $(P)$  is principal, as  $K[x]$  is a principal ideal domain. Moreover,  $(P)$  is not the entire ring, because  $P \cap R = 0$ . So  $(P) = (p)$  for some  $p \in K[x]$ , with  $p$  having degree at least 1.

We can impose that  $p \in P$ ; if it isn't, then we can multiply  $p$  by the least common multiple of the quotients of the coefficients of  $p$  to get it in  $R[x]$ . Also,  $R[x] \cap (P) = P$ ; if  $x \in (P) \cap R[x]$  and, then there's a nonzero  $r \in R$  such that  $rx \in P$ , but  $r \notin P$ , so  $x \in P$ . (Also,  $P \subset R[x]$  and  $P \subset (P)$ ).

Further, we can impose that the leading coefficient of  $p$  divides the leading coefficient of any element of  $P$ .

This means that  $p$  must be prime in  $R[x]$ ; let  $r, s \in R[x]$  with  $rs = p$ . One of  $r$  or  $s$  must have degree at least one, then. Then  $rs \in P$ .

Now, we imposed that  $p \in P$ , so  $(p) \subset P$ .

Next, let  $q \in P$ . Then  $q \in (P) \subset K[x]$ , so  $q \in (p) \subset K[x]$ . That means

that  $p \mid q$  in  $K[x]$ ; there is an  $r \in K[x]$  such that  $q = pr$ . By multiplying by the least common multiple of the quotients of the coefficients of  $r$ , we can say that there is a  $k \in R$  such that  $kq = pr'$  for some  $r' \in R[x]$ . That is,  $kq \in (p)$  for some  $k \in R$ . But  $(p)$  is prime, and  $(p) \subset P$ . So  $k \notin (p)$ , so  $q \in (p)$ .

So  $(p) = P$ ;  $P$  is a principal ideal.