

## Solutions to Homework #21

1. Saracino, Section 20, Problem 20.1. Let  $p$  be a prime. Prove that  $\mathbb{F}_p[X]/\langle X^2 + 1 \rangle$  is a field if and only if the equation  $x^2 \equiv -1 \pmod{p}$  has no solution (modulo  $p$ ).

**Proof.** Let  $f = X^2 + 1 \in \mathbb{F}_p[X]$ .

( $\implies$ ): Since  $\mathbb{F}_p[X]/\langle f \rangle$  is a field, we have that  $\langle f \rangle$  is a maximal ideal in  $\mathbb{F}_p[X]$ , by Theorem 17.7. By Theorem 20.2,  $f$  is irreducible in  $\mathbb{F}_p[X]$ . By Theorem 19.8,  $f$  has no roots in  $\mathbb{F}_p$ . That is, there are no elements  $x \in \mathbb{F}_p$  such that  $x^2 + 1 = 0$ . Equivalently, there are no solutions in  $\mathbb{Z}$  to the equation  $x^2 \equiv -1 \pmod{p}$ .

( $\impliedby$ ): There are no solutions in  $\mathbb{Z}$  to the equation  $x^2 \equiv -1 \pmod{p}$ , and hence there are no elements  $x \in \mathbb{F}_p$  such that  $x^2 + 1 = 0$ . Since  $\deg(f) = 2$ , Theorem 19.8 says that  $f$  is irreducible in  $\mathbb{F}_p[X]$ . Therefore, by Theorem 20.2,  $\langle f \rangle$  is a maximal ideal in  $\mathbb{F}_p[X]$ . Hence, by Theorem 17.7,  $\mathbb{F}_p[X]/\langle f \rangle$  is a field. QED

2. Saracino, Section 20, Problem 20.4. Let  $K = \{0, 1, \alpha, \alpha + 1\}$  be the four-element field constructed in Example 1 of Section 20 (pages 206–207), where I have written  $\alpha$  for the element Saracino denotes  $\bar{X}$ . Write the polynomial  $X^2 + X + 1$  as a product of factors of degree 1 in  $K[X]$ .

**Solution.** We have  $\alpha^2 + \alpha + 1 = 0$  in  $K$ , so [since  $-1 = 1$  in both  $\mathbb{F}_2$  and  $K$ ], we also have  $\alpha^2 + \alpha = 1$ , and hence  $\alpha(\alpha + 1) = 1$ .

Thus,  $X^2 + X + 1 = (X + \alpha)(X + \alpha + 1)$ , and we are done.

“Wait, what?” I hear you cry. Remember,  $K = \mathbb{F}_2[X]/I$ , where  $I = \langle X^2 + X + 1 \rangle$ . So every element of  $K$  is a coset of the form  $I + f$  for some  $f \in \mathbb{F}_2[X]$ . When we write  $0 \in K$ , we mean the coset  $I + 0$ ; similarly  $1 \in K$  really means the coset  $I + 1$ . Meanwhile,  $\alpha = \bar{X} \in K$  is shorthand for the coset  $I + X$ , and  $\alpha + 1 = \bar{X} + 1 \in K$  is shorthand for the coset  $I + X + 1$ .

In particular,  $\alpha^2$  means  $(I + X)(I + X) = I + X^2 = I - (X + 1) = I + X + 1$ , where the second equality is by the coset relation (since  $X^2 + X + 1 \in I$ ), and the third is because  $-1 = 1$  in  $\mathbb{F}_2$ . Thus,  $\alpha^2 = \alpha + 1$ . So we have  $\alpha + (\alpha + 1) = 2\alpha + 1 = 1$ , and  $\alpha(\alpha + 1) = \alpha^2 + \alpha = (\alpha + 1) + \alpha = 2\alpha + 1 = 1$ , where we’re again using the fact that  $2 = 0$  in  $\mathbb{F}_2$  and hence also in  $K$ . Thus,  $X^2 + X + 1 = (X + \alpha)(X + \alpha + 1)$ .

3. Saracino, Section 20, variant of Problem 20.7(a). Construct a field of 8 elements.

**Solution.** Let  $f = X^3 + X + 1 \in \mathbb{F}_2[X]$ . Then  $f(0) = 1 \neq 0$  and  $f(1) = 1 \neq 0$ , so  $f$  has no roots in  $\mathbb{F}_2$ . Since  $f$  is cubic, Theorem 19.8 says that  $f$  is irreducible.

Thus,  $I = \langle f \rangle$  is a maximal ideal in  $\mathbb{F}_2[X]$  (Theorem 20.2). Define  $K = \mathbb{F}_2[X]/I$ , which is a field by Theorem 17.7. It remains to show that  $|K| = 8$ .

We claim that  $K = \{I + a_0 + a_1X + a_2X^2 \mid a_i \in \mathbb{F}_2\}$ . The reverse inclusion ( $\supseteq$ ) is clear. For the forward inclusion, given  $I + g \in K$ , by the division algorithm there are polynomials  $q, r \in \mathbb{F}_2[X]$  with  $\deg(r) < 3$  and  $g = qf + r$ . Thus,  $g - r = qf \in I$ . Meanwhile, we may write  $r = a_0 + a_1X + a_2X^2$  with  $a_i \in \mathbb{F}_2$ . Hence,  $I + g = I + r \in \text{RHS}$ , proving the claim.

In addition, if  $I + a_0 + a_1X + a_2X^2 = I + b_0 + b_1X + b_2X^2$ , then  $(a_0 - b_0) + (a_1 - b_1)X + (a_2 - b_2)X^2 \in I$  is a multiple of  $f$  and hence is of the form  $qf$  for some  $q \in \mathbb{F}_2[X]$ . If  $q \neq 0$ , then  $\deg q \geq 0$ , and hence  $\deg(qf) \geq \deg f = 3$ ; but the explicit polynomial above is of degree at most 2, giving a contradiction. Thus,  $q = 0$ , and hence the above polynomial is zero, i.e.,  $a_i = b_i$  for each  $i = 0, 1, 2$ .

Thus, each element of  $K$  may be written *uniquely* as  $I + a_0 + a_1X + a_2X^2$ . Hence,  $K$  has exactly  $2^3 = 8$  elements, since there are two choices for each  $a_i \in \mathbb{F}_2$ . QED

**Note:** Instead of  $X^3 + X + 1$ , we could have instead used the polynomial  $X^3 + X^2 + 1$  for  $f$ . These are the only two irreducible polynomials of degree 3 in  $\mathbb{F}_2[X]$ . (Can you prove that?)

---

4. Saracino, Section 20, Problem 20.7(b). Construct a field of 9 elements.

**Solution.** Let  $f = X^2 + 1 \in \mathbb{F}_3[X]$ . Then  $f(0) = 1 \neq 0$  and  $f(1) = f(2) = 2 \neq 0$ , so  $f$  has no roots in  $\mathbb{F}_3$ . Let  $I = \langle f \rangle$  and let  $K = \mathbb{F}_3[X]/\langle I \rangle$ . By Problem 1 (Saracino problem 20.1), we have that  $K$  is a field. It remains to show that  $|K| = 9$ .

We claim that  $K = \{I + a_0 + a_1X \mid a_i \in \mathbb{F}_3\}$ . The reverse inclusion ( $\supseteq$ ) is clear. For the forward inclusion, given  $I + g \in K$ , by the division algorithm there are polynomials  $q, r \in \mathbb{F}_2[X]$  with  $\deg(r) < 2$  and  $g = qf + r$ . Thus,  $g - r = qf \in I$ . Meanwhile, we may write  $r = a_0 + a_1X$  with  $a_i \in \mathbb{F}_3$ . Hence,  $I + g = I + r \in \text{RHS}$ , proving the claim.

In addition, if  $I + a_0 + a_1X = I + b_0 + b_1X$ , then  $(a_0 - b_0) + (a_1 - b_1)X \in I$  is a multiple of  $f$  and hence is of the form  $qf$  for some  $q \in \mathbb{F}_2[X]$ . If  $q \neq 0$ , then  $\deg q \geq 0$ , and hence  $\deg(qf) \geq \deg f = 2$ ; but the explicit polynomial above is of degree at most 1, giving a contradiction. Thus,  $q = 0$ , and hence the above polynomial is zero, i.e.,  $a_i = b_i$  for each  $i = 0, 1$ .

Thus, each element of  $K$  may be written *uniquely* as  $I + a_0 + a_1X$ . Hence,  $K$  has exactly  $3^2$  elements, since there are three choices for each  $a_i \in \mathbb{F}_3$ . QED

---

**Note:** Instead of  $X^2 + 1$ , we could have instead used any of the polynomials  $2X^2 + 2$ ,  $X^2 + X + 2$ ,  $2X^2 + 2X + 1$ ,  $X^2 + 2X + 2$ , or  $2X^2 + 1X + 1$  for  $f$ . These are the only six irreducible polynomials of degree 2 in  $\mathbb{F}_3[X]$ . (Can you prove that?)