NAP PROBLEM SET #1, SOLUTIONS

ROGER AND SYLVIA WIEGAND

1. We follow the procedure in section 1.8 of the book. Also, we will use "-1" instead of "2" (since coefficients are in $\mathbb{F}_3$).

Using the division algorithm thrice, we get

$$\begin{gathered} X^5 + X + 1 = (X^2 - X - 1)(X^3 + X^2 - X - 1) + (X^2 - X) \\ X^3 + X^2 - X - 1 = (X - 1)(X^2 - X) + (X - 1) \\ X^2 - X = X(X - 1) + 0 \end{gathered}$$

The GCD is the last non-zero remainder, namely $X - 1$. Using the first equation, we express $X^2 - X$ in terms of $\alpha =^{\text{def}} X^3 + X^2 - X - 1$ and $\beta =^{\text{def}} X^5 + X + 1$:

eq1.1

$$X^2 - X = -(X^2 - X - 1)\alpha + \beta\,. \tag{0.1}$$

Now use the second equation to express $X - 1$ in terms of $X^2 - X$ and α, plug in the expression for $X^2 - X$ from (0.1), and combine terms, getting the equation

$$X - 1 = (X^3 + X^2 - 1)\alpha + (-X + 1)\beta\,.$$

(Of course it would be a good idea to check this last equation.) □

2. Neither 1 nor -1 is a root of $f(X) = X^4 - 10X^2 + 1$, so by Proposition 1.11 $f(X)$ has no linear factors. Thus we assume that $f(X) = g(X)h(X)$, where $g(X)$ and $h(x)$ are quadratic polynomials in $\mathbb{Q}[X]$, and we seek a contradiction. Letting c be the leading coefficient of $g(X)$, and replacing $g(X)$ and $h(X)$ by $c^{-1}g(X)$ and $ch(X)$ respectively, we may assume that both $g(X)$ and $h(X)$ are monic. Moreover, by Proposition 1.14, both $g(X)$ and $h(X)$ are in $\mathbb{Z}[X]$. (One could also use Proposition 1.13 (Gauss's Lemma) to get to this point.)

Write $g(X) = X^2 + aX + b$ and $h(X) = X^2 + cX + d$. Comparing constant terms in the expression

$$X^4 - 10X^2 + 1 = (X^2 + aX + b)(X^2 + cX + d)\,,$$

we have

eq2.1

$$b = d = \pm 1\,. \tag{0.2}$$

Comparing coefficients of X^3, we see that $0 = a + c$, that is,

eq2.2

$$c = -a\,. \tag{0.3}$$

Comparing coefficients of X^2, we find that $-10 = b + ac + d$; combining this with (0.3), we have

eq2.3

$$a^2 = b + d + 10\,. \tag{0.4}$$

Now we combine (0.4) with (0.2), getting either

$$a^2 = 12 \qquad \text{or} \qquad a^2 = 8\,,$$

the desired contradiction. □

3. Let's prove uniqueness first. Since $\hat{\varphi}(c) = \varphi(c)$ for each $c \in R$ and $\hat{\varphi}(X) = \alpha$, and since $\hat{\varphi}$ is required to be a ring homomorphism, it follows that

eq3.1

$$\hat{\varphi}(a_m X^m + \cdots + a_1 X + a_0) = \varphi(a_m)\alpha^m + \cdots + \varphi(a_1)\alpha + \varphi(a_0)\,. \tag{0.5}$$

Thus, for each $f(X) \in R[X]$, we have an explicit formula for $\hat{\varphi}(f(X))$, and this proves uniqueness. To complete the proof, we just have to show that the map

Date: 17 May, 2016.

$\hat{\varphi} : R[X] \to S$ given by (0.5) is a homomorphism. It's tempting to say that this is obvious, but let's try to give a proof.

We have $\hat{\varphi}(1_{R[X]}) = \varphi(1_R) = 1_S$. (The first equality is from the formula (0.5), and the second holds because φ is assumed to be a ring homomorphism.) Now we have to show that $\hat{\varphi}$ preserves addition and multiplication. Suppose $f(X) = g(X) + h(X)$ in $R[X]$. We want to show that $\hat{\varphi}(f(X)) = \hat{\varphi}(g(X)) + \hat{\varphi}(h(X))$. Write $g(X) = b_m X^m + \cdots + b_0$ and $h(X) = c_m X^m + \cdots + c_0$. (If $g(X)$ and $h(X)$ don't have the same degree, we just add on some zero terms to one or the other.) Now

$$f(X) = (b_m + c_m)X^m + \cdots + (b_0 + c_0)\,,$$

and by (0.5) we have $\hat{\varphi}(f(X)) = \varphi(b_m + c_m)\alpha^m + \cdots + \varphi(b_0 + c_0)$. Since φ is a homomorphism, the right-hand side of this equation is

$$\begin{aligned} (\varphi(b_m) + \varphi(c_m))\alpha^m + \cdots + (\varphi(b_0) + \varphi(c_0)) = \\ (\varphi(b_m)\alpha^m + \cdots + \varphi(b_0)) + (\varphi(c_m)\alpha^m + \cdots + \varphi(c_0)) = \\ \hat{\varphi}(g(X)) + \hat{\varphi}(h(X))\,. \end{aligned}$$

As for multiplication, an easy and similarly dreary computation shows that

$$\hat{\varphi}(ch(X)) = \hat{\varphi}(c)\hat{\varphi}(h(X)) \qquad \text{and} \qquad \hat{\varphi}(Xh(X)) = \hat{\varphi}(X)\hat{\varphi}(h(X))\,,$$

for all $c \in R$ and $h(X) \in R[X]$. Thus $\hat{\varphi}$ respects addition, multiplication by constants, and multiplication by X. Since multiplication by any $g(X) \in R[X]$ can be accomplished by repeatedly using these three operations, we see that $\hat{\varphi}$ preserves multiplication. □

4. Let $G = \langle x \rangle$, and write $g = x^m$ and $h = x^n$, where m and n are non-negative integers. If m is even, say, $m = 2\ell$, then $g = (x^\ell)^2$, contrary to our assumption. Thus m is odd, and similarly n is odd. Therefore $m + n$ is even, say, $m + n = 2q$. Now we have

$$gh = x^m x^n = x^{m+n} = x^{2q} = (x^q)^2\,.$$

This shows that gh is a square. (Note that the proof did not use the hypothesis that $|G|$ is even. The result is *vacuously* true if $|G|$ is odd, since in that case *every* element of G is a square.)

5 a): If $X^4 + X^2 + 1$ is not irreducible, we obtain, exactly as in the solution of Problem 2, a factorization

$$X^4 + X^2 + 1 = (X^2 + aX + b)(X^2 + cX + d)\,,$$

where $a, b, c, d \in \mathbb{Z}$. Comparing coefficients, we obtain (0.2) and (0.3) as well as the followig variant of (0.4):

$$a^2 = b + d - 1\,.$$

From (0.2), we see that $b = d = 1$ and $a^2 = 1$. Thus either $a = -c = 1$ or $a = -c = -1$. We learn nothing new from comparing coefficients of X. Hmm, it is beginning to look as if the polynomial is reducible, and, indeed, we have

$$X^4 + X^2 + 1 = (X^2 + X + 1)(X^2 - X + 1)\,.$$

The factors are both irreducible since they have no rational roots. (This shows that the skeptical approach, trying to prove irreducibility, can sometimes lead to a factorization. Whoo hoo!) □

5 b) The approach in Problems 2 and 5 a) would work, but for variety we can use Eisenstein. Make the substitution $X = Y + 1$. We have

$$g(Y) =^{\mathrm{def}} (Y + 1)^4 + 1 = Y^4 + 4Y^3 + 6Y^2 + 4Y + 2\,.$$

Using Eisenstein with $p = 2$, we conclude that $g(Y)$ is irreducible in $\mathbb{Q}[Y]$. Why does this imply that $f(X) =^{\mathrm{def}} X^4 + 1$ is irreducible? Well, if $f(X) = h(X)k(X)$ were a non-trivial factorization, we would have

$$g(Y) = (Y + 1)^4 + 1 = f(Y + 1) = h(Y + 1)k(Y + 1)\,,$$

contradicting irreducibility of $g(Y)$. □

5 c) $X^5 - 1 = (X - 1)(X^4 + X^3 + X^2 + X + 1)$. The first factor is irreducible, and the second one is too, by Problem 5 e).

5 d) This problem turned out to be *much* harder than we had intended. It will be very interesting to see if any of you got it by an easier method than we found. Anyway, to do penance for our carelessness, we will present a solution.

If $f(X) = X^9 + X^3 + 1$ is not irreducible, then there is a factorization

$$X^9 + X^3 + 1 = g(X)(h(X),$$

where $g(X), h(X) \in \mathbb{Z}[x]$ and both have degrees between 1 and 8.

Then in $\mathbb{F}_2$, $\overline{X^9 + X^3 + 1} = \overline{g(X)(h(X)}$, where $1 \le \deg(g), \deg(h) \le 8$.

We make some observations about irreducible polynomials in $\mathbb{F}_2[X]$:

1. The only irreducible polynomials of degrees ≤ 3 are:

$$X, X + 1, X^2 + X + 1, X^3 + X^2 + 1, X^3 + X + 1.$$

2. $\overline{f(X)}$ has no roots in $\mathbb{F}_2$ and so it has no linear factors. Moreover, in $\mathbb{F}_2[X]$,

$$X^9 + X^3 + 1 = (X^2 + X + 1)(X^7 + X^6 + X^4 + X^3) + 1,$$
$$X^9 + X^3 + 1 = (X^3 + X^2 + 1)(X^6 + X^5 + X^4 + X^2 + 1)$$
$$X^9 + X^3 + 1 = (X^3 + X + 1)(X^6 + X^4 + X^3 + X^2 + 1) + (X^2 + X)$$
$$(X^6 + X^5 + X^4 + X^2 + 1) = (X^3 + X^2 + 1)(X^3 + X^2 + 1) + 1$$

That is, $f(X)$ can be factored in $\mathbb{F}_2$ but only in one way, as a product of the degree 3 and degree 6 polynomials shown, which are irreducible. The polynomial $X^6 + X^5 + X^4 + X^2 + 1$ is irreducible in $\mathbb{F}_2[X]$, because if not it would have an irreducible factor of degree ≤ 3 in $\mathbb{F}_2[X]$. It has no roots in $\mathbb{F}_2$, since $f(X)$ doesn't and it is a factor of $f(X)$. Similarly, it has no irreducible factor of degree 2, and also doesn't have the factors $X^3 + X^2 + 1$ or $X^3 + X + 1$.

By the equation above, that

$$X^9 + X^3 + 1 = g(X)h(X) \implies \overline{X^9 + X^3 + 1} = \overline{g(X)(h(X)},$$

we have that deg $g = 3$, deg $h = 6$.

We may assume that g, h are monic and have integer coefficients by Gauss's Lemma and arguments from class. Also we may suppose that

$$\overline{g(X)} = X^3 + X + 1 \quad \text{and} \quad \overline{h(X)} = X^6 + X^5 + X^4 + X^2 + 1,$$

where the polynomials are in $\mathbb{F}_2[X]$. Write

$$g(X) = X^3 + aX^2 + bX + c, \quad h(X) = X^6 + e_5X^5 + e_4X^4 + e_3X^3 + e_2X^2 + e_1X + e_0.$$

If we require that $f(X) = g(X)h(X)$, we see immediately that $a \equiv 1 \pmod 2, b \equiv 0 \pmod 2$, and $c = e_0 = 1$ or $c = e_0 = -1$.

For convenience, we separate into two cases: Case i: $c = e_0 = 1$, and Case ii: $c = e_0 = -1$.

In case i, we are looking at Equation 0.6:

eq5.d.1 (0.6) $X^9+X^3+1 = (X^3+aX^2+bX+1)(X^6+e_5X^5+e_4X^4+e_3X^3+e_2X^2+e_1X+1)$

We proceed by matching up coefficients of powers of X in the product from Equation 0.6:

X^8 term: $0 = e_5 + a \implies \boxed{e_5 = -a}$.

X^7 term: $0 = e_4 + ae_5 + b \implies e_4 = -ae_5 - b = a^2 - b \implies \boxed{e_4 = a^2 - b}$.

X term: $0 = b + e_1 \implies \boxed{e_1 = -b}$.

X^2 term: $0 = a + be_1 + e_2 \implies e_2 = -a - be_1 = b^2 - a \implies \boxed{e_2 = b^2 - a}$.

X^3 term: $1 = 1 + ae_1 + be_2 + e_3 \implies e_3 = -ae_1 - be_2 = -a(-b) - b(b^2 - a) \implies \boxed{e_3 = 2ab - b^3}$.

Now rewrite Equation 0.6:

eq5.d.2 (0.7)
$X^9+X^3+1 = (X^3+aX^2+bX+1)(X^6-aX^5+(a^2-b)X^4+(2ab-b^3)X^3+(b^2-a)X^2-bX+1)$

Now we equate the other powers of X:

X^6 term: $0 = 2ab - b^3 + a^3 - ab - ab + 1 = -b^3 + a^3 + 1 \implies \boxed{b^3 = a^3 + 1}$.

Since a, b are integers, the only possibilities are $\boxed{a = -1, b = 0}$ or $\boxed{a = 0, b = 1}$.

The solution $a = 0, b = 1$ does not fit the requirements that $a \equiv 1 \pmod 2$, so we discard that.

X^4 term: $0 = -b + a(b^2 - a) + b(2ab - b^3) + a^2 - b$.

If we put $a = -1, b = 0$ into the last equation we have that $0 = 0 + (-1)(1) + 0 + 1$. No contradiction yet.

X^5 term: $0 = -b^2 - a + a(2ab - b^3) + b(a^2 - b) - a$.

If we put $a = -1, b = 0$ into this equation we have that $0 = 0 + 1 + 0 + 0 + 1$, a contradiction.

Therefore, in case i, there is no such factorization.

In case ii, we do a similar analysis and use that $a \equiv 1 \pmod 2, b \equiv 0 \pmod 2$. I am tired of typing, but I can show you if you'd like.

The upshot is that the polynomial is irreducible. Whew!! This is almost (but not quite) enough to make us try to learn to use PARI or some other computer algebra program!

5 e). As in the solution to 5 b), we substitute $X = Y + 1$. Let

$$f(X) = X^4 + X^3 + X^2 + X + 1 = \frac{X^5 - 1}{X - 1}\,.$$

Let

$$g(Y) = f(Y+1) = \frac{(Y+1)^5 - 1}{Y + 1 - 1} = \frac{Y^5 + 5Y^4 + 10Y^3 + 10Y^2 + 5Y}{Y} =$$
$$Y^4 + 5Y^3 + 10Y^2 + 10Y + 5\,.$$

Eisenstein implies that $g(Y)$ is irreducible, and the argument in 5b) shows that $f(X)$ is too. □