Math 71 Homework Solutions

292/1 (c) $\varphi : \mathbb{Q} \to \mathbb{Q}$ ring homo $\varphi(1) = k$ some $k \in \mathbb{Q}$.

$\therefore \varphi(n) = nk \,,\; n \in \mathbb{Z}$

$4k^2 = \varphi(2)\varphi(2) = \varphi(4) = 4k \quad \therefore k^2 = k$ so

$k(k-1) = 0 \quad \therefore k = 0$ or 1. $k=0$ does not give an isom. Suppose $k=1$. $\varphi(n) = n \quad \forall n \in \mathbb{Z}$.

Consider $p/q \in \mathbb{Q} \qquad p = q\,(p/q)$

$\therefore \; p = \varphi(p) = \varphi(q\,(p/q)) = q\,\varphi(p/q)$

$\therefore \varphi(p/q) = p/q. \qquad \therefore \varphi = id$, the identity homo

301/1 Let $I = (f(x))$, $\overline{g(x)} = g(x) + I$

$g(x) = q(x)\,f(x) + r(x)$, $r(x) = 0$ or $\deg r < \deg f = n$

$g(x) - r(x) = q(x)\,f(x) \in I \qquad \therefore \overline{g(x)} = r(x) + I$

Let $g_0(x) = r(x)$ so $\overline{g(x)} = \overline{g_0(x)}$. Now show $r(x)$ unique. Suppose $s(x) \in F[x]$ $\deg s \le n-1$

and $\overline{g}(x) = \overline{s(x)} \;\therefore\; \overline{r(x)} = \overline{s(x)}$ so $r(x) - s(x) \in I$

$= (f(x))$ $\therefore r(x) - s(x)$ is a multiple of $f(x)$

$\deg r(x) - s(x) \le n-1$, $\deg f = n$. $\therefore r(x) - s(x) = 0$

$\therefore r(x) = s(x)$

301/8 By long division, $x^3 - 2 = (x^2 - x + 1)(x+1) + (-3)$

$x+1 = -3\left(-\frac{x}{3} - \frac{1}{3}\right)$

By the euclidean algorithm -3 is a gcd. But -3 is a unit. $\therefore 1$ is the gcd.

$x^3 - 2 = (x^2 - x + 1)(x+1) + (-3)$

Divide by (-3) to find A, B such that $A(x^3-2) + B(x+1) = 1$

306/3 R is subring: if $f(x)$ and $g(x)$ have no x term, the same is true for $f(x) + g(x)$ and $f(x)g(x)$ (show this)

Now suppose $x^2 = f(x)\,g(x)$, $f(x), g(x) \in R$.

$\frac{311}{9}$ If $x^2-\sqrt{2}$ ured / $\mathbb{Z}[\sqrt{2}]$, $\exists$ $a+b\sqrt{2}$ $\in \mathbb{Z}[\sqrt{2}]$, $a,b\in\mathbb{Z}$ such that $(a+b\sqrt{2})^2=\sqrt{2}$. $\therefore$ $a^2+2b^2=0$ and $2ab=1$. There are no a,b satisfying this.

$\frac{312}{14}$ Just do x^8-1 (a) $x^8-1=(x^2-1)(x^2+1)(x^4+1)=(x-1)(x+1)(x^2+1)(x^4+1)$. Know x^2+1 irred. What about x^4+1. This has no real roots, $\therefore$ no linear factors. What about $x^4+1=(x^2+ax+1)(x^2+bx+1)$. This gives $a+b=0$ and $2+ab=0$. A similar argument for $(x^2+ax-1)(x^2+bx-1)$. Therefore above we have factored x^8-1 into irreducibles.

(b) The factorization above holds for $\mathbb{Z}_2$ but x^2+1 and x^4+1 may not be irred. / $\mathbb{Z}_2$ $x^2+1=(x+1)(x+1)$

$x^4+1=(x^2+1)(x^2+1)=(x+1)^4$ $\therefore$ x^8-1 $(=x^8+1)=(x+1)^8$

(c) Does x^2+1 have a root in $\mathbb{Z}_3$? no. $\therefore$ irred.

Does x^4+1 have a root in $\mathbb{Z}_3$ no. $\therefore$ no linear factors. But can this factorization occur ~~in~~/ $\mathbb{Z}_3$:

$$x^4+1=(x^2+ax+b)(x^2+cx+d)$$

$a,b,c,d\in\mathbb{Z}_3$ You decide.

$\frac{312}{16}$ $f(x)=a_0+a_1x+a_nx^n$. $f(\frac{1}{x})=a_0+\frac{a_1}{x}+\cdots+\frac{a_n}{x^n}$

$g(x)=x^nf(\frac{1}{x})=a_n+a_{n-1}x+\quad+a_1x^{n-1}+a_0x^n$

If $g(x)=b_0+b_1x+\quad+b_nx^n$, $b_i=a_{n-i}$

Show $f(x)$ irred $\Rightarrow g(x)$ irred: Suppose $g(x)=h(x)k(x)$, $\deg h=r$, $\deg k=s$, $r,s<n$. Then $x^nf(\frac{1}{x})=h(x)k(x)$. Replace x by $\frac{1}{x}$, $\frac{1}{x^n}f(x)=h(\frac{1}{x})k(\frac{1}{x})$. Multiply by x^n

$f(x)=(x^rh(\frac{1}{x}))(x^sk(\frac{1}{x}))$ contradicting irreducibility of $f(x)$ $\therefore$ $g(x)$ irred. For the opposite implication note that f is the reverse of g, so from what was just proved g irred $\Rightarrow f$ irred.

Since there are no polynomials of degree 1, $\deg f = 2$ and $\deg g = 0$ (or other way around) $\therefore g(x)$ is a unit $\therefore x^2$ is irreducible. A similar argument for x^3

$\therefore x^6 = x^2 x^2 x^2 = x^3 x^3$ $\quad$ R not UFD

$\frac{3 \| }{3}$ Let $h(x) = (x-1)(x-2)\cdots(x-n)-1$, $h(i) = -1$ for $i = 1, 2, .., n$ Suppose $h(x) = f(x)g(x)$, $\deg f = p$, $\deg g = q$

$f(i) = 1$ or -1 for $i = 1, .., n$ Suppose $f(i) = 1$ for r values of i $\therefore g(i) = -1$ for these values of i and $f(i) = -1$ for s values of i $(r+s = n)$ and $g(i) = 1$ for these s values of i.

$f(x) - 1$ is a polynomial of degree p with r roots $\therefore r \le p$ Similarly $g(x)+1$ has r roots, $r \le q$

Also ~~...~~, $s \le p$, $s \le q$. If $r < p$

$n = r+s < p+q = n$ impossible $\therefore r = p$

Similarly $s = q$. Also

$p = r \le q$ and $q = s \le p$ so $p = q$ and $\therefore r = s$

Conclusion n even $= 2k$ $\quad f, g$ polynomials degree k

$f(x) - 1$ has k roots among $1, .., n$

$g(x) - 1$ has k roots among remaining $1, .., n$

$\therefore (f(x)-1)(g(x)-1)$ has roots $1, 2, .., n$.

$\therefore (f(x)-1)(g(x)-1) = (x-1)(x-2)\cdots(x-n)$

$\therefore f(x)g(x) - f(x) - g(x) + 1 = h(x) + 1$

$\therefore f(x) + g(x) = 0$ $\qquad \therefore g(x) = -f(x)$

$\therefore h(x) = f(x)g(x) = -f(x)^2$

Now compare constant terms: $(2k)! - 1 = -a_0^2$ where a_0 is constant term of $f(x)$. Impossible since LHS > 0 and RHS ≤ 0.

Does anyone have a shorter proof?