SOLUTIONS TO LECTURE 27 PROBLEMS 109 – 114

P109 # 28 from pg. 292 Gallian

Let F be a field and $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in F[x]$
PROVE $x-1$ is factor of $f(x) \iff a_n + a_{n-1} + \cdots + a_0 = 0$

Observe, given $f(x)$ as above,

$$f(1) = a_n 1^n + a_{n-1} 1^{n-1} + \cdots + a_0 = a_n + a_{n-1} + \cdots + a_0$$

Thus, by Factor Th$^{\underline{m}}$ (aka Coro. 2 on pg. 288), $f(1) = 0$ iff $(x-1) \mid f(x)$ which means $a_n + a_{n-1} + \cdots + a_0 = 0$ iff $(x-1)$ is factor of $f(x)$.

P110 # 38 from p. 292 Gallian

Let R be commutative ring with unity. If I is a prime ideal of R then prove $I[x]$ is prime ideal of $R[x]$

Suppose $a, b \in R$ and $ab \in I \Rightarrow a \in I$ or $b \in I$ where I is an ideal of the commutative ring with unity R.
Consider $f(x), g(x) \in R[x]$ where $f(x) g(x) \in I(x)$. In particular, $f(x) = a_n x^n + \cdots + a_0$ and $g(x) = b_m x^m + \cdots + b_0$ where $a_i, b_j \in R$ and let $c_0, c_1, .., c_{n+m} \in I$ where

$$f(x)\, g(x) = (a_n x^n + \cdots + a_0)(b_m x^m + \cdots + b_0)$$
$$= \underbrace{a_n b_m}_{c_{n+m}} x^{n+m} + \cdots + \underbrace{a_0 b_0}_{c_0} \qquad \text{generally } c_k = \sum_{l=0}^{k} a_l b_{k-l}$$

we know $c_0, c_1, .., c_{n+m} \in I$ as $f(x) g(x) \in I(x)$.
Since I prime, $a_0 b_0 \in I \Rightarrow a_0 \in I$ or $b_0 \in I$.
For $c_1 = a_0 b_1 + a_1 b_0$ if $a_0 \in I$ then $a_0 b_1 \in I \Rightarrow c_1 - a_0 b_1 \in I$ thus $a_1 b_0 = c_1 - a_0 b_1 \in I \Rightarrow a_1 \in I$ or $b_0 \in I$. Also, if $b_0 \in I$ then $a_1 b_0 \in I$ hence $c_1 - a_1 b_0 = a_0 b_1 \in I$ thus $a_0 \in I$ or $b_1 \in I$
Thus, either $a_0 b_0$ has both a_0 and $b_0 \in I$ or $a_0 + a_1 x \in I[x]$ or $b_0 + b_1 x \in I[x]$.

P110 continued

Suppose I is a prime ideal of a commutative ring with unity R. It follows R/I is an integral domain. The natural homomorphism $\pi : R \longrightarrow R/I$ defined by $\pi(r) = r + I$ induces a natural homomorphism of $R[x]$ and $(R/I)[x]$ by mapping the coefficients from R to the corresponding cosets in R/I. Explicitly, $\psi : R[x] \longrightarrow (R/I)[x]$

$$\psi(a_0 + a_1x + \cdots + a_nx^n) = (a_0 + I) + (a_1 + I)x + \cdots + (a_n + I)x^n$$

it is not difficult to prove ψ is a homomorphism of rings, we can express $\psi\left(\sum_{j=0}^{n} a_j x^j\right) = \sum_{j=0}^{n} (a_j + I)x^j$. Additivity,

$$\begin{aligned}\psi\left(\sum_{j=0}^{\infty} a_j x^j + \sum_{j=0}^{\infty} b_j x^j\right) &= \psi\left(\sum_{j=0}^{\infty} (a_j + b_j)x^j\right) \\ &= \sum_{j=0}^{\infty} (a_j + b_j + I)x^j \\ &= \sum_{j=0}^{\infty} (a_j + I)x^j + \sum_{j=0}^{\infty} (b_j + I)x^j \\ &= \psi\left(\sum_{j=0}^{\infty} a_j x^j\right) + \psi\left(\sum_{j=0}^{\infty} b_j x^j\right).\end{aligned}$$

Likewise, $\psi(f(x)\,g(x)) = \psi(f(x))\,\psi(g(x))$ can be shown.

Note, $\mathrm{Ker}(\psi) = \{a_0 + \cdots + a_nx^n \in R[x] \mid a_0 + I + \cdots + (a_n + I)x^n = 0\}$ but, $a_0 + I + \cdots + (a_n + I)x^n = 0 \Rightarrow a_0, a_1, \ldots, a_n \in I$ hence $\mathrm{Ker}(\psi) = I(x)$. Also, note $a_0 + I + (a_1 + I)x + \cdots + (a_n + I)x^n$ is mapped to by $\psi(a_0 + a_1x + \cdots + a_nx^n)$ $\therefore$ ψ is surjective. By 1st isomorphism Thm, $R[x]/I[x] \approx (R/I)[x]$. Notice, R/I is int. domain $\Rightarrow (R/I)[x]$ is int. domain $\Rightarrow \dfrac{R[x]}{I[x]}$ int. domain. Therefore, we find $I[x]$ is prime ideal.

P111 Gallian # 39 p. 292

Let F be a field and $f(x), g(x) \in F[x]$.
If $\nexists$ polynomial of positive degree that divides both $f(x)$ and $g(x)$ then prove $\exists\, h(x), k(x) \in F[x]$ for which
$f(x)h(x) + g(x)k(x) = 1$ (such $f(x), g(x)$ are <u>relatively prime</u>)

Construct $I = \langle f(x), g(x) \rangle = \{ a(x)f(x) + b(x)g(x) \mid a(x), b(x) \in F[x] \}$

it is clear I forms an ideal of $F[x]$ and since

$F[x]$ is a PID it follows $I = \langle j(x) \rangle = \{ j(x)\ell(x) \mid \ell(x) \in F[x] \}$

notice $\underbrace{a(x)}_{1} f(x) + \underbrace{b(x)}_{0} g(x) = f(x) = \ell(x) j(x) \Rightarrow j(x) \mid f(x)$.

likewise $g(x) = 0 \cdot f(x) + 1 \cdot g(x) = \ell(x) j(x) \Rightarrow j(x) \mid g(x)$.

Hence the generator of I divides both $f(x)$ and $g(x)$
As $\nexists\, j(x) \in F[x]$ with $\deg(j(x)) \geq 1$ with $j(x) \mid f(x), g(x)$
we find $j(x) = c$ thus $\langle c \rangle = \langle f(x), g(x) \rangle$
if $c = 0$ then $f(x) = 0$ and $g(x) = 0$ which $\rightarrow\!\leftarrow$ the
non existence of divisors of positive degree. Hence $c \neq 0$

and $\langle c \rangle = I$ thus,

$$c = a(x)f(x) + b(x)g(x) \quad \text{for some } a(x), b(x) \in F[x]$$

$$\Rightarrow 1 = \left(\frac{a(x)}{c}\right) f(x) + \left(\frac{b(x)}{c}\right) g(x)$$

Let $h(x) = \frac{1}{c} a(x)$ and $k(x) = \frac{1}{c} b(x)$ to see we have established the existence of $h(x), k(x) \in F[x]$ for which $h(x)f(x) + g(x)k(x) = 1$.

P112 # 8 of p. 308 of Gallian

Construct a field of order 27

Strategy, find irred. over $\mathbb{Z}_3$ order 3 $P(x)$ for which $\frac{\mathbb{Z}_3[x]}{\langle P(x)\rangle}$ is field.

Let $P(x) = x^3 + 2x + 2$ notice $P(0) = 2$, $P(1) = 2$, $P(2) = 2$ modulo 3 hence $x^3 + 2x + 2 \in \mathbb{Z}_3[x]$ is irreducible over $\mathbb{Z}_3$.

Consequently, $\mathbb{Z}_3[x]/\langle x^3+2x+2\rangle = \{ a+bx+cx^2 + \langle x^3+2x+2\rangle \mid a,b,c \in \mathbb{Z}_3\}$ forms a field with 27 elements.

P113 # 10 of p. 308 of Gallian

Determine which polynomials below are irred. over $\mathbb{Q}$

(a.) $x^5 + 9x^4 + 12x^2 + 6$ is irred. by Eisenstein's Criterion with $P=3$ as $3 \mid 9$, $3 \mid 12$, $3 \mid 6$ but $3^2 \nmid 6$. (irred. over $\mathbb{Q}$ to be clear)

(b.) $x^4 + x + 1 = f(x)$ gives $\overline{f(x)} \in \mathbb{Z}_2[x]$ for which $\overline{f(0)} = 1$ and $\overline{f(1)} = 1$ thus $\overline{f(x)}$ is irreducible over $\mathbb{Z}_2$ hence $f(x)$ irred over $\mathbb{Q}$.

(c.) $x^4 + 3x^2 + 3$ is irred. over $\mathbb{Q}$ by $P=3$ application of Eisenstein.

(d.) $x^5 + 5x^2 + 1$ provides $\overline{f(x)} = x^5 + x^2 + 1$ in $\mathbb{Z}_2[x]$ and as $\overline{f(0)} = 1$ and $\overline{f(1)} = 1+1+1 = 1$ we find $\overline{f(x)}$ irred. over $\mathbb{Z}_2$ thus $x^5 + 5x^2 + 1$ is irred. over $\mathbb{Q}$

(e.) $f(x) = \frac{5}{2}x^5 + \frac{9}{2}x^4 + 15x^3 + \frac{3}{7}x^2 + 6x + \frac{3}{14}$

$\Rightarrow 14f(x) = 35x^5 + 63x^4 + 210x^3 + 6x^2 + 84x + 3$

note $3 \mid 63$, $3 \mid 210$, $3 \mid 6$, $3 \mid 84$, $3 \mid 3$ and $9 \nmid 3$ Thus $14f(x)$ irred. over $\mathbb{Q}$

If $f(x) = f_1(x)f_2(x) \Rightarrow 14f(x) = 14f_1(x)f_2(x) \Rightarrow$ $f(x)$ also irred. over $\mathbb{Q}$.

P114 Gallian # 29 of p. 309

We wish to show x^4+1 is reducible over $\mathbb{Z}_p$ for any prime p.
It turns out in $\mathbb{Z}_p$ we have a sol$^{\underline{n}}$ to

i.) $a^2 = -1$
ii.) $a^2 = 2$
iii) $a^2 = -2$

and in each case we may reduce x^4+1 in view of such an element.

i.) $a^2 = -1 \Rightarrow x^4+1 = x^4 - a^2 = (x^2-a)(x+a)$

ii.) $a^2 = 2 \Rightarrow x^4+1 = \underbrace{(x^2+ax+1)(x^2-ax+1)}_{\text{from Gallian's key. Let's check on this claim,}}$

$$\begin{aligned}(x^2+ax+1)(x^2-ax+1) &= x^4 + x^3(-a+a) + x^2(1-a^2+1) + x(a-a)+1 \\ &= x^4 + x^2(2-a^2)+1 \\ &= x^4+1.\end{aligned}$$

iii.) $$\begin{aligned}(x^2+ax-1)(x^2-ax-1) &= x^4+x^3(-a+a)+x^2(-1-a^2-1)+x(-a+a)+1 \\ &= x^4+x^2(-a^2-2)+1 \\ &= x^4+1\end{aligned}$$ given $a^2=-2$.

Thus, if we can show $\exists\, a \in \mathbb{Z}_p$ for which $a^2=-1$, $a^2=2$, $a^2=-2$ for any prime p then we find x^4+1 reduces according to the factorizations shown above. It remains to show such $a \in \mathbb{Z}_p$ exist for any prime p.

P114 continued

Consider $\varphi : \mathbb{Z}_p^{\times} \longrightarrow \mathbb{Z}_p^{\times}$ defined by $\varphi(x) = x^2 \quad \forall x \in \mathbb{Z}_p^{\times} = \mathbb{Z}_p - \{0\}$.

Observe $\varphi(xy) = (xy)^2 = x^2y^2 = \varphi(x)\varphi(y)$ thus φ is a homomorphism of the multiplicative group $\mathbb{Z}_p^{\times}$. Moreover,

$$\mathrm{Ker}\,\varphi = \{x \in \mathbb{Z}_p^{\times} \mid \varphi(x) = x^2 = 1\}$$

$$\mathrm{Ker}\,\varphi = \{1, -1\}$$

If $p > 2$ then $|\mathrm{Ker}\,\varphi| = 2$. Let $H = \varphi(\mathbb{Z}_p^{\times})$ and note $\mathbb{Z}_p^{\times}/\mathrm{Ker}\,\varphi \approx H$ hence

$$\frac{\mathbb{Z}_p^{\times}}{H} \approx \frac{\mathbb{Z}_p^{\times}}{\mathbb{Z}_p^{\times}/\mathrm{Ker}\,\varphi} \approx \mathrm{Ker}\,\varphi \qquad \text{(fun with quotients!)}$$

thus $\mathbb{Z}_p^{\times}/H$ has two elements H and xH for some $x \notin H$.

① If $-1, 2 \notin H$ then $-H = 2H$ and since $\mathbb{Z}_p^{\times}/H \approx \{-1, 1\}$ the non-identity element squares to give identity

$$(-H)(-H) = H \quad \text{and} \quad (2H)(2H) = H$$

Also, $(-H)(-H) = (-H)(2H) = -2H = H \therefore -2 \in H. \Rightarrow \exists a \in \mathbb{Z}_p$ for which $\underline{a^2 = -2}$.

② If $-1, 2 \in H$ then $\exists a \in \mathbb{Z}_p$ s.t. $\underline{a^2 = -1}$ and $\underline{a^2 = 2}$

Finally, $p = 2$ we treat separately, $x^4 + 1 = x^4 - 1 = (x^2+1)(x^2-1)$.