Homework 6 Solutions

Ch 16: 25, 27, 35, 37, 57, 58, 63, 64 - 66 (these are all related), 67, 68

25. If $x-2$ is a factor of $p(x) = x^4 - 2x - 2$, then $p(2) = 0$, $p(2) = 10 \bmod p = 0$ so $p = 2$ and $p = 5$.

27. (Used hint from the book here.) $U(p)$ is abelian of order $p-1$, if $U(p)$ were not cyclic, then by the fundamental theorem of abelian groups, for some q prime, $q \mid p-1$, there is $H \simeq \mathbb{Z}_q \times \mathbb{Z}_q < (U(p), \cdot, 1)$ (the multiplicative group). Let $\phi : \mathbb{Z}_q \times \mathbb{Z}_q \simeq H$ and let $x_{a,b} = \phi(a,b) \in U(p)$, then $x_{a,b}^q = 1$ and so $p(x) = x^q - 1$ has q^2 many solutions, which we know is impossible.

35. Show that $p(x) = x^3 - 2x^2 - 9$ has a root in every field. $p(3) = 3^3 - 2(3^2) - 9 = 3(3^2) - 2(3^2) - 3^2 = (3-2-1)(3^2) = 0$. So 3 is a root in any field. In $\mathbb{Z}_2$, $3 = 1$ and in $\mathbb{Z}^3$, $3 = 0$, but the argument still holds.

37. Let F be a field and $I = \{f(x) \in F[x] \mid f(1) = 0 \text{ and } f(2) = 0\}$. Find $g(x) \in F[x]$ so that $I = (g(x))$.

Let $g(x) = (x-1)(x-2) = x^2 - 3x + 2$, then $(g(x)) = \{f(x)(x-1)(x-2) \mid f(x) \in F[x]\}$. Clearly, $(g) \subseteq I$, conversely, the division algorithm shows that if $f(x) \in I$, then $f(x) = f'(x)(x-1)(x-2)$ for some $f'(x)$.

57. Show that in $\mathbb{Z}_p[x]$, $x^{p-1} - 1 = \prod_{a=1}^{p-1}(x-a)$.

This is because $a^{p-1} = 1$ in $\mathbb{Z}_p$ for all $a \in U(p) = \{1, \cdots, p-1\}$. Thus each element is a root of $x^{p-1} - 1$, and so the factorization follows.

58. (Wilson's Theorem) For every integer $n > 1$, $(n-1)! \bmod n = n-1$ iff n is prime.

If n is prime, then

$$x^{n-1} - 1 = (x-1)(x^{n-2} + x^{n-3} + \cdots + 1) = (x-1)(x-2)\cdots(x-(n-1))$$

So

$$x^{n-2} + x^{n-3} + \cdots + 1 = (x-2)(x-3)\cdots(x-(n-1)) \bmod n$$

Evaluating both sides at $x = 1$ gives

$$n - 1 = (-1)(-2)\cdots(-(n-1)) = (n-1)(n-2)\cdots(1) = (n-1)! \bmod n$$

Conversely, if $n = s \cdot t$ is not prime, then $n \mid (n-1)!$ so $(n-1)! = 0 \bmod n$.

63. For a field that properly contains the field of complex numbers, the first thing that comes to mind is the quotient field of $\mathbb{C}[x]$. That is the field of rational functions over $\mathbb{C}$.

64. If I is an ideal of R show that $I[x]$ is an ideal of $R[x]$. It is clear that $I[x]$ is closed under addition. For the multiplicative closure a little effort is required, consider $p(x) \in I[x]$ with coefficients $a_i \in I$ and $q(x) \in R[x]$ with coefficients $b_i \in R$, then the coefficient of x^i in $p(x)q(x)$ is

$$c_i = \sum_{j=0}^{i} a_j b_{i-j} \in I$$

So $p(x)q(x) \in I[x]$.

65. $2\mathbb{Z}$ is a maximal ideal in $\mathbb{Z}$, since $\mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}_2$ is a field. But, $\mathbb{Z}[x]/2\mathbb{Z}[x] \simeq \mathbb{Z}_2[x]$ is an integral domain, but not a field.

66. Show that if I is a prime ideal of R (commutative and unitary), then $I[x]$ is a prime ideal of $R[x]$.

If I is prime, then R/I is an integral domain. Now $R[x]/I[x] \simeq (R/I)[x]$ and since R/I is an integral domain, so is $R/I[x]$.

Note To prove $R[x]/I[x] \simeq (R/I)[x]$ define the map $\phi : R[x] \to (R/I)[x]$ by $\sum_{i=1}^{n} r_i x^i \mapsto \sum_{i=1}^{n} (r_i/I) x^i$. It is easy to see that this is a homomorphism and is surjective. Now show that $\ker(\phi) = I[x]$.

67. Show that $x = 1$ is the only solution to $x^{25} - 1$ in $\mathbb{Z}_{37}$.

For $x^{25} = 1$ in $U(37)$ we know that $|x| \mid 25 = 5^2$, on the other hand, $|x| \mid |U(37)| = 36 = 6^2$. Only $\gcd(36, 25) = 1$ so $|x| = 1$ and hence $x = 1$.

68. Show that $\mathbb{Q}[x]/)(x^2 - 2) \simeq \mathbb{Q}[\sqrt{2}]$.

There are several ways to do this. Here is one. Define $\phi : \mathbb{Q}[x] \to \mathbb{Q}[\sqrt{2}]$ by $x \mapsto \sqrt{2}$ and everything else maps as must be. A little effort verifies this to be a homomorphism and onto. So suppose $\phi(p(x)) = 0$, then $\sqrt{2}$ is a root of $p(x)$. We know $\overline{p(\sqrt{2})} = \bar{p}(\overline{\sqrt{2}}) = p(-\sqrt{2}) = 0$ as well, so $x^2 - 2 \mid p(x)$ and thus $\ker(\phi) = (x^2 - 2)$.

Note Here as usual $\overline{a + b\sqrt{2}} = a - b\sqrt{2}$.

Ch 17: 7, 12, 14, 15, 19, 28, 38, 39, 40

Ch 18: 17, 30, 33, 36, 37, 38, 41, 42