

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 $a \in U(p) = \{1, \dots, p - 1\}$. 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

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

So

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

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 $\phi : R[x] \rightarrow (R/I)[x]$ 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 $\phi : \mathbb{Q}[x] \rightarrow \mathbb{Q}[\sqrt{2}]$ 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 $\overline{p(\sqrt{2})} = \overline{p}(\sqrt{2}) = p(-\sqrt{2}) = 0$ 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

7. Suppose $r + 1/r$ is an odd integer, show that r is irrational.

Let n be an integer and consider $2n + 1 = x + 1/x$ or $x^2 - (2n + 1)x + 1 = 0$. If r is rational, then this must factor over \mathbb{Q} . But if this factors over \mathbb{Q} , then it factors over \mathbb{Z} as $(x - p)(x - q)$ with $p, q \in \mathbb{Z}$ so that either $p = q = 1$ or $p = q = -1$ and $2n + 1 = p + q = \pm 2$.

12. Construct a field of order 27.

Consider $x^3 + 2x + 1$. This has no root in \mathbb{Z}_3 , so it is irreducible in $\mathbb{Z}_3[x]$ and hence $\mathbb{Z}_3[x]/(x^3 + x + 1)$ is a field, since $\mathbb{Z}_3[x]$ is a PID. The classes of $\mathbb{Z}_3[x]$ are given by $ax^2 + bx + c$ with $a, b, c \in \mathbb{Z}_3$ so there are $3^3 = 27$ elements.

14. Which of the following are irreducible over \mathbb{Q} ?

a. $x^5 + 9x^4 + 12x^2 + 6$: This is irreducible over \mathbb{Q} since $3 \nmid 1$, $3 \mid 9, 12, 6$, and $3^2 \nmid 6$.

b. $x^4 + x + 1$: $x^4 + x + 1$ has no linear factors since the only possible roots are ± 1 . If it factors into quadratics, then we must have $x^4 + x + 1 = (x^2 + ax + 1)(x^2 + bx + 1) = x^4 + (a+b)x^3 + (ab+2)x^2 + (a+b)x + 1$. But then $a+b = 1$ and $a+b = 0$, so this can't happen either.

c. $x^4 + 3x^2 + 3$: This is like (a.). $3 \nmid 1$, $3 \mid 0, 3, 3$, and $3^2 \nmid 3$.

d. $x^5 + 5x + 1$: Let's see if this is irreducible in $\mathbb{Z}_2[x]$. There are no linear factors, no roots in \mathbb{Z}_2 . If there is a quadratic factor it must be one of $x^2, x^2 + 1, x^2 + x, x^2 + x + 1$. Each of $x^2, x^2 + 1, x^2 + x$ have roots in \mathbb{Z}_2 so these can't be a factor. So $x^2 + x + 1$ is the only option. Actually, this does not work as $(x^2 + x + 1)(x^3 + x^2 - 1) = x^5 + 5x + 1$ in $\mathbb{Z}_2[x]$.

We can try $\mathbb{Z}_3[x]$. The quadratic factor would have to be $x^2 + ax + b$ and the only of those that do not have a root in \mathbb{Z}_3 are $x^2 + 1, x^2 + x + 2$, and $x^2 + 2x + 2$ (see Example 8 in text). We can try long division with these and see that none divide evenly, so $x^5 + 5x + 1$ is irreducible in $\mathbb{Z}_3[x]$.

e. $(5/2)x^5 + (9/2)x^4 + 15x^2 + 6x + 3/14$: $(1/14)(35x^5 + 63x^4 + 210x^2 + 84x + 3)$. Again, as above $3 \nmid 35$, $3 \mid 63, 210, 84, 3$, and $3^2 \nmid 3$. So the polynomial is irreducible.

15. Consider $\mathbb{Z}_2[x]/(x^3 + x + 1)$.

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

and noting that $1 = -1 = x^3 + x$ we can divide $x^3 + x$ by $x^2 + x$ and get $x + 1$.

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

So $(x^2 + x)^{-1} = x + 1$.

19. Consider $F = \mathbb{Z}_7[x]/(x^2 + 2)$. $x^2 + 2$ has no roots in \mathbb{Z}_7 so $x^2 + 2$ is irreducible and $\mathbb{Z}_7[x]/(x^2 + 2)$ is a field.

$$\begin{array}{ll} x^1 = x, & x^2 = -2 = 5, \\ x^3 = 5x, & x^4 = 5^2 = 25 = 4, \\ x^5 = 4x, & x^6 = 4x^2 = 20 = 6, \\ x^7 = 6x, & x^8 = 6x^2 = 30 = 2, \\ x^9 = 2x, & x^{10} = 2x^2 = 10 = 3, \\ x^{11} = 3x, & x^{12} = 15 = 1 \end{array}$$

So $|x| = 12$

$$\begin{array}{ll} (x+1) = x+1, & (x+1)^2 = 2x+6, \\ (x+1)^3 = x+2, & (x+1)^4 = 3x, \\ (x+1)^5 = 3x+1, & (x+1)^6 = 4x+2, \\ (x+1)^7 = 6x+1, & (x+1)^8 = 3 \\ (x+1)^9 = 3x+3, & (x+1)^{10} = 6x+4 \\ (x+1)^{11} = 3x+6, & (x+1)^{12} = 2x \\ \vdots & \vdots \end{array}$$

I got tired of this one so I made [python do it for me](#). We see here that $U(F)$ is cyclic, and $(x+1)$ is a primitive 48^{th} root of unity.

A better solution: $(x+1)^m = (x+1)^{8k}(x+1)^m$ for $m = 0, 2, \dots, 7$. $(x+1)^{8k} = ((x+1)^8)^k = 3^k \pmod{7}$. Now in \mathbb{Z}_7 :

$$3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 2^2 = 4, 3^5 = 2 \cdot 6 = 5, 3^6 = 6^2 = 1$$

Now check that $(x+1)^{8k}(x+1)^m \neq 1$ for $k = 1, \dots, 5$ and $m = 0, \dots, 7$. For example

$$\begin{aligned} (x+1)^{8 \cdot 4}(x+1) &= 4x+4, & (x+1)^{8 \cdot 4}(x+1)^2 &= 4(2x+6) = x+3, \\ (x+1)^{8 \cdot 4}(x+1)^3 &= 4(x+2) = 4x+1, & (x+1)^{8 \cdot 4}(x+1)^4 &= 4(3x) = 5x, \\ (x+1)^{8 \cdot 4}(x+1)^5 &= 4(3x+1) = 5x+4, & (x+1)^{8 \cdot 4}(x+1)^6 &= 4(4x+2) = 2x+1, \end{aligned}$$

28. (a) and (b) seem to be asking the same thing as the quadratic monic polynomials are just those polynomials of the form $x^2 + ax + b$. These are irreducible so long as they have no root in \mathbb{Z}_p . That is $x^2 + ax + b \neq (x-m)(x-n) = x^2 - (m+n)x + mn$ for any $m, n \in \mathbb{Z}_p$. There are $p(p-1)/2$ of the form $(x-m)(x-n)$ where $m \neq n$ and p where $m = n$ for a total of $p(p-1)/2 + p$ many reducible monomial quadratics and thus $p^2 - (p(p-1)/2 + p) = p^2 - (p^2 - p)/2 + p = p^2/2 + p/2 = (p)(p+1)/2$ irreducible.

38. If $x^{p-1} - x^{p-2} + \dots - x + 1 = p(-x) = (-x)^{p-1} + (-x)^{p-2} + \dots + (-x)^1 + 1 = f(x)g(x)$ with $\deg(g), \deg(f) > 0$. Then $p(x) = p(-x) = x^{p-1} + x^{p-2} + \dots + x + 1 = f(-x)g(-x) = f_1(x)g_2(x)$. But this contradicts the irreducibility of the cyclotomic polynomial.

39. The evaluation map is obviously a homomorphism. Let $f(x) \in \ker(\phi)$. If $p(x) \nmid f(x)$, then as $p(x)$ is irreducible, we know $\gcd(f(x), p(x)) = 1$ (constant polynomial). We can use the Euclidean algorithm to find $q(x)$ and $r(x)$ so that $q(x)p(x) + r(x)f(x) = 1$. This is a contradiction since $q(a)p(a) + r(a)f(a) = q(a) \cdot 0 + r(a) \cdot 0 = 0 \neq 1$. So $p(x) \mid f(x)$.

40. We have seen before that $\mathbb{Z}[x]/(x^2+1) \simeq \mathbb{Z}[i]$ is an integral domain, but not a field, so (x^2+1) is prime and not maximal.

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

17. Show in $\mathbb{Z}[i]$ that 3 is irreducible, hence prime, since $\mathbb{Z}[i]$ is a PID, and hence UFD, but 2 and 5 are not irreducible.

$$2 = (1-i)(1+i)$$

and

$$5 = (1-2i)(1+2i)$$

Suppose $3 = (a+bi)(c+di)$, then

$$3\bar{3} = 9 = (a+bi)(c+di)\overline{(a+bi)(c+di)} = (a+bi)\overline{(a+bi)}(c+di)\overline{(c+di)} = (a^2+b^2)(c^2+d^2)$$

But then, $3 \mid a^2 + b^2$ (or $3 \mid c^2 + d^2$). This is the same as $a^2 + b^2 = 0 \pmod{3}$ and this in turn is the same as

$$(a \pmod{3})^2 + (b \pmod{3})^2 = 0 \pmod{3}$$

But we can just check the values for $a \bmod 3$ and $b \bmod 3$. Using the symmetry that we have here, we can just check the pairs (r, s) for (r, s) in $\{(0, 0), (1, 0), (2, 0), (1, 1), (2, 1), (2, 2)\}$ the only one satisfying $r^2 + s^2 = 0$ is for $r = 0 = s$. So we must $3 \mid a, b$ and hence $3 \mid a + bi$ and so

$$3 = 3(a' + b'i)(c + di)$$

but then $a' + b'i, c + di \in \{1, -1\}$ (a unit) so 3 is irreducible.

29. Show that if $p \mid n$, then p is prime in \mathbb{Z}_n .

If $p \mid a \cdot b$ in \mathbb{Z}_n , then $a \cdot b = p \cdot m \bmod n$ so $n \mid a \cdot b - p \cdot m$, that is $a \cdot b - p \cdot m = n \cdot q$ and so $p \cdot m = a \cdot b - n \cdot q$ and since $p \mid n$ we must have $p \mid a \cdot b$ so $p \mid a$ or $p \mid b$. It is easy to see that if $p \mid a$, then $p \mid a \bmod n$.

So p is a prime in \mathbb{Z}_n .

30. You might think that since all primes are irreducible, we are done from #29. But this was only true in an integral domain. So we must argue the point.

If $p^2 \nmid n$, then n/p and p are relatively prime, so there are s and t such that $sp + t(n/p) = 1$, but then $p = p(sp) + tn$ and thus $p = p(sp) \bmod n$ witnesses that p is decomposable since p and sp are not a units in \mathbb{Z}_n .

Conversely, if $p^2 \mid n$ and $p = ab$, then $p - ab = mn$ so $1 - ab/p = m(n/p)$. We know $p \mid b$ or $p \mid a$. Suppose $p \mid b$. We know $q \nmid a$ for any prime factor of n' and so $\gcd(a, n') = \gcd(a, n) = 1$ and so a is a unit in \mathbb{Z}_n .

33. This is a trivial induction. Suppose for all $m < n$ is $p \mid a_1 \cdots a_{m-1}$, then $p \mid a_i$ for some $i < m$. Then if $p \mid a_1 \cdots a_{n-1}$ we have $p \mid a_1 \cdots a_{n-2}$ or $p \mid a_{n-1}$. In the latter case, we are done. In the first case, we apply the induction hypothesis to $m = n - 1$.

36. Show that every integral domain with the descending chain condition is a field. First, we may assume $|R|$ is infinite since we already know that any finite integral domain is a field.

If R is not a field, let $r \neq 0$ be a non-unit of R . If $(r^2) = (r)$, then $r = r^2 t$ for some t , but then $r - r^2 t = r(1 - rt) = 0$, so either $r = 0$ or r is a unit. Either is a contradiction. So $(r^2) \subset (r)$. Continuing, we get $(r^3) = (r^2)$ implies $r^2 = r^3 t$ so $r^2(1 - rt) = 0$ and either $r^2 = 0$ or r is a unit. Again, neither can be true so $(r^3) \subset (r^2)$. We can continue thus to get $(r^{n+1}) \subset (r^n)$ for all n . This contradicts the descending chain condition. So it must be that R is a field.

37. Show that R satisfies ACC iff every ideal is finitely generated.

Suppose R satisfies ACC. Fix an ideal I . Take $a_1 \in I$, if $(a_1) \neq I$, then take $a_2 \in I - (a_1)$. If $(a_1, a_2) \neq I$, take $a_3 \in I - (a_1, a_2)$, etc. Since R satisfies ACC, we must reach some k so that $(a_1, a_2, \dots, a_k) = I$.

Suppose every ideal is finitely generated. Let $I_1 \subset I_2 \subset \cdots$ be proper ideals. Let $I = \bigcup_i I_i$. I is finitely generated so get k such that $(a_1, \dots, a_k) = I$. Take n so that $a_i \in I_n$ for $i = 1, 2, \dots, k$. Then $I_n = I$ and we have ACC.

38. It is not true that a subdomain of a Euclidean domain needs be Euclidean as $\mathbb{Z}[x] \subset \mathbb{Q}[x]$ demonstrates. Both are domains, but $\mathbb{Z}[x]$ is not Euclidean.

41. In $\mathbb{Z}[-7]$, clearly $N(6 + 2\sqrt{-7}) = 6^2 + 7 \cdot 2^2 = 36 + 28 = 1 + 63 = 1^2 + 3^2 \cdot 7 = N(1 + 3\sqrt{-7})$. Also, if $u \in U(\mathbb{Z}[\sqrt{-7}])$, then $N(u) = 1 = a^2 + 7b^2$ where $a, b \in \mathbb{Z}$. The only option here is

$u = \pm 1$, that is $U(\mathbb{Z}[\sqrt{-7}]) = \{1, -1\}$. Clearly, $6 + 2\sqrt{-7} \neq \pm(1 + 3\sqrt{-7})$ so $6 + 2\sqrt{-7}$ and $1 + 3\sqrt{-7}$ are not associates.

42. Let $R = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \cdots = \sum_{i \in \mathbb{N}} \mathbb{Z}$. Let $r_i = (1, 1, 1, \dots, 1, 0, 0, \dots) \in R$ so that r_i has i many 1's followed by 0's. Clearly $(r_i) \subset (r_{i+1})$, basically,

$$(r_i) = R^i \times \{0\} \times \{0\} \times \cdots \subset R^{i+1} \times \{0\} \times \{0\} \times \cdots = (r_{i+1}).$$