

Homework 6 Solutions

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 $a \pmod{3}$ and $b \pmod{3}$. 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 $a \cdot b = p \cdot m \pmod{n}$ 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 $p \mid a \pmod{n}$.

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 $p = p(sp) \pmod{n}$ witnesses that p is decomposable since p and sp are not units in \mathbb{Z}_n .

Conversely, if $p^2 \mid n$ and $p = ab \pmod{n}$, then $p - ab = mn$ so $1 - ab/p = 1 - ab' = m(n/p) = mn'$, in \mathbb{Z} . We know $p \mid b$ or $p \mid a$. Suppose $p \mid b$. In \mathbb{Z} we have now $1 = ab' + mn'$ and so $1 = \gcd(a, n') = \gcd(a, n)$ 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 $\mathbb{Z}[\sqrt{-7}]$, 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,

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

Ch 19: 1 – 3, 14 – 16, 20, 22, 24, 25, 36, 37, 43, 44, 47

1. Describe $\mathbb{Q}(\sqrt[3]{5})$.

$\mathbb{Q}(\sqrt[3]{5}) = \mathbb{Q}[x]/\langle x^3 - 5 \rangle$ so one description is as the set of all elements $q(x) + \langle x^3 - 5 \rangle$, where $q(x) = a_0 + a_1x + a_2x^2$ (by Euclidean algorithm). Letting $\alpha = x + \langle x^3 - 5 \rangle$, or if you like, let $\sqrt[3]{5} = x + \langle x^3 - 5 \rangle$, then the elements of $\mathbb{Q}[x]/\langle x^3 - 5 \rangle$ are of the form $a_0 + a_1\alpha + a_2\alpha^2$ so that

$$\mathbb{Q}(\sqrt[3]{5}) = \{a_0 + a_1(5^{1/3}) + a_2(5^{2/3}) \mid a_0, a_1, a_2 \in \mathbb{Q}\}$$

Another less useful description is $\mathbb{Q}(\sqrt[3]{5})$ is the smallest field containing \mathbb{Q} as a subfield with a root of $x^3 - 5$.

2. Show that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Clearly, $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ so to get equality, we just need $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Notice, $(\sqrt{2} + \sqrt{3})(\sqrt{2} + \sqrt{3}) = 2 + 2\sqrt{6} + 3 \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. So $\sqrt{6} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. This means $(\sqrt{2} + \sqrt{6})(\sqrt{2} + \sqrt{6}) = 2 + 2\sqrt{2}\sqrt{6} + 6 = 8 + 4\sqrt{3}$, so $\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Similarly, $\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

3. Find the splitting field of $x^3 - 1$. Let $\omega = e^{i\frac{2\pi}{3}}$ be the principle cubic root unity. Then $x^3 - 1$ has roots $1, \omega, \omega^2$ and so $\mathbb{Q}(\omega)$ is the splitting field.

14. Find all ring automorphisms of $\mathbb{Q}(\sqrt{5})$ and of $\mathbb{Q}(\sqrt[3]{5})$.

The automorphisms must take roots of the irreducible polynomial to each other. So for $x^2 - 5$ the roots are $\pm\sqrt{5}$, and thus there are two automorphisms, the identity, and $\sqrt{5} \mapsto -\sqrt{5}$.

For $x^3 - 5$ the roots are $\sqrt[3]{5}\omega^m$ for $m = 0, 1, 2$ where $\omega = e^{i\frac{2\pi}{3}}$. Since any automorphism of $\mathbb{Q}(\sqrt[3]{5})$ must send $\sqrt[3]{5}$ to one of $\sqrt[3]{5}\omega^m$ for $m = 0, 1, 2$, there is only one possibility. Namely, $\sqrt[3]{5}$ must be fixed, and hence there is only the identity automorphism.

Note This is a different question, than understanding the automorphisms of the splitting field $\mathbb{Q}(\sqrt[3]{5}, \omega)$, i.e., $\text{Gal}(x^3 - 5)$.

15. Let F be a field of characteristic p and let $f(x) = x^p - a$ show that f either splits or is irreducible over F .

Let α be a root of $f(x)$ in a field $F \subseteq E$ (possibly $E = F$), since E is also of characteristic p we have $\alpha^p - a = 0$ so $a = \alpha^p$ and $f(x) = x^p - \alpha^p = (x - \alpha)^p$. If $\alpha \in F$, then $f(x)$ splits over F .

If $\alpha \notin F$ let $g(x)$ be an irreducible factor of $f(x)$. We know, in E , that $g(x) = (x - \alpha)^k$ for some $1 < k < p$ since $f(x) = (x - \alpha)^p$, but then $g(x) = h(x^p)$ (Theorem 19.6) and so it must be that $k = p$, hence $f(x) = g(x)$, that is, $f(x)$ is irreducible.

16. Suppose β is a zero of $f(x) = x^4 + x + 1$ in some field extension E of \mathbb{Z}_2 . Write $f(x)$ as a product of linear factors in $E[x]$.

We can perform polynomial division:

$$\begin{array}{r}
 x^3 + \beta x^2 + \beta^2 x + (1 + \beta^3) \\
 x - \beta \overline{) x^4 + x + 1} \\
 \underline{x^4 - \beta x^3} \\
 \beta x^3 \\
 \underline{\beta x^3 - \beta^2 x^2} \\
 \beta^2 x^2 + x \\
 \underline{\beta^2 x^2 - \beta^3 x} \\
 (1 + \beta^3)x + 1 \\
 \underline{(1 + \beta^3)x - \beta(1 + \beta^3)} \\
 \beta^4 + \beta + 1 = 0
 \end{array}$$

Now

$$\begin{aligned}
 x^3 + \beta x^2 + \beta^2 x + \beta^3 + 1 &= x^2(\beta + x) + \beta^2(\beta + x) + 1 \\
 &= (x^2 + \beta^2)(x + \beta) + 1 = (x + \beta)^2(x + \beta) + 1 = (x + \beta)^3 + 1 \\
 &= (x + \beta)^3 - 1 \\
 &= (x + \beta - 1)((x + \beta)^2 + (x + \beta) + 1)
 \end{aligned}$$

Now

$$\begin{aligned}
 (x + \beta)^2 + (x + \beta) + 1 &= x^2 + \beta^2 + x + \beta + 1 \\
 &= x^2 + \beta^2 + x + \beta^4 && (\text{since } \beta^4 = -(1 + \beta) = 1 + \beta) \\
 &= (x + \beta^2)(x + \beta^2 + 1)
 \end{aligned}$$

So

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

20. Find $p(x)$ in $\mathbb{Q}[x]$ so that $\mathbb{Q}(\sqrt{1 + \sqrt{5}}) = \mathbb{Q}[x]/\langle p(x) \rangle$

$$\begin{aligned}
 x^2 &= 1 + \sqrt{5} \\
 x^2 - 1 &= \sqrt{5} \\
 (x^2 - 1)^2 &= 5 \\
 x^4 - 2x^2 - 4 &= 0
 \end{aligned}$$

We cannot use Theorem 17.4 (Eisenstein's Criteria) to see that $p(x) = x^4 - 2x^2 - 4$ is irreducible. If $p(x)$ were reducible, then $x^4 - 2x^2 - 4 = (x^2 + ax + b)(x^2 + cx + d)$ with $a, b \in \mathbb{Z}$. Since $ax^3 + cx^3 = 0$ we have $c = -a$ and hence we have $x^4 - 2x^2 - 4 = (x^2 + ax + b)(x^2 - ax + d)$. Now we have $adx - abx = 0$, so either $a = 0$ or $b = d$. $b = d$ is not possible since $b^2 \neq -4$ and $a = 0$ is also not possible since then $x^4 - 2x^2 - 4 = (x^2 + b)(x^2 + d) = x^4 + (b + d)x + bd$ with $b + d = -2$ and $bd = -4$, hence $b = -2 - d$ and $(-2 - d)d = -2d + d^2 = -4$ or $d^2 - 2d + 4 = 0$ for an integer d . With some effort, we have shown that $p(x)$ is irreducible.

22. Suppose $f(x)$ and $g(x)$ are relatively prime in $F[x]$ and K is an extension field of F , then $f(x)$ and $g(x)$ remain relatively prime in $K[x]$.

If $f(x)$ and $g(x)$ are relatively prime in $F[x]$, this means that there are $h(x)$ and $k(x)$ in $F[x]$ so that $h(x)f(x) + k(x)g(x) = 1$. (Recall $f(x)$ and $g(x)$ are relatively prime if there is $l(x)$ a non-unit with $l(x) \mid f(x), g(x)$.) But since $F[x]$ is a PID, this means that $(f(x)) + (g(x)) = F[X]$ and this, in turn, means that the desired $h(x)$ and $k(x)$ exist.

But then, $h(x)f(x) + k(x)g(x) = 1$ continues to hold in $K[x]$ so $f(x)$ and $g(x)$ remain relatively prime.

24. Describe the elements of $\mathbb{Q}(\sqrt[4]{2})$ over $\mathbb{Q}(\sqrt{2})$.

$\mathbb{Q}[x]/\langle x^4 - 2 \rangle = \mathbb{Q}(\sqrt{2})[x]/\langle x^2 - \sqrt{2} \rangle = \mathbb{Q}(\sqrt[4]{2})$ and so

$$\mathbb{Q}(\sqrt[4]{2}) = \{a + b\sqrt[4]{2} \mid a, b \in \mathbb{Q}(\sqrt{2})\} = \{a + b2^{1/4} + c2^{1/2} + d2^{3/2} \mid a, b, c, d \in \mathbb{Q}\}$$

25. What can you say about the order of the splitting field of $x^5 + x^4 + 1 = (x^2 + x + 1)(x^3 + x + 1)$ over \mathbb{Z}_2 ?

Let α be a root of $x^2 + x + 1$, that is, $\alpha = x + \langle x^2 + x + 1 \rangle$ in $\mathbb{Z}_2[x]/\langle x^2 + x + 1 \rangle$. So

$$\mathbb{Z}_2(\alpha) = \{a + b\alpha \mid a, b \in \mathbb{Z}_2\} = \{0, 1, \alpha, 1 + \alpha\}$$

and the multiplication table is

	α	$1 + \alpha$
α	$1 + \alpha$	1
$1 + \alpha$	1	α

Here is how you get this, $\alpha^2 = x^2 + \langle x^2 + x + 1 \rangle$, $(\alpha + 1)^2 = \alpha^2 + 1$ (Recall that $(a+b)^2 = a^2 + b^2$ here.), and $\alpha(1 + \alpha) = \alpha^2 + \alpha$. First we compute α^2 :

$$\begin{array}{r} 1 \\ x^2 \overline{) x^2 + x + 1} \\ \underline{x^2} \\ x + 1 \end{array}$$

So $x^2 = x + 1 \pmod{x^2 + x + 1}$ so $\alpha^2 = \alpha + 1$. Hence $(\alpha + 1)^2 = \alpha^2 + 1 = \alpha + 2 = \alpha$ and $\alpha(\alpha + 1) = \alpha^2 + \alpha = 2\alpha + 1 = 1$.

We know that if $g(x) = x^3 - x + 1$ factored in $\mathbb{Z}_2(\alpha)$, then there must be one linear factor and hence a root in $\mathbb{Z}_2(\alpha)$, but we can check that this is not the case.

$$g(\alpha) = \alpha^3 + \alpha + 1 = \alpha^2\alpha + \alpha^2 = \alpha^2(\alpha + 1) = (\alpha + 1)^2 = \alpha \neq 0$$

and

$$g(\alpha + 1) = (\alpha + 1)^3 + (\alpha + 1) + 1 = (\alpha + 1)^2(\alpha + 1) + \alpha = \alpha(\alpha + 1) + \alpha = 1 + \alpha \neq 0$$

We already know that $g(0)$ and $g(1)$ are not 0. So we see that $g(x)$ is still irreducible over $\mathbb{Z}_2(\alpha)$. Let β be a root of $g(x)$, that is, $\beta = x + \langle g(x) \rangle$ in $\mathbb{Z}_2(\alpha)$. Then $[\mathbb{Z}_2(\alpha, \beta) : \mathbb{Z}_2(\alpha)] = 3$ and hence $|\mathbb{Z}_2(\alpha, \beta)| = 4^3 = 64$. Notice $[\mathbb{Z}_2(\alpha, \beta) : \mathbb{Z}_2] = [\mathbb{Z}_2(\alpha, \beta) : \mathbb{Z}_2(\alpha)][\mathbb{Z}_2(\alpha) : \mathbb{Z}_2] = 3 \cdot 2 = 6$ and so $\mathbb{Z}_2(\alpha, \beta) = 2^6 = 64$.

Now $\mathbb{Z}_2(\alpha, \beta) = \mathbb{Z}_2(\alpha)(\beta) = \mathbb{Z}_2(\alpha)(\beta)$ and

$$\mathbb{Z}_2(\alpha)(\beta) = \{a_0 + a_1\beta + a_2\beta^2 \mid a_i \in \mathbb{Z}_2(\alpha)\}$$

whereas

$$\mathbb{Z}_2(\beta)(\alpha) = \{a_0 + a_1\alpha \mid a_i \in \mathbb{Z}_2(\beta)\}$$

In either case, we have that a typical element of $\mathbb{Z}_2(\alpha, \beta)$ has the form

$$\begin{aligned} (a_0 + a_1\beta + a_2\beta^2) + (b_0 + b_1\beta + b_2\beta^2)\alpha &= a_0 + b_0\alpha + a_1\beta + b_1\beta\alpha + a_2\beta^2 + b_2\alpha\beta^2 \\ &= c_0 + c_1\alpha + c_2\beta + c_3\alpha\beta + c_4\beta^2 + c_5\alpha\beta^2 \end{aligned}$$

where $c_i \in \mathbb{Z}_2$.

36. Find the splitting field for $x^4 + 1 = (x^2 + x + 2)(x^2 + 2x + 2)$ over \mathbb{Z}_3 .

Let α be a root for $x^2 + x + 2$, the elements of $\mathbb{Z}_3(\alpha)$ are of the form $a_0 + a_1\alpha$ and these are

$$0, 1, 2, \alpha, 2\alpha, 1 + \alpha, 1 + 2\alpha, 2 + \alpha, 2 + 2\alpha$$

Note that $\alpha^2 = -\alpha - 1 = 2 + 2\alpha$ with this, we can compute all other multiples. Let's check the status of $g(x) = x^2 + 2x + 1$

$$g(\alpha) = \alpha^2 + 2\alpha + 1 = 2 + 2\alpha + \alpha + 1 = 0$$

So $g(x)$ already has a root in $\mathbb{Z}_3(\alpha)$ and hence splits. So the splitting field of $x^4 + 1$ is $\mathbb{Z}_3(\alpha)$.

Note Not the differences between (25) and (36). When doing iterated extensions, what happens depends on whether the roots from one extension are already roots of a future extension.

37. This is sort of stated poorly. Obviously, if there is smallest field containing F and a_1, \dots, a_n , then

$$\bigcap \{E \mid F \subseteq E \text{ and } \{a_1, \dots, a_n\} \subset E\}$$

must be this smallest field, by definition of "smallest":)

The point is that the intersections of fields is a field; this is easy.

43. Let $F = \mathbb{Z}_p(t)$ and $f(x) = x^p - t$. Show that $f(x)$ is irreducible and has multiple roots.

$f'(x) = px^{p-1} = 0$ since F has characteristic p . Thus $f(x)$ and $f'(x)$ do have a common factor in $F[x]$, namely $f(x)$. Thus $f(x)$ has repeated roots.

By exercise (15) above, $f(x)$ is irreducible unless it splits in F . If $f(x)$ splits over F , then $t = \alpha^p = (p(t)/q(t))^p$ for some $p(t), q(t) \in \mathbb{Z}_p[t]$ with $q(t) \neq 0$ and

$$t(a_0 + a_1t + \dots + a_nt^n)^p = (b_0 + b_1t + \dots + b_mt^m)^p$$

hence $\deg(LHS) = np + 1 = mp = \deg(RHS)$, which absurd. So $f(x)$ is irreducible over F .

44. Let $f(x)$ be an irreducible polynomial over a field F . Prove that the number of distinct zeros of $f(x)$ in a splitting field divides $\deg f(x)$.

If the characteristic of F is 0, then there are $\deg(f(x))$ distinct roots. If $\text{char}(F) = p$, then $f(x) = (x - a_1)^m \dots (x - a_k)^m$ where $km = \deg(f)$. This follows from the corollary to Theorem 19.9.

47. What is the splitting field of $f(x) = x^3 - 2$ over $\mathbb{Q}(\sqrt[3]{2})$? What is the splitting field over $\mathbb{Q}(\sqrt{3}i)$?

We know that the splitting field of $f(x)$ is $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$ where $\omega = e^{i\frac{2\pi}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. So

$$E = \mathbb{Q}(\sqrt[3]{2})(\omega) = \mathbb{Q}(\sqrt[3]{2})(\sqrt{3}i) = \mathbb{Q}(\sqrt{3}i)(\sqrt[3]{2})$$