Homework 5 Solutions

Ch 14: 10, 22, 42, 48, 51, 55, 60, 62, 67, 73, 78, 80

10. In $\mathbb{Z}[x]$ show that $(2x, 3) = (x, 3)$. Clearly, $2x \in (x, 3)$ so $(2x, 3) \subseteq (x, 3)$. Conversely, $3x \in (2x, 3)$ so $x = 3x - 2x \in (2x, 3)$.

22. Let R be a finite commutative ring and I be prime. Then R/I is a finite integral domain and hence a field. We have shown before that any finite integral domain is a field, the reason is simple, let a be a non-zero element of a finite integral domain, then $ab = ac \iff a(b-c) = 0 \iff b - c = 0 \iff b = c$, so the map $c \mapsto ac$ is 1-1 and hence onto. So $ac = 1$ for some c.

42. Show that $\mathbb{R}[x]/(x^2 + 1)$ is a field. Consider $\phi : \mathbb{R}[x] \to \mathbb{C}$ given by $x \mapsto i$ (or $x \mapsto -i$) and extended uniquely to $\mathbb{R}[x]$. Clearly, ϕ is a homomorphism and $p(x) \in \ker(\phi) \iff p(i) = 0 \iff (x - i) \mid p(x)$. Since $p(x) \in \mathbb{R}[x]$ $-i$ must also be a root, namely, z is a root of $p(x)$ iff $\bar{z}$ is a root of $\bar{p}(z)$, so $(x - i)(x + i) = x^2 + 1 \mid p(x)$. So $(x^2 + 1) = \ker(\phi)$.

48. Let $I = \{a + bi \mid a, b \in 2\mathbb{Z}\} = (2, 2i)$. So I is clearly an ideal. There will be four classes, I, $1 + I$, $i + I$, $(1 + i) + I$ and $\mathbb{Z}[i]/I$ will be isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. Note $\mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i$ as an inner direct product and $I = 2\mathbb{Z} + 2\mathbb{Z}i$ and $(\mathbb{Z} + \mathbb{Z}i)/(2z + 2\mathbb{Z}i) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \mathbb{Z}_2 \times \mathbb{Z}_2$. This can't be a field, but is an integral domain. (Integral domains are closed under products, fields are not.)

51. In $\mathbb{Z}[x]$ show that $I = \{f(x) \mid f(0) \text{ is even }\} = (x, 2)$. It is clear that $f(x) \in I \iff f(x) = p(x) \cdot x + a$ for $a \in 2\mathbb{Z}$. This has just two elements, I and $1+I$, and $\mathbb{Z}[x]/I$ is isomorphic to $\mathbb{Z}_2$. This is a field, so I is maximal, hence prime.

55. In $\mathbb{Z}_5[x]$ let $I = (x^2 + x + 2)$ find a multiplicative inverse to $(2x + 3) + I$. We are looking for $p(x)$ so that $(2x + 3)p(x) = r(x)(x^2 + x + 2) + 1$. Solved by "guessing" $(2x + 3)(3x + 1) = 6x^2 + 11x + 3 = (x^2 + x + 2) + 1$.

60. In a principal ideal domain, show that every prime ideal is maximal. Let (p) be prime, if (p) were not maximal, then, there is J so that $(p) \subset J \subset R$. But $J = (q)$ since we are in a principal ideal domain and hence $q \mid p$, and so $p = q \cdot r$. But then $p \mid q$ or $p \mid r$. Suppose $p \mid r$, then $r = p \cdot d$ and we have $p = q \cdot r = q \cdot p \cdot d$ so $p \cdot (1 - q \cdot d) = 0$ and thus $q \cdot d = 1$ and so q is a unit. This is a contradiction since $(q) \neq R$. A similar argument works if $p \mid q$. In this case, we get r as a unit, so that $(p) = (q)$, again a contradiction.

62. Showing that $N(A)$ is an ideal is straightforward. Suppose $r, s \in N(A)$ so that $r^n, s^m \in A$; let $k = \max\{m, n\}$, then $(r + s)^k = \sum_{i=0}^{k} \binom{k}{i} r^i s^{k-i}$. In every term either r^i or s^{k-i} will be in A since $i \geq n$ or $k - i \geq m$ for all i. So $(r + s)^k \in A$. That $r \cdot s \in N(A)$ for all $r \in R$ and $s \in N(A)$ is simpler.

Here is even more!

$$N(A) = \bigcap\{J \supset A \mid J \text{ is prime}\}$$

First notice that for any $r \in R$ with $r^n \in A$, if $A \subset J$ and J is prime, then $r^n \in J$ and hence $r \in J$ (as J is prime). So we have containment $N(A) \subseteq \bigcap\{J \supset A \mid J \text{ is prime}\}$.

Now suppose $r \notin N(A)$, then we want to find a prime ideal J with $A \subset J$ and $r \notin J$. Look at $\mathcal{I}$ being the set of all ideals of R such that $r^n \notin I$ for any n. We can find a maximal such ideal J, we just need to show that J is prime. Suppose $a \cdot b \in J$ and $a, b \notin J$. By maximality, this means that $r^n \in (a) + J$ and $r^m \in (b) + J$ so $r^n = at + s$ and $r^m = bt' + s'$ for $t, t' \in R$ and $s, s' \in J$. This means $r^{n+m} = abtt' + ats' + bt's + ss' \in J$ which is a contradiction, so $a \in J$ or $b \in J$.

67. First notice that by the polynomial division algorithm $p(x) = ax + b \bmod x^2 + x + 1$ for all $p(x) \in \mathbb{Z}_2[x]$. So the elements of the field are $0, 1, x$, and $1 + x$ here $x(1 + x) + (x^2 + x + 1) = 1 + (x^2 + x + 1)$ so $x^{-1} = 1 + x$ and we see that $\mathbb{Z}_2[x]$ is a field.

73. Show that if R is a PID, then R/I is a PID for all ideals $I \subset R$. Let $J \subset R/I$ be an ideal, then $J = J'/I$ for $J' = \{r \in R \mid r + I \in J\}$. We know $J' = (p)$ in R and so $J = (p)/I = (p/I)$. So R/I is a PID.

78. Show that the characteristic of $R = \mathbb{Z}[i]/(a + bi)$ divides $a^2 + b^2$.

Just for fun here is a 3Blue1Brown video discussing Gaussian numbers and Gaussian primes.

To begin with we have **Fact** $\mathbb{Z}[i]/(a + bi) \simeq \mathbb{Z}_{a^2+b^2} = \mathbb{Z}/(a^2 + b^2) = \mathbb{Z}/(a^2 + b^2)\mathbb{Z}$.

For this see here.

So consider the general case where $\gcd(a, b) \neq 1$. Notice that in this case there are 0-divisors in R.

First, why is $\mathbb{Z}[i]/(a + bi)$ finite? It turns out that $\mathbb{Z}[i]$ is Euclidean, and hence a PID with the function witnessing that $\mathbb{Z}[i]$ is Euclidean being the multiplicative norm $n(z) = z \cdot \bar{z}$. (See notes where $\mathbb{Z}[\sqrt{-5}]$ is discussed. $\mathbb{Z}[\sqrt{-5}]$ is definitely not a PID since is irreducible and not prime.) For a proof of this see here.

Claim: $\mathbb{Z}[i]/I$ is finite for every (non-trivial) ideal I.

This is because $\mathbb{Z}[i]/I = \mathbb{Z}[i]/(z)$ for some z and the classes are $w + (z)$ where $n(w) < n(z)$. So if $z = a + bi$, then $w = c + di$ where $c^2 + d^2 < a^2 + b^2$ and there are only finitely many such integers (c, d). (Integer lattice points in a circle of radius $\sqrt{a^2 + b^2}$.

Now we might just ask what $\mathbb{Z}[i]/(a + bi)$ is and this is an interesting topic. (See here and here.)

Back down to Earth and the problem at hand: Let n be the characteristic of $\mathbb{Z}[i]/(a + bi)$ so we know $n \in (a + bi)$ and so $n = (a + bi)(c + di)$. $\gcd(c, d) = 1$ else we could factor out a common factor and get $n' = (a + bi)(a' + d'i)$ where $n' < n$ contradicting the definition of n. So there is α and β in $\mathbb{Z}$ satisfying $\alpha c + \beta d = 1$. We also have $ad + bc = 0$ and so we get

$$\begin{aligned} a\alpha c + a\beta d &= a & \qquad b\alpha c + b\beta d &= b \\ \alpha ac - \beta bc &= a & \qquad -\alpha ad + \beta bd &= b \end{aligned}$$

So

$$n = ((\alpha a - \beta b)c - (\alpha a - \beta b)di)(c + di) = (\alpha a - \beta b)(c^2 + d^2)$$

On the other hand we know that

$$n^2 = n\bar{n} = (a + ib)(a - bi)(c + di)(c - di) = (a^2 + b^2)(c^2 + d^2)$$

So

$$n = \frac{a^2 + b^2}{\alpha a - \beta b}$$

80. Let $R = \mathbb{Z}[\sqrt{-5}]$ and $I = \{a + b\sqrt{-5} \mid a - b \text{ is even}\}$. Show that I is maximal.

Consider the map

$$\phi(a + b\sqrt{-5}) = \begin{cases} 1 & a - b \text{ is odd} \\ 0 & a - b \text{ is even} \end{cases}$$

Check that $\phi : \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}_2$ is a surjective homomorphism. The main thing is multiplication where we have

$$\phi((a + b\sqrt{-5})(c + d\sqrt{-5})) = \begin{cases} 1 & (ac - 5bd) - (ad + bc) \text{ is odd} \\ 0 & (ac - 5bd) - (ad + bc) \text{ is even} \end{cases}$$

We have

$$(ac - 5bd) - (ad + bc) = (ac + bd) - (ad + bc) - 6bd = a(c - d) + b(d - c) - 6bd = (a - b)(c - d) - 6bd$$

So $(ac - 5bd) - (ad + bc)$ is odd only when $(a - b)$ and $(c - d)$ are odd. This is what we need here.

Since $\mathbb{Z}_2$ is a field, I is maximal.

Ch 15: 12, 14, 26, 31, 34, 38, 40, 44, 46, 50, 65, 67

12. The point here is that if $\phi : m\mathbb{Z} \to n\mathbb{Z}$, then

$$\phi(mk) = \underbrace{\phi(m) + \cdots + \phi(m)}_{k \text{ times}} \Longmapsto k\phi(m)$$

so clearly everything is determined by $\phi(m)$ and if we hope to be onto, then $\phi(m) = \pm n$ must hold. But then we have

$$\phi(m \cdot (mn)) = mn\phi(m) = mn^2 \neq n(n^2) = n\phi(m^2) = \phi(m^2 n)$$

So the map cannot work on products.

14. Show that $\mathbb{Z}_3[i] \simeq \mathbb{Z}_3[x]/(x^2 + 1)$. Nothing is special about 3 here except that it is prime, so $\mathbb{Z}_3$ is a field.

Define $\phi : \mathbb{Z}_3[x] \to \mathbb{Z}_3[i]$ by $\phi(f(x)) = f(i)$, this is clearly a ring homomorphism. (This sort of evaluation map is always a homomorphism.) The map is clearly onto as $\phi(a + bx) = a + bi$. $f(x) \in \ker(\phi)$ iff $f(i) = 0$. Since the coefficients are in $\mathbb{Z}_3$ we have $\overline{f(i)} = \overline{f}(-i) = f(-i) = 0$.

this by the division algorithm we have that $(x - i)(x + i) = x^2 + 1 \mid f(x)$ since if not $f(x) = (x^2 + 1)q(x) + (ax + b)$ so $f(i) = b + ia = 0$ and so $a = b = 0$.

26. Determine all ring homomorphisms $\phi : \mathbb{Z}_n \to \mathbb{Z}_n$.

If we insist that $\phi(1) = 1$, i.e., that ϕ is a homomorphism of unitary rings, then there is just one, namely $\phi(1) = 1$ and so $\phi(m) = \phi(m \cdot 1) = m\phi(1) = m$, so just the identity.

If we allow $\phi(1) \neq 1$, then we still have that ϕ is determined by $\phi(1)$ since $\phi(m) = \phi(m \cdot 1) = m\phi(1)$. since $\phi(1 \cdot 1) = \phi(1)\phi(1) = \phi(1)$ we have $\phi(1) = k$ for some $k \in \mathbb{Z}_n$ satisfying $k^2 = k$ or $k(k-1) = 0$. (That is $\phi(1)$ must be an idempotent element of $\mathbb{Z}_n$.

We can count the number of idempotents. If $n = p_1^{m_1} \cdots p_k^{m_l}$, then

$$\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{m_1}} \times \mathbb{Z}_{p_2^{m_2}} \times \cdots \times \mathbb{Z}_{p_k^{m_l}}$$

so any idempotent k can be associated to $(k_1, \ldots, k_l)$ where each k_i is idempotent in $\mathbb{Z}_{p_i^{m_i}}$, but this means that $p_i^{m_i} \mid k_i(k_i - 1)$ and as p_i can only divde one of k_i or $k_i - 1$ we know that either $k_i = p_i^{m_i}$ or $k_i = 1$. Thus there are 2^l many idempotents and so 2^l many homomorphisms of $\mathbb{Z}_n$ where there are l many distinct prime divisors of n.

31. Prove that $R[x]/(x^2)$ is ring isomorphic to $\left\{ \left[\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right] \;\middle|\; a, b \in R \right\}$.

Let $\phi(a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n) = \left[\begin{smallmatrix} a_0 & a_1 \\ 0 & a_0 \end{smallmatrix}\right]$. Preservation of addition is trivial. For multiplication notice

$$f(x)g(x) = (a_0 + a_1 x + q(x)x^2)(b_0 + b_1 x + r(x)x^2) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + s(x)x^2$$

and so

$$\phi(f(x))\phi(g(x)) = \left[\begin{smallmatrix} a_0 & a_1 \\ 0 & a_0 \end{smallmatrix}\right]\left[\begin{smallmatrix} b_0 & b_1 \\ 0 & b_0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} a_0 b_0 & a_0 b_1 + a_1 b_0 \\ 0 & a_0 b_0 \end{smallmatrix}\right] = \phi(f(x)g(x))$$

We have $f(x) \in \ker(\phi)$ iff $f(x) = 0 + 0x + q(x)x^2 \in (x^2)$, so

$$R[x]/\ker(\phi) = R[x]/(x^2) \simeq \left\{ \left[\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right] \;\middle|\; a, b \in R \right\}$$

34. Let $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_a \times \mathbb{Z}_b$ be given by $\phi(m, n) = (m \bmod a, n \bmod b)$. It is easy to see that ϕ is a surjective homomorphism.

$$(m, n) \in \ker(\phi) \iff m \bmod a = 0 \text{ and } n \bmod b = 0 \iff (m, n) \in (a) \times (b)$$

So $\mathbb{Z} \times \mathbb{Z}/\ker(\phi) = (\mathbb{Z} \times \mathbb{Z})/((a) \times (b)) \simeq \mathbb{Z}_a \times \mathbb{Z}_b$.

38. Let n be given in base 10 as, $n = d_k d_{k-1} \cdots d_1 d_0 = d_k 10^k + d_{k-1} 10^{k-1} + \cdots d_1 10 + d_0$ where $d_i \in \mathbb{Z}_{10}$. Then, since $10 - -1 \bmod 11$,

$$\begin{aligned} n \bmod 11 &= d_k(10 \bmod 11)^k + d_{k-1}(10 \bmod 11)^{k-1} + \cdots d_1(10 \bmod 11) + d_0 \\ &= (d_k(-1)^k + d_{k-1}(-1)^{k-1} + \cdots + d_1(-1) + d_0) \bmod 11 \end{aligned}$$

So

$$11 \mid n \iff 11 \mid d_k(-1)^k + d_{k-1}(-1)^{k-1} + \cdots + d_1(-1) + d_0$$

40. Suppose $\phi : \mathbb{Z}_m \to \mathbb{Z}_n$ is a ring homomorphism. Then as discussed above, it must be the case that $\phi(1)$ completely determines ϕ, and it must be that $\phi(1)^2 = \phi(1)$ and $n \mid m\phi(1)$, since $\phi(0) = 0$ is required. If $\phi(1) = 1$, then we must have $n \mid m$.

44. Clearly, $R[x]/(x) \simeq R$ so (x) is maximal iff R is a field. So (x) is maximal in $Z_n[x]$ iff Z_n is a field iff n is prime.

46. Show that if $\phi : F \to F$ is a field homomorphism, then the prime subfield is fixed by F.

There are two ways to define the prime subfield, F_0. The official definition is

$$F_0 = \bigcap \{F' \subseteq F \mid F' \text{ is a subfield}\}$$

Since the intersection of subfields is a subfield, this definitely defines F_0 as the minimal subfield. On the other hand, F_0 is the subfield generated by 1_F, for a field of prime characteristic p, this is just the copy of $\mathbb{Z}_p$ generated from 1_F. For a field of characteristic 0, F_0 is the copy of $\mathbb{Q}$ of the form $n_F m_F^{-1}$ where $m \neq 0$ and $n_F = 1_F + \cdots + 1_F$, n-times.

So, according to each definition, there is a proof. The proof using the second definition is trivial, just using the fact that $\phi(1_F) = 1_F$.

The proof using the first definition is, perhaps, more interesting. The point is that $\ker(\phi) = \{0_F\}$, assuming that $\ker(\phi) \neq F$. This is because $F/(0_F) \simeq F$ is a field, and so $(0_F) = \{0_F\}$ is a maximal ideal, so there are no non-trivial ideals, and hence every epimorphism is an automorphism. So $\phi(F_0) = \bigcap\{\phi(F') \mid F' \text{ a subfield of } F\} = \bigcap\{F' \mid F' \text{ a subfield of } F\} = F_0$. This argument would not work except that ϕ is a bijection and

$$F' \text{ is a subfield of } F \iff \phi(F') \text{ is a subfield of } \phi(F) = F$$

and

$$F' \text{ is a subfield of } \phi(F) = F \iff \phi^{-1}(F') \text{ is a subfield of } F$$

50. Prove that $x \mapsto x^p$ is a ring homomorphism in a ring of prime characteristic p. We have already done the hard work

$$(x+y)^p = x^p + y^p \text{ (previous exercise) } (x \cdot y)^p = x^y \cdot y^p \text{ (trivial)}$$

Now any field epimorphism of F is an isomorphism unless $\ker(\phi) = F$, and clearly $ker(\phi) \neq F$ for the Frobenius map.

65. Let Q be the field of quotients of $\mathbb{Z}[i]$ and define $\phi : Q \to \mathbb{Q}[i]$ by $(a, b) \mapsto a \cdot b^{-1}$. We can check that this is well-defined and a field homomorphism.

To see that the map is well-defined, suppose $(a, b) = (a', b')$, that is $ab' - a'b = 0$. Then in $\mathbb{Q}[i]$ it is also true that $ab' = a'b$ and so $ab^{-1} = a'b'^{-1}$ so $\phi((a, b)) = \phi((a', b'))$.

Next we check addition, $\phi((a, b) + (a'b')) = \phi((ab' + a'b, bb')) = (ab' + a'b)(bb')^{-1} = ab^{-1} + a'b'^{-1} = p\phi((a, b)) + \phi((a', b'))$. Multiplication is similar.

The map is necessarily 1-1, being a map between fields, so all that is left is seeing that it is onto. Let $r + si \in \mathbb{Q}[i]$, then $r = a/b$ and $s = a'/b'$ where $a, a', b, b' \in \mathbb{Z}$ so $r + si = (ab' + a'bi)(bb')^{-1} \in \mathrm{Img}(\phi)$.

67. Let D be an integral domain and F the field of quotients. Let E be a field that contains D, then E contains naturally a copy of F.

This is exactly as above, define $\phi : F \to E$ by $(a, b) \mapsto ab^{-1}$. Then $\mathrm{Img}(\phi)$ is the desired copy.