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 mutiplicative 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