Math 122, Solution Set No. 13

1 10.3.4

Let $f \in (2) \cup (x) \subset \mathbb{Z}[x]$. Since $x \nmid 2$ and $2 \nmid x$, we have $f = 2xg(x)$ and so $f \in (2x)$. Conversely, if $f \in (2x) \subset \mathbb{Z}[x]$ we have $f = 2xg(x) \Rightarrow f \in (2) \cup (x)$. $\therefore (2) \cup (x) = (2x) \subset \mathbb{Z}[x]$.

2 10.3.6

Let $I := \{\sum_0^n a_k x^k \in \mathbb{Z}[x] | 2^{k+1} | a_k\}$. Note $2 \in I$, but $x \in \mathbb{Z}$ and $x \cdot 2 \notin I$. So I is not an ideal.

3 10.3.8

(a) Let $F : \mathbb{R}[x, y] \to \mathbb{R}$ sends $f(x, y)$ to $f(0, 0)$. Then $\ker F = (x, y)$. (b) If $F : \mathbb{R}[x] \to \mathbb{C}$ is given by $F(f(x)) = f(2+i)$, then $\ker F$ is all real polynomials having $(2+i)$ as a root. Any such polynomial necessarily has $(2-i)$ as a root, and so $\ker F = ((2+i)(2-i)) = (x^2 - 4x + 5)$.

4 10.3.24

(a) Let $N = N(R)$ be the nilradical of a commutative ring R. Let $x, y \in N \Rightarrow x^n = y^n = 0$ for some sufficiently large n. Then if $z \in R$, $(zx)^n = z^n x^n = 0$ and furthermore $-x \in N$. Finally, $(x+y)^{2n} = \sum_{p+q=2n} c_i x^p y^q$ so we always have $p > n$ or $q > n$ and so this sum is zero. Therefore N is an additive subgroup closed under multiplication by arbitrary elements of R, i.e. N is an ideal. (b) Let $R = \mathbb{Z}/n\mathbb{Z}$ and $N = N(R)$. Write the prime factorization $n = \prod p_i e_i$ and let I be the image of the ideal $(\prod p_i)$ in R (by correspondence). Then $I \subset N$ because if $x \in I, x^{\max e_i} = 0$. Also $N \subset I$ because any nilpotent element must clearly contain all the prime factors of n. So $N = (\prod p_i) \subset R$. As a corollary, we have $N(\mathbb{Z}/12\mathbb{Z}) = (6)$ and $N(\mathbb{Z}) = N(\mathbb{Z}/0\mathbb{Z}) = (0)$.

5 10.6.2

Let R be a finite integral domain. Then if $x \neq 0$ is an element of R, the set $\{x, \ldots, x^n, \ldots\}$ must contain some nonzero duplicate $x^n = x^{n+k}$ since R is a domain. Therefore $1 = x^k = (x)(x^{k-1})$ and so all nonzero elements of R have inverses, i.e. R is a field.

6 10.6.5

If R is a domain of order 10, note that R must have the additive structure of $\mathbb{Z}/10\mathbb{Z}$ which is the only abelian group of order 10. It follows from the Sylow Theorems that there are nonzero elements x, y such that $x+x+x+x+x = y+y = 0$. By the distribution property, $x(1+1+1+1+1) = y(1+1) = 0$ and since R is a domain, $1+1+1+1+1 = 1+1 = 0 \Rightarrow 0 = 1 \Rightarrow R = \{0\}$ which is nonsense. Therefore such a ring does not exist.

NOTE: Finite fields necessarily have order that is the power of a prime (I required you to prove this if you used it), and not just prime order.

7 10.7.1

We have that all ideals in $\mathbb{Z}$ are principal, and that $\mathbb{Z}/n\mathbb{Z}$ is a field exactly when n is prime. Therefore corollary (7.3) implies the desired result.

8 10.7.7

By Cor. (7.3) this amounts to showing whether the appropriate ideals are maximal. Consider $I = (x^3 + x + 1) = (f) \subset \mathbb{F}_2[x]$. From class, $\mathbb{F}_2[x]$ is a PID, and so I is maximal iff (f) is an irreducible polynomial. However, since it has degree 3, it would have to have a linear factor and therefore a root in $\mathbb{F}_2$ ir it were reducible. However $f(0) = f(1) = 1$ and so I is maximal. Now consider $I(x^3 + x + 1) = (x - 1)(x^2 + x - 1)$ in $(\mathbb{F}_3[x]$ and so $I \subset ((x + 2))$ and is therefore not maximal.

9 10.7.9

Define the bijective correspondence by identifying the plane with $\mathbb{C}$ and identifying the ideal $(x-p)$ for any point p on the real line and the ideal $(x - z)(x - \overline{z})$ with any point $z = a + bi$ with $b > 0$. Because $\mathbb{R}[x]$ is a principal ideal domain, these ideals are clearly maximal since they are generated by irreducible polynomials; it is easy to check that any maximal ideal in $\mathbb{R}[x]$ has this form.

10 10.7.10

Let R, M be as given and suppose N is an ideal properly containing M. Then by hypothesis, N contains a unit and so $N = R$. Therefore M is maximal. Suppose N is a maximal ideal of R. Then N must contain no units and so $N \subseteq M \Rightarrow N = M$. Therefore M is the unique maximal ideal of R, and R is called a **local ring** with maximal ideal M.

11 10.8.11

Define $f_1 = x^2 + y^2 - 1, f_2 = x^2 - y + 1, and f_3 = xy - 1$.

(a) Set all three polynomials equal to 0. Then subtracting f_2 from f_1 gives $y^2 + y = 2$. This gives $y = 1$ or $y = -2$. In the first case, we have by f_2 that $x = 0$ and then $f_3 \neq 0$. The second implies by f_2 that $x = \sqrt{3i}$ and then again $f_3 \neq 0$. So the polynomials have no common zeroes.

(b) The following polynomials, supplied by Edo Gallo, are such that $p_1 f_1 + p_2 f_2 + p_3 f_3 = 0$: $p_1 = x - xy + 1$, $p_2 = y - x + xy + 1$, $p_3 = y - x - 1$.