MATH 436: Homework X.
Due on Friday, Dec 12

1. **Prime coverings.** Let R be a commutative ring (with 1 as usual). Let I be an ideal of R and $P_1, \ldots, P_n$ be prime ideals of R such that $I \subseteq P_1 \cup \cdots \cup P_n$. Show that $I \subseteq P_j$ for some $j = 1, \ldots, n$. (Hint: Assume not. Reduce to the case $I \cap P_j - \cup_{i \neq j} P_i \neq \emptyset$ for all j and choose elements a_j in these sets for each j. Show that $a_1 + a_2 a_3 \ldots a_n$ is in $I - P_1 \cup \cdots \cup P_n$ and obtain a contradiction.)

2. **A domain which lacks unique factorization.**
(a) Check that $R = \{a + b\sqrt{10} | a, b \in \mathbb{Z}\}$ is a subring of the field of real numbers (and hence an integral domain), which as an additive group is isomorphic to a free Abelian group of rank 2. Check that $D : (R, \cdot) \to (\mathbb{Z}, \cdot)$ given by $D(a + b\sqrt{10}) = a^2 - 10b^2$ is a homomorphism of monoids. Conclude that $M = \{a^2 - 10b^2 | a, b \in \mathbb{Z}\}$ is a submonoid of $(\mathbb{Z}, \cdot)$. Show that if $c \in M$ then $c \equiv 0, 1$ or $4 \bmod 5$.
(b) Show that $D(u) = 0 \leftrightarrow u = 0$. Show that u is a unit of $R \leftrightarrow D(u) = \pm 1$. Describe the units of R.
(c) Calculate $D(2), D(3)$ and $D(4 \pm \sqrt{10})$. Use this together with (a) and (b) to show that $2, 3, 4 + \sqrt{10}, 4 - \sqrt{10}$ are irreducibles of R. Show that these four irreducibles are not associate in R.
(d) Show that the number 6 has two distinct factorizations into irreducibles in R and hence conclude that the four irreducibles in (c) are not prime elements of R. Thus conclude that R is not a UFD and hence not a PID or ED.
(e) However using the homomorphism D, show that any nonzero element of R can be factored into a finite product $u\alpha_1 \ldots \alpha_k$ where u is a unit of R, and α_j is irreducible in R for all $j = 1, \ldots, k$. (Usual empty product convention if the element is a unit.) [Note: We have seen above that this factorization will not be unique however!]

3. **Localizations** Let R be an integral domain and S a multiplicative submonoid of R which does not contain 0. Recall we have shown in class that if I is an ideal of R, then $S^{-1}I = \{[\frac{x}{s}] | x \in I, s \in S\}$ is an ideal of $S^{-1}R$. We have also seen that every ideal J of $S^{-1}R$ is of the form $S^{-1}I$ for some (not necessarily unique) ideal I of R. Finally recall that the correspondence $P \leftrightarrow S^{-1}P$ gives a bijection between the prime ideals P of R not intersecting S and the prime ideals of $S^{-1}R$.
(a) Show that if R is a PID then $S^{-1}R$ is also a PID. Furthermore up to

associates, show that there is a bijective correspondence between the prime elements in $S^{-1}R$ and the prime elements in R which do not occur in any factorizations of any elements of S.
(b) Show that if R is a UFD then $S^{-1}R$ is also a UFD. Show that there is a correspondence between the primes as in (b).
(c) Let $R = \mathbb{Z}$ and p a prime of $\mathbb{Z}$. Let $S = \{p^k | k \in \mathbb{N}\}$. We denote $S^{-1}R$ by $\mathbb{Z}[\frac{1}{p}]$. Describe the elements of $\mathbb{Z}[\frac{1}{p}]$. Explain why $\mathbb{Z}[\frac{1}{p}]$ is a PID and explain why p is a unit of $\mathbb{Z}[\frac{1}{p}]$. Explain why $Spec(\mathbb{Z}[\frac{1}{p}]) = Spec(\mathbb{Z}) - \{(p)\}$ as sets.
(d) Let $R = \mathbb{Z}$ and p be a prime of $\mathbb{Z}$. Let $S = R - (p)$. We denote $S^{-1}R$ by $\mathbb{Z}_{(p)}$ and call it the ring of integers localized at p. Describe the elements of $\mathbb{Z}_{(p)}$. Explain why $\mathbb{Z}_{(p)}$ is a PID with a unique prime element $p = [\frac{p}{1}]$ up to associates. Conclude that any nonzero $\alpha \in \mathbb{Z}_{(p)}$ can be written uniquely as $\alpha = up^{\nu_p(\alpha)}$ where u is a unit of $\mathbb{Z}_{(p)}$ and $\nu_p(\alpha) \in \mathbb{N}$. Give a complete list of all the distinct ideals of $\mathbb{Z}_{(p)}$.
(e) For each proper ideal I, show that $\mathbb{Z}_{(p)}/I$ is isomorphic as a ring to one of $\mathbb{Z}/p^k\mathbb{Z}$ for $k \in \mathbb{N}$.

4. **Formal power series** Let $R[[x]]$ denote the ring of formal power series with coefficients in a ring R. Given $f(x) = \sum_{n=0}^{\infty} a_n x^n \in R[[x]]$ and $\alpha \in R$ we denote $f(\alpha x) = \sum_{n=0}^{\infty} a_n \alpha^n x^n \in R[[x]]$.

Let $\mathbf{k}$ be a field of characteristic zero (e.g., $\mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$). Thus $n \neq 0$ in $\mathbf{k}$ for all $n \in \mathbb{Z} - \{0\}$ and so $\frac{1}{n} \in \mathbf{k}$ for all $n \in \mathbb{Z} - \{0\}$. Thus we may define $e^x = \sum_{n=0}^{\infty} \frac{1}{n!} x^n \in \mathbf{k}[[x]]$ using the usual convention $0! = 1$.
(a) Check that $e^{(a+b)x} = e^{ax}e^{bx}$ in $\mathbf{k}[[x]]$ for any field $\mathbf{k}$ of characteristic zero and any $a, b \in \mathbf{k}$. [Note the reader is warned that while e^{ax} makes sense as a formal power series, there is no meaning to e^a itself as it would represent an infinite sum in $\mathbf{k}$. This is not defined unless we know how to speak of convergence in $\mathbf{k}$ which is a different issue.]
(b) Similarly for fields of characteristic zero, we may define

$$cos(x) = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k)!} x^{2k}$$

and

$$sin(x) = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k+1)!} x^{2k+1}$$

in $\mathbf{k}[[x]]$. Show that if $\mathbf{k}$ contains an element i of mutiplicative order 4 then $e^{iax} = cos(ax) + isin(ax)$. Conclude that $(cos(ax))^2 + (sin(ax))^2 = 1$ in $\mathbf{k}[[x]]$

for all $a \in \mathbf{k}$.
(c) Consider $e^x \in \mathbb{Q}[[x]]$. Explain why $e^x - 1 = xg(x)$ where g is a unit in $\mathbb{Q}[[x]]$. We will write $g^{-1}(x) \in \mathbb{Q}[[x]]$ as $F(x) = \frac{x}{e^x-1}$ and write $\frac{x}{e^x-1} = \sum_{k=0}^{\infty} \frac{B_k}{k!}x^k$. Find a recurrence relation for the B_k and show that $B_0 = 1, B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}$. The B_k are called the Bernoulli numbers.
(d) Show that $F(-x) = x + F(x)$ and use this to conclude that $B_k = 0$ if k odd and $k \neq 1$.
(e) Let $n \in \mathbb{N}$ and p be a prime. Write $n = p^{\nu_p(n)}m$ where $\nu_p(n) \in \mathbb{N}$ and m is relatively prime to p. Show that $\nu_p(n!) = \sum_{k=1}^{\infty} \lfloor \frac{n}{p^k} \rfloor$ where for a real number r, $\lfloor r \rfloor$ is the largest integer less than or equal to r. Conclude that $\nu_p(n!) \leq n$.
(f) Show that for any prime p in $\mathbb{Z}$ and any $k \in \mathbb{N}$, $\frac{p^k}{k!} = \frac{m}{n}$ where $m, n \in \mathbb{N}$ and n is relatively prime to p. Use this to show that if p is a prime of $\mathbb{Z}$ then $e^{px}, cos(px), sin(px)$ define formal power series in $\mathbb{Z}_{(p)}[[x]]$. where $\mathbb{Z}_{(p)}$ is the integers localized at p.
(g) Consider the quotient ring homomorphisms $\mathbb{Z}_{(p)} \to \mathbb{Z}/p^k\mathbb{Z}$ for various positive $k \in \mathbb{N}$. These induce ring epimorphisms from $\mathbb{Z}_{(p)}[[x]] \to (\mathbb{Z}/p^k\mathbb{Z})[[x]]$. Thus the series $e^{px}, cos(px)$ and $sin(px)$ define formal power series in $(\mathbb{Z}/p^k\mathbb{Z})[[x]]$ for all primes p, and positive integers k. Since the reduction is a ring homomorphism, these series will inherit the algebraic identities that they satisfied in $\mathbb{Q}[[x]]$ for example

$$e^{apx}e^{bpx} = e^{(a+b)px} \text{ in } (\mathbb{Z}/p^k\mathbb{Z})[[x]]$$

etc.
Write our the first 9 terms of the image of the formal power series e^{2x} in $(\mathbb{Z}/8\mathbb{Z})[[x]]$ where $\mathbb{Z}/8\mathbb{Z}$ is the ring of integers modulo 8. Use only canonical representatives $\bar{0}, \bar{1}, \ldots, \bar{7}$ for the coefficients of the series. (Hint: You might consider proving and using $n^2 \equiv 1 \bmod 8$ when n is an odd integer.)