Math 60210, Basic Algebra, Problem Set 11, Fall 2018
due Wed, November 28
Do 8 of these problems. One counts as two problems

1. Let $\zeta = e^{2\pi i/3}$ and let $R = \mathbf{Z}[\zeta]$. Prove that R is a Euclidean domain.

2. Let F be a field and consider the subring

$$R = \{p(x) = \sum_{i,j \in \mathbf{Z}_{\geq 0}, i+j \in 2\mathbf{Z}} a_{i,j} x^i y^j : a_{i,j} \in F\}$$

of $F[x, y]$. Prove that x^2 is irreducible in R but is not prime in R.

3. Let F be a field. Show that $F[x, y]$ is not a principal ideal domain.

4. Note that by Example 2.7.5 of Ash, $R = \mathbf{Z}[i]$ is a Euclidean domain. In this exercise and the next, we will compute the nonzero primes of R and relate them to the problem of determining whether a prime number in $\mathbf{Z}$ is a sum of two squares. We call a prime of R a Gaussian prime, and a prime of $\mathbf{Z}$ an integral prime.

(a) Let $\pi = a + bi \in R$ be a prime of R. Define $N(\pi) = \pi \cdot \overline{\pi}$, and prove that $N(\pi)$ is either p or p^2, where p is a prime of $\mathbf{Z}$. Moreover, if π is not associate to a prime element of $\mathbf{Z}$, then prove $N(\pi) = p$ is a prime of $\mathbf{Z}$ (hint: let $N(\pi) = n$, and factor n as a product of primes in $\mathbf{Z}$).

(b) Let $p = 4k + 3$ be a prime of $\mathbf{Z}$. Then $p \neq a^2 + b^2$ for any $a, b \in \mathbf{Z}$, and p is prime in $\mathbf{Z}[i]$ (hint: compute each side modulo 4).

(c) Factor 2 as a product of Gaussian primes. Write 2 as a sum of two squares.

5. Continuing notation of problem 5:

(i) Let $p = 4k + 1$ be a prime integer and for $a \in \mathbf{Z}$, let $\overline{a} = a \pmod{p} \in \mathbf{Z}_p$. Show that there is $a \in \mathbf{Z} - p\mathbf{Z}$ such that the order of $\overline{a} \in \mathbf{Z}_p^*$ is 4 (hint: let $G = \mathbf{Z}_p^*/N$, where $N = \{\pm 1\}$. Show there is $\alpha \in G$ of order 2, and choose $\overline{a} \in \mathbf{Z}_p^*$ such that $\alpha = \overline{a}N$. Prove that $\overline{a}$ has order 4 in $\mathbf{Z}_p^*$).

(ii) Using notation of (i), Prove that p divides $a^2 + 1$. Prove that p is not a Gaussian prime (hint: use definition of prime, and $a^2 + 1 = (a + i)(a - i)$).

(iii) Prove that if $\pi = a + bi$ is a Gaussian prime factor of $p = 4k + 1$, then $p = N(\pi) = a^2 + b^2$.

(iv) Prove that up to multiplication by units, the Gaussian primes are :

(1) p, where $p = 4k + 3$ is an integral prime.

(2) $1 + i$

(3) $\pi = a \pm bi$, where $a^2 + b^2 = p$ is congruent to 1, modulo 4, and p is an integral prime.

6-7. Let R be a unique factorization domain, and let $\{\mathfrak{p}_i : i \in I\}$ be the collection of nonzero principal prime ideals of R. For each $\mathfrak{p}_i$, choose $p_i \in R$ so that $\mathfrak{p}_i = (p_i)$, and let $\mathcal{P} = \{p_i : i \in I\}$. Recall that if $a \in R$ is nonzero, we can write a in the form $a = u \cdot p_{i_1}^{e_{i_1}} \cdots p_{i_k}^{e_{i_k}}$, with $p_{i_j} \in \mathcal{P}$, $k \geq 0$, and $e_{i_j} \geq 0$.. Let F be the fraction field of R, and if $\alpha \in F^\times$, we can write $\alpha = \frac{a}{b} p^e$ with $a, b \in R$ and p divides neither a nor b. We define $v_p(\alpha) = e$ and recall that v_p is independent of choices, and define $v_p(0) = \infty \geq e$ for all $e \in \mathbf{Z}$. Let $f = a_0 + a_1 x + \cdots + a_n x^n$ be a nonzero polynomial in $F[x]$, and for $p \in \mathcal{P}$, let $v_p(f)$ be the minimum of $\{v_p(a_i) : i = 0, \ldots, n\}$.

Prove the following assertions.

(1) If $\alpha = \frac{a}{b} \in F^\times$, then $c(\alpha) = \prod p_i^{\mathrm{ord}_{p_i}(\alpha)}$, where the product is over primes $p_i \in \mathcal{P}$ such that p_i divides a or b.

(2) $c(\alpha \cdot f) = c(\alpha) \cdot c(f)$.

(3) $c(c(\alpha)) = c(\alpha)$.

(4) $c(f) \in R$ if and only if $f \in R[x]$.

(5) $c(\alpha) = u \cdot \alpha$, for some $u \in R^*$. In particular, for $\alpha \in R$, $c(\alpha) = 1$ if and only if $\alpha \in R^*$.

(6) If $\beta \in F^\times$, then $c(\alpha \cdot \beta) = c(\alpha) \cdot c(\beta)$ (hint: use Exercise 0.7(1)).

8. Let R be a principal ideal domain. Let p in R be prime, and let $R_{(p)} = S^{-1}R$, where $S = R - (p)$. Show that $R_{(p)}$ is isomorphic to a subring of the fraction field of R. Prove that $R = \cap R_{(p)}$, where the intersection is over all primes p of R, and takes place in the fraction field F of R (hint: the general case is not very different from the case where $R = \mathbf{Z}$).

9. Let R be an integral domain with multiplicative subset S. Let $f : R \to S^{-1}R$ be the ring homomorphism $f(a) = \frac{a}{1}$.

(i) For an ideal I of R, let $S^{-1}I = \{\frac{a}{s} : a \in I, s \in S\}$. Prove that $S^{-1}I$ is an ideal of $S^{-1}R$.

(ii) For a ring A, let $Spec(A)$ denote the set of prime ideals of A. Define $f^* : Spec(S^{-1}R) \to Spec(R)$ by $f^*(P) = f^{-1}(P)$. Prove that if P is a prime of $S^{-1}R$, then $S^{-1}f^*(P) = P$, f^* is injective, and the image $Im(f^*) = \{P \in Spec(R) : P \cap S = \emptyset\}$.

(iii) If $S = R - P$, where P is a prime ideal of R, prove that $S^{-1}P$ is the unique maximal ideal of $S^{-1}R$.

10. Let $R = \mathbf{Z}$, and let p be prime in $\mathbf{Z}$. Let $S = \{p^n : n \geq 0\}$. Prove that

$$S^{-1}\mathbf{Z} \cong \{\frac{a}{p^k} \in \mathbf{Q} : k \geq 0\}.$$

11. Let F be a field, and consider the integral domain $R = F[[x]]$. Show that the fraction field $Frac(R)$ of R coincides with the subset $\{\frac{a}{x^n} : a \in F[[x]]\}$ of $Frac(R)$.

12. Let $R = \mathbf{Z}/12\mathbf{Z}$. For $a \in \mathbf{Z}$, denote also by a the equivalence class of $a \in R$.

(i) If $S = \{1, 3, 9\}$, prove that $S^{-1}R \cong \mathbf{Z}/4\mathbf{Z}$.

(ii) If $S = \{1, 4\}$, find m so that $S^{-1}R \cong \mathbf{Z}/m\mathbf{Z}$.

(iii) If $R = \mathbf{Z}/n\mathbf{Z}$. Let p be a prime factor of n and assume p^k divides n but p^{k+1} does not divide n. Let $a = p^k \pmod{n}$, and let $S = \{a^t : t \in \mathbf{Z}_{\geq 0}\}$. Conjecture a formula for $S^{-1}R$. You do not need to prove your conjecture.

13. (i) Find an irreducible polynomial of degree 3 in $\mathbf{Z}_2[x]$ and construct a field with 8 elements.

(ii) Construct a field with 25 elements and a field with 49 elements.