Honors Algebra 4, MATH 371 Winter 2010

Assignment 3

Due Friday, February 5 at 08:35

1. Let $R \neq 0$ be a commutative ring with 1 and let $S \subseteq R$ be the subset of nonzero elements which are not zero divisors.

   (a) Show that S is multiplicatively closed.

   (b) By definition, *the total ring of fractions of* R is the ring $\mathrm{Frac}(R) := S^{-1}R$; it is a ring equipped with a canonical ring homomorphism $R \to S^{-1}R$. If T is any multiplicatively closed subset of R that is contained in S, show that there is a canonical injective ring homomorphism $T^{-1}R \to \mathrm{Frac}(R)$, and conclude that $T^{-1}R$ is isomorphic to a subring of $\mathrm{Frac}(R)$.

   (c) If R is a domain, prove that $\mathrm{Frac}(R)$ is a field and hence that $T^{-1}R$ is a domain for any T as above.

   Solution:

   (a) If a, b are nonzero and are not zero-divisors, then ab can't be zero on the one hand, and can't be a zero divisor on the other since if $sab = 0$ then $(sa)b = 0$ which forces $sa = 0$ as b is not a zero divisor, and this forces $s = 0$ as a is not a zero divisor.

   (b) Because $T \subseteq S$, under the canonical map $\varphi : R \to S^{-1}R$, every element of T maps to a unit. Thus, this map uniquely factors as the composite of the canonical map $R \to T^{-1}R$ with a unique ring homomorphism $\psi : T^{-1}R \to S^{-1}R$. If r/t maps to zero, then there exists $s \in S$ with $sr = 0$. But s must be nonzero and not a zero divisor, whence we must have $r = 0$ and hence $r/t = 0$. We conclude that ψ is injective, hence an isomorphism onto its image, which is a subring of $S^{-1}R$.

   (c) If R is a domain, then $S = R \setminus 0$ and every nonzero element of $S^{-1}R$ is invertible (If $r/s \neq 0$ then in particular $r \neq 0$ and hence $r \in S$ so $s/r \in S^{-1}R$ and is the inverse of r/s). Thus, $S^{-1}R$ is a field. Since any subring of a field is necessarily a domain, we conclude as desired.

2. Let R be a commutative ring with 1.

   (a) Let $S \subseteq R$ be a multiplicatively closed subset. Prove that the prime ideals of $S^{-1}R$ are in bijective correspondence with the prime ideals of R whose intersection with S is empty.

   (b) If $\mathfrak{p}$ is an ideal of R, show that $S := R \setminus \mathfrak{p}$ is a multiplicatively closed subset if and only if $\mathfrak{p}$ is a prime ideal. Writing $R_{\mathfrak{p}}$ for the ring of fractions $S^{-1}R$, show that $R_{\mathfrak{p}}$ has a unique maximal ideal, and that this ideal is the image of $\mathfrak{p}$ under the canonical ring homomorphism $R \to R_{\mathfrak{p}}$. (In other words, the *localization of* R *at* $\mathfrak{p}$ is a *local ring*).

(c) Let $r \in R$ be arbitrary. Show that the following are equivalent:

i. $r = 0$

ii. The image of r in $R_{\mathfrak{p}}$ is zero for all prime ideals $\mathfrak{p}$ of R.

iii. The image of r in $R_{\mathfrak{p}}$ is zero for all maximal ideals $\mathfrak{p}$ of R.

Solution:

(a) Denote by $\varphi : R \to S^{-1}R$ the canonical map. If $\mathfrak{p}$ is a prime ideal of R not meeting S, we claim that

$$S^{-1}\mathfrak{p} := \{x/s \ : \ x \in \mathfrak{p}, \ s \in S\}$$

is a prime ideal of $S^{-1}R$. Indeed, if $(r_1/s_1)(r_2/s_2) = x/s \in S^{-1}\mathfrak{p}$ then there exists $t \in S$ with

$$t(sr_1r_2 - s_1s_2x) = 0$$

in R. Since x and 0 lie in $\mathfrak{p}$, we conclude that $tsr_1r_2 \in \mathfrak{p}$. Since $S \cap \mathfrak{p} = \emptyset$, it follows that $r_1r_2 \in \mathfrak{p}$ whence $r_1 \in \mathfrak{p}$ or $r_2 \in \mathfrak{p}$ as $\mathfrak{p}$ is prime. It follows that $S^{-1}\mathfrak{p}$ is prime.

Conversely, if $\mathfrak{p}$ is a prime ideal of $S^{-1}R$ then $\varphi^{-1}\mathfrak{p}$ is a prime ideal of R by a previous homework, and it remains to show that for any prime ideal $\mathfrak{p}$ of R, we have

$$\varphi^{-1}(S^{-1}\mathfrak{p}).$$

If $\varphi(r) = x/s$ lies in $S^{-1}\mathfrak{p}$ then $t(rs - x) = 0$ for some $t \in S$. Arguing as above, we conclude that $r \in \mathfrak{p}$.

(b) The first part follows immediately from the definition of prime. The second follows easily from (2a) since the prime ideals of R not meeting $S := R \setminus \mathfrak{p}$ are exactly the prime ideals of R contained in $\mathfrak{p}$.

(c) Clearly (i) $\implies$ (ii) $\implies$ (iii). If R is the zero ring then the equivalence is obvious, so we may assume that R is nonzero. Let $x \in R$ and denote by

$$\mathrm{ann}(x) := \{r \in R \ : \ rx = 0\}$$

the *annihilator* of x in R; it is easily seen to be an ideal of R. Suppose that the image of x in $R_{\mathfrak{p}}$ is zero for all maximal ideals $\mathfrak{p}$ If $\mathrm{ann}(x)$ is not the unit ideal, then there exists a maximal ideal $\mathfrak{p}_0$ containing $\mathrm{ann}(x)$. However, our hypothesis on x implies that then there exists $s \in R \setminus \mathfrak{p}_0$ with $sx = 0$, i.e. $\mathrm{ann}(x)$ is not contained in $\mathfrak{p}_0$ which is a contradiction. It follows that $1 \in \mathrm{ann}(x)$ and hence that $x = 0$.

3. Do exercises 8–11 in §7.6 of Dummit and Foote (inductive and projective limits).

Solution: This is important stuff, but extremely tedious to write up in TEX. If you have any questions about it, I'll be more than happy to discuss.

4. A *Bézout domain* is an integral domain in which every finitely generated ideal is principal.

(a) Show that a Bézout domain is a PID if and only if it is noetherian.

(b) Let R be an integral domain. Prove that R is a Bezout domain if and only if every pair of elements $a, b \in R$ has a GCD $d \in R$ that can be written as an R-linear combination of a and b, *i.e.* such that there exist $x, y \in R$ with $d = ax + by$.

(c) Prove that a ring R is a PID if and only if it is a Bézout domain that is also a UFD.

(d) Let R be the quotient ring of the polynomial ring $\mathbf{Q}[x_0, x_1, \ldots]$ over $\mathbf{Q}$ in countably many variables by the ideal I generated by the set $\{x_i - x_{i+1}^2\}_{i \geq 0}$. Show that R is a Bézout domain which is not a PID (Hint: have a look at Dummit and Foote, §9.2 # 12).

Remark: The above example of a Bézout domain which is not a PID is somewhat artificial. More natural examples include the "ring of algebraic integers" (*i.e.* the set of all roots of monic irreducible polynomials in one variable over $\mathbf{Z}$) and the ring of holomorphic functions on the complex plane. The proofs that these are B'ezout domains is, as far as I know, difficult. For example, in the case of the algebraic integers, one needs the theory of class groups).

Solution:

(a) Easy unravelling of definitions.

(b) If R is a Bézout domain then the finitely generated ideal (a, b) is principal, say with generator d, whence there exist x and y with $ax + by = d$. Clearly d is a GCD of a and b. Conversely, suppose R has a GCD algorithm of the type described, and that I is an ideal of R generated by $a_1, \ldots, a_n$. Let d be a gcd of a_1 and a_2. Then by definition of GCD, we have $a_1 \in (d)$ and $a_2 \in (d)$ whence $I \subseteq (d, a_3, \cdots, a_n)$. Since also we have $d = a_1 x + a_2 y$, we get the reverse inclusion and R can be generated by $n - 1$ elements. By descent on n, we deduce that I is principal and hence that R is Bézout.

(c) We have seen that PID implies UFD and Bézout. Conversely, suppose that R is a Bézout UFD and let I be a nonzero ideal of R. For each irreducible element r of R, denote by e_r the minimal exponent of r occurring in the unique factorizations of nonzero elements of I and write b_r for any element of I realizing this exponent of r. Clearly $e_r = 0$ for all but finitely many r, say for $r_1, \ldots, r_n$.

An easy induction using (4b) shows that there exists a GCD d of $b_{r_1}, \ldots, b_{r_n}$ which may be expressed as an R-linear combination

$$d = x_i b_{r_1} + \cdots + x_n b_{r_n},$$

so $d \in I$. On the other hand, the exponent of r_i in d is at most e_{r_i} since $d | b_{r_i}$ whence it must be exactly r_i by minimality. If $a \in I$ is not divisible by d then there is some i for which the exponent of r_i in the unique factorization of a is strictly less than e_{r_i}, a contradiction to the minimality of the e_{r_i}. Thus $I \subseteq (d)$ and we must then have $I = (d)$ is principal.

(d) For each i, we have an injective $\mathbf{Q}$-algebra homomorphism $\varphi_i : \mathbf{Q}[x_i] \to R$ given by sending x_i to x_i. We write $\psi_i : \mathbf{Q}[x_i] \to \mathbf{Q}[x_{i+1}]$ for the $\mathbf{Q}$-algebra himomorphism taking x_i to x_{i+1}^2, so that

$$\varphi_i \circ \psi_i = \varphi_{i+1}$$

and note that ψ_i is injective. Write $R_i := \mathrm{im}(\phi_i)$; it is a subring of R that is isomorphic to $\mathbf{Q}[x_i]$ and is hence a PID. Moreover, the mappings ψ_i give ring inclusions $R_i \subseteq R_{i+1}$ and it is easy to see from the very definition of R that $R = \cup_{i=1}^{\infty} R_i$. We conclude immediately that R is Bézout: indeed, any finitely generated ideal of R is contained in some R_i (as this is the case for each of its generators, and the R_i form a chain) and each R_i is principal. I claim that the ideal M generated by all x_i can not be finitely generated. There are probably a billion ways to see this, so I'll just pick one that comes to mind: For each i, denote by $2^{1/2^i}$ the unique positive 2^i th root of 2 in $\overline{\mathbf{Q}}$ and consider the $\mathbf{Q}$-algebra homomorphism $\mathbf{Q}[x_0, x_1, \ldots] \to \overline{\mathbf{Q}}$ sending x_i to $2^{1/2^i}$. Clearly, I is in the kernel of this map so we get a homomorphism of $\mathbf{Q}$-algebras $\Psi : R \to \overline{\mathbf{Q}}$. If M were finitely generated, the image of Ψ would be a finitely generated $\mathbf{Q}$-subalgebra of $\overline{\mathbf{Q}}$ and in particular would be $\mathbf{Q}$-vector space of finite dimension $d < \infty$. It follows that any element of the image would satisfy a polynomial with rational coefficients having degree at most d. But this image contains $2^{1/2^i}$, which can not satisfy a polynomial with $\mathbf{Q}$-coefficients of degree less than 2^i. Indeed, on the one hand $2^{1/2^i}$ is a root of $F_i := T^{2^i} - 2$, which is irreducible over $\mathbf{Q}$ be Gauss's Lemma and Eisenstein's criterion applied with $p = 2$. On the other hand, if g is any nonzero polynomial of minimal degree satisfied by $2^{1/2^i}$, then by the division algorithm we have $F_i = gq + r$ for some rational polynomials q and r with $\deg r < \deg g$ whence $r = 0$ by minimality and $F_i = gq$. As F_i is irreducible, we conclude that q is a unit and hence an element of $\mathbf{Q}^\times$ so $\deg(g) = 2^i$.

5. Let $R = \mathbf{Z}[i] := \mathbf{Z}[X]/(X^2 + 1)$ be the ring of *Gaussian integers*.

(a) Let $N : R \to \mathbf{Z}_{\geq 0}$ be the *field norm*, that is

$$N(a + bi) := (a + bi)(a - bi) = a^2 + b^2.$$

Prove that R is a Euclidean domain with this norm. Hint: there is a proof in the book on pg. 272, but you should try to find a different proof by thinking *geometrically*.

(b) Show that N is multiplicative, *i.e.* $N(xy) = N(x)N(y)$ and deduce that $u \in R$ is a unit if and only if $N(u) = 1$. Conclude that $R^\times$ is a cyclic group of order 4, with generator $\pm i$.

(c) Let $p \in \mathbf{Z}$ be a (positive) prime number. If $p \equiv 3 \bmod 4$, show that p is prime in $\mathbf{Z}[i]$ and that $\mathbf{Z}[i]/(p)$ is a finite field of characteristic p which, as a vector space over $\mathbf{F}_p$, has dimension 2.

If $p = 2$ or $p \equiv 1 \bmod 4$, prove that p is not prime in $\mathbf{Z}[i]$, but is the norm of a prime $\mathfrak{p} \in \mathbf{Z}[i]$ with $\mathbf{Z}[i]/(\mathfrak{p})$ isomorphic to the finite field $\mathbf{F}_p$. Conclude that $p \in \mathbf{Z}$ can be written as the sum of two integer squares if and only if $p = 2$ or $p \equiv 1 \bmod 4$.

Solution:

(a) In the complex plane, $\mathbf{Z}[i]$ corresponds to the integer lattice consisting of all points (a, b) with integral coordinates. The norm of an element $a + bi$ is precisely the square of the Euclidean distance from the origin to the point (a, b) corresponding to $a + bi$. Suppose now that $x = c + di$ and $y = a + bi$ are Gaussian integers with $y \neq 0$. The quotient x/y (as complex numbers) is located inside (or on the perimeter of) a unit square in the complex plane whose vertices have integral coordinates. The minimal (Euclidean) distance from x/y to a vertex of this square is at most half the diagonal of the square, or $\sqrt{2}/2$. We conclude that there exist a Gaussian integer q (a vertex of minimal distance) with

$$N(\frac{x}{y} - q) \leq (\frac{\sqrt{2}}{2})^2$$

or in other words, there exist Gaussian integers q and $r := x - yq$ with

$$x = yq + r \quad \text{and} \quad N(r) \leq \frac{1}{2}N(y) < N(y)$$

so we indeed have a division algorithm and $\mathbf{Z}[i]$ is Euclidean.

(b) The multiplicativity of N is a straightforward (albeit tedious) calculation. By definition $u \in \mathbf{Z}[i]$ is a unit if there exists $v \in \mathbf{Z}[i]$ with $uv = 1$; taking norms gives $N(u)N(v) = 1$ so since N is nonnegative we conclude that $N(u) = 1$. Conversely, if $u = a + bi$ satisfies $N(u) = 1$, then

$$1 = N(u) = (a + bi)(a - bi)$$

so u is a unit. It's easy to see that the only integer solutions to $a^2 + b^2 = 1$ are the 4 points $(a, b) = (\pm 1, 0), (0, \pm 1)$ corresponding to $\pm 1, \pm i$. Since $(\pm i)^2 = -1$ we conclude that $\mathbf{Z}[i]^\times$ is cyclic of order 4 generated by $\pm i$.

(c) Let p be a prime of $\mathbf{Z}$. If

$$p = (a + bi)(c + di)$$

then taking norms gives $p^2 = (a^2+b^2)(c^2+d^2)$ so if neither $a+bi$ nor $c+di$ is a unit then we deduce that $p = a^2 + b^2$ for integers a and b. If $p \equiv 3 \bmod 4$ then reducing this equation modulo 4 implies that $3 = a^2 + b^2$ has a solution in $\mathbf{Z}/4\mathbf{Z}$ which it obviously doesn't (by inspection, sums of squares in $\mathbf{Z}/4\mathbf{Z}$ can be $0, 1, 2$ only). Thus any factorization of $p \equiv 3 \bmod 4$ in $\mathbf{Z}[i]$ as above has one of the two factors a unit; we conclude that p is irreducible and hence prime and hence maximal (we're in a Euclidean domain after all). The quotient $\mathbf{Z}[i]/(p)$ is therefore a field which is also an $\mathbf{F}_p$-vector space. Using the isomorphism $\mathbf{Z}[i] \simeq \mathbf{Z}[X]/(X^2+1)$ and the third isomorphism theorem for rings, we have

$$\mathbf{Z}[i]/(p) \simeq (\mathbf{Z}[X]/(p))/(x^2+1) = \mathbf{F}_p[X]/(X^2+1)$$

which as an $\mathbf{F}_p$-vector space has basis $1, X$ so is of dimension 2.

If $p \equiv 1 \bmod 4$ we claim that -1 is a square modulo p. Indeed, the group of units $\mathbf{F}_p^\times$ is cyclic of order $p-1$ (proof?) so for any generator u we have $u^{p-1} = 1$ in $\mathbf{F}_p$. It follows that $u^{(p-1)/2} = \pm 1$ and we must have the negative sign since u is a generator. Since $p \equiv 1 \bmod 4$ so $(p-1)/2$ is even, we conclude that -1 is a square mod p. Thus, the equation

$$x^2 + 1 = py$$

has a solution for integers x, y. If p were prime in $\mathbf{Z}[i]$ then we would have

$$p|(x-i)(x+i)$$

which would force $p|(x-i)$ or $p|(x+i)$ both of which are absurd. Thus, p is not prime in $\mathbf{Z}[i]$ and we have a factorication

$$p = (a+bi)(c+di)$$

with the norm of each factor strictly bigger than 1. Taking norms, we conclude that $p = N(a+bi)$. Moreover, $\mathfrak{p} := (a+bi)$ must be prime in $\mathbf{Z}[i]$ as is easily seen by taking norms. Similarly, $(a-bi)$ is prime.

It is easy to see that the two prime ideals $(a+bi)$ and $(a-bi)$ are co-maximal as the ideals (a) and (b) of $\mathbf{Z}$ must be comaximal (why?) and hence by the Chinese Remainder Theorem we have

$$\mathbf{Z}[i]/(p) = \mathbf{Z}[i]/(a+bi) \times \mathbf{Z}[i]/(a-bi).$$

The ring $\mathbf{Z}[i]/(p) \simeq \mathbf{Z}[X]/(p, x^2+1) \simeq \mathbf{F}_p[X]/(X^2+1)$ is a vector space of dimension 2 over $\mathbf{F}_p$ and hence has cardinality p^2. It follows easily from this that $\mathbf{Z}[i]/(a+bi)$ and $\mathbf{Z}[i]/(a-bi)$ each have cardinality p and so the canonical map of rings $\mathbf{F}_p \to \mathbf{Z}[i]/(a+bi)$ must be an isomorphism.

To handle 2, we argue as above using that $2 = (1+i)(1-i)$. We conclude that p is a sum of integer squares if and only if p is 2 or $p \equiv 1 \bmod 4$.