

Math 593 Exam I Fall 2005

0. Write your name on all papers you turn in (5 points).

1. TRUE OR FALSE. No explanation needed. (15 points)

F a). Every UFD is a PID.

T b). The polynomial $x^{17} + 17x^7 + 17x + 17$ is irreducible in $\mathbb{Z}[x]$.

T c). The ideal generated by x in the polynomial ring $\mathbb{Z}[x, y]$ is prime.

T d). Let R be the ring of continuous \mathbb{R} -valued functions on the interval $[0, 1]$. Then the subset of functions vanishing at $1/2$ is a maximal ideal of R .

F e). In the ring $\mathbb{Z}[\sqrt{7}]$, the element 7 generates a prime ideal.

T f). There is a ring isomorphism $\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

F g). If R is a UFD, so is R/I for any ideal I .

T h). If R is a domain, so is the polynomial ring $R[x]$.

T i). If I and J are ideals of R , so is $I \cap J$.

F j). If I and J are ideals of R , so is $I \cup J$.

T k). The polynomial ring $k[x_1, x_2, \dots, x_n]$ is a UFD, where k is a field.

F l). There is a ring isomorphism $\mathbb{Z}/25\mathbb{Z} \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

F m). Some abelian groups can not be given a \mathbb{Z} -module structure.

T n). The group ring $\mathbb{Z}G$ commutative if and only if the group G is abelian.

T o). In $R[x]$, the ideals $(x + 1)$ and (x) are comaximal (where R is any commutative ring).

2. a). Let R be a Euclidean domain, and say that m is the minimum integer in the set of norms of non-zero elements of R . Prove that any non-zero element of norm m is a unit in R .

Fix non-zero x with $N(x) = m$. Then write $1 = xq + r$ where $r = 0$ or $N(r) < N(x)$. By minimality assumption on $N(x)$, we conclude $r = 0$, so q is the inverse of x and x is a unit.

b). Prove that every Euclidean domain is a PID.

Fix an ideal I in R . Let x be an element of minimal norm from among all elements of I . We claim $I = (x)$. Clearly $(x) \subset I$. For any $y \in I$, write $y = qx + r$, where $r = 0$ or $N(r) < N(x)$. Since $r = y - qx \in I$, the minimality assumption on $N(x)$ forces $r = 0$. So $y \in (x)$ and $I = (x)$.

3. Let R be a PID, let (f) be any non-zero proper ideal of R , and for an element g in R , let \bar{g} denote the image of g under the natural quotient map $R \rightarrow R/(f)$.

a). Prove that \bar{g} is a unit in $R/(f)$ if and only if $(f, g) = 1$.

We have $(f, g) = 1$ if and only if there exist a, b in R such that $af + bg = 1$. Modulo (f) , this holds if and only if $\bar{b}\bar{g} = 1$, that is, if and only if \bar{g} is a unit modulo in $R/(f)$.

b). Prove that the number of (proper) prime ideals in $R/(f)$ is equal to the number of distinct irreducible elements appearing in a factorization of f into irreducibles.

The ideals of $R/(f)$ are in one-one correspondence with the ideals of R containing (f) . If $(f) \subset I$, then also $\frac{R/(f)}{I/(f)} \cong R/I$, so under this correspondence, the prime ideals of $R/(f)$ are in one-one correspondence with the prime ideals of R containing (f) (using the fact that P is prime if and only if R/P is a domain). So we want to count the prime ideals of R containing (f) . Note also that the prime ideals in a PID are precisely those generated by irreducible elements.

Factor $f = g_1^{a_1} g_2^{a_2} \dots g_n^{a_n}$ uniquely (up to unit multiple and permutation) where the g_i are distinct irreducibles. If $f \in P$, a prime of R , the definition of primeness forces some $g_i \in P$. But since the irreducible elements generate maximal ideals in a PID, it follows that $(g_i) = P$. Clearly also each (g_i) is a prime ideal containing f . By uniqueness of the factorization of f , there are no other possibilities for an irreducible element g to generate a prime ideal of R containing (f) . Furthermore, the (g_i) are all distinct since $(g_i) = (g_j)$ forces g_i and g_j to differ by unit multiple. Thus the prime ideal of $R/(f)$ are the n distinct ideals generated by the images of the g_i in $R/(f)$.

4. Let R be a commutative ring. The characteristic of R is defined to be the non-negative integer n generating the kernel of the natural ring map $\mathbb{Z} \rightarrow R$ sending 1 to the identity element of R .

a). Determine the characteristic of the following five rings:

$\mathbb{Z}/(n)$; characteristic n

$\mathbb{Q}[x]$; characteristic 0

$\mathbb{Q}[x, y]/(xy)$; characteristic 0

$\mathbb{F}[[x]]$ where \mathbb{F} is a field of two elements; characteristic 2

the p -adic numbers \mathbb{Z}_p ; characteristic 0

b). Prove that the characteristic of a field must be a prime number, or zero.

We have an injection $\mathbb{Z}/(\ker\phi) \hookrightarrow R$ where ϕ is the natural map described above. Thus if R is a field (or any domain), then so is the subring $\mathbb{Z}/(\ker\phi)$. Hence $\ker\phi$ is either (0) or (p) , whence the characteristic is zero or p , where p is a prime number.

c). If R has characteristic p , where p is a prime number, prove that the p -th power map

$$R \rightarrow R; \quad r \mapsto r^p$$

is a ring homomorphism. (This is the famous and very important Frobenius map; nothing like this is true in characteristic zero.)

The map obviously takes 1 to 1, and rs to $(rs)^p = r^p s^p$ (by commutativity), so preserves the multiplicative structure of R in any characteristic. On the other hand, $(r+s)^p = \sum_{i=0}^p \binom{p}{i} r^i s^{p-i}$, where for an integer n and $x \in R$, the product nx can be interpreted via the natural \mathbb{Z} -module action on R given by the natural map $\mathbb{Z} \rightarrow R$ above. Now, by definition, $\binom{p}{i} = \frac{p!}{i!(p-i)!}$, so if $1 \leq i \leq p-1$, it is clear by the unique factorization property in \mathbb{Z} that the integer p divides $\binom{p}{i}$. Since R has characteristic p , this means that the integers $\binom{p}{i}$ act by zero on R for all $1 \leq i \leq p-1$. Hence the middle terms of the expression for $(r+s)^p$ are all zero and we see that $(r+s)^p = r^p + s^p$. Thus the p -th power map preserves the additive structure in prime characteristic as well.

5. a). Fix a commutative ring A . Note that for positive integers $n \geq m$, there is a natural map of rings $A[x]/(x^n) \rightarrow A[x]/(x^m)$. Let $R = \varprojlim A[x]/(x^n)$ be the inverse limit of these maps. Find a natural ring homomorphism $A[[x]] \rightarrow R$ and prove that it is an isomorphism.

To give a map from $A[[x]]$ to R is equivalent to giving maps from $A[[x]]$ to each $A[x]/(x^i)$, compatible with the natural maps that make up the inverse limit system (this is the universal property of inverse limits discussed in Exercise 7.6.10d). The truncation maps $A[[x]] \rightarrow A[x]/(x^n)$ sending a power series $\sum a_i x^i$ to $\sum_{i=0}^{n-1} a_i x^i$ modulo (x^n) clearly have this property. This gives the map $A[[x]] \rightarrow R$.

Explicitly, we can define $A[[x]] \rightarrow R$ by sending a formal power series $\sum a_i x^i$ to the string of elements

$$(\overline{a_0} \leftarrow \overline{a_0 + a_1 x} \leftarrow \dots \overline{a_0 + a_1 x + \dots + a_{i-1} x^{i-1}} \leftarrow \dots)$$

in the direct product $\prod_i A[x]/x^i$. It is clear that this element lies in the subring R , since $a_0 + a_1 x + \dots + a_{n-1} x^{n-1}$ modulo (x^m) is $a_0 + a_1 x + \dots + a_{m-1} x^{m-1}$ whenever $n \geq m$. It is also clear that this map is a ring homomorphism, since the sum and product are defined coordinatewise by usual sum or product of power series modulo (x^i) .

To see that this map is an isomorphism, we use the fact that each equivalence class of $A[x]/(x^i)$ has a unique representative by a polynomial of degree less than i . These can be thought of as the "partial sums"

for the infinite power series $\sum a_i x^i$. So if each of these partial sums is zero, then all a_i are zero, and $\sum a_i x^i$ is zero. Similarly, the surjectivity follows, since the any element of R is uniquely represented by

$$(a_0, a_0 + a_1 x, \dots, a_0 + a_1 x + \dots + a_{i-1} x^{i-1} \dots) \in \prod_{i=1}^{\infty} A[x]$$

which is the image of the infinite power series $\sum a_i x^i$.

b). Let

$$S = \varprojlim \mathbb{Z}/(10^n \mathbb{Z})$$

where the maps are the natural projections. Prove that there is a ring isomorphism $S \cong \mathbb{Z}_2 \times \mathbb{Z}_5$, where \mathbb{Z}_p denotes the ring of p -adic numbers.

Define a map

$$R \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_5; (\bar{a}_i)_{a_i \in \mathbb{Z}/(10^i)} \mapsto (\bar{a}_i \bmod 2^i) \times (\bar{a}_i \bmod 5^i).$$

This map is well defined because the corresponding maps

$$\mathbb{Z}/(10^i) \rightarrow \mathbb{Z}/(2^i) \times \mathbb{Z}/(5^i)$$

are well-defined and commute with the maps given by the inverse limit system. (This last condition is crucial; it ensures that the image of an element $(\bar{a}_i) \in R$ is not an arbitrary element of the direct product $(\prod_i \mathbb{Z}/(2^i)) \times (\prod_i \mathbb{Z}/(5^i))$, but really lies in the proper subring of the inverse limit). Now the Chinese Remainder theorem ensures that, because $(2^i, 5^i) = 1$ for all i , this map is in fact a bijection. Hence it is an isomorphism, and the proof is complete.