Mathematics 371 Fall, 2012 (SHATZ)

Assignment # 4, due Nov. 13, 2012

Part A

AI) In class, we showed that for a ring the two statements below are equivalent:

① Every strictly ascending chain of principal ideals must stop.

② Every non-empty family of principal ideals has maximal elements.

Copy these arguments (suitably changed) to show that the following three statements are equivalent in a ring:

ⓐ Every ideal is finitely generated

ⓑ Every strictly ascending chain of ideals must stop

ⓒ Every non-empty family of ideals has maximal elements.

Remark. You need only show ⓐ ⇒ ⓑ, ⓑ ⇒ ⓒ, and ⓒ ⇒ ⓐ. You should be prepared to explain why only these three implications need be proved.

AII) 378/1.3

AIII) 378/1.5

AIV) 379/2.9, 2.10

AV) 380/4.8

Part B

BI). The additive group of a ring is always abelian and the simplest abelian groups are cyclic. Let C be a cyclic group (under +) and write e for a generator of C. The elements of C are then $\pm ke$, with $k \in \mathbb{Z}$, $k \geq 0$ (case when C is infinite) or $0, e, 2e, \ldots, (n-1)e$, if C is finite of order n. We investigate here the various ways C can be given a multiplication to make it a ring.

a) Show that if C is to be a ring all we need to know is which element of C equals e^2. So, say $e^2 = le$ + write $C(l)$ for the corresponding ring with C as + group + mult given by $e^2 = le$.

b) Now assume C is infinite. Is there any restriction on l in order that $C(l)$ be a ring? If we want $C(l)$ to be a ring with unity, is there a restriction on l? Be explicit. Can $C(l)$ be isomorphic to $C(\lambda)$, for which l and λ? (Here, we don't necessarily have a ring with unity.)

c) Here, we assume $C(l)$ $(0 \leq l \leq n-1)$ is finite of size n. Show that the element ke is another generator of C if and only if k and n are relatively prime. Now say we fix the generator e and look at $C(l)$, $C(\lambda)$ (here, $0 \leq l, \lambda \leq n-1$), the two rings given by $e \cdot e = le$ and $e * e = \lambda e$. ($*$ is the mult in $C(\lambda)$.) What is the condition on l and λ in order that there be an isomorphism $\varphi: C(l) \to C(\lambda)$?

(OVER)

d) Next, assume we want $C(\ell)$ to have a unit element. Exactly what is the condition on ℓ in order that this be true? What is the unit element for mult. when this holds (it is some multiple of e, which one?)? (Of course if d is this unit element, then $d^2 = d$.) Show that d must generate C as an additive group.

e) Lastly, say $n = p$ or pq where p, q are distinct prime numbers. Completely classify all the possible $C(\ell)$ up to isomorphism.

BII) In class, we showed that a PID has the following three properties:

① Every ideal is finitely generated (this is a tautology because in a PID every ideal has one generator).

② Any two elements have a g.c.d.

③ If a, b are given, their g.c.d. is a linear combination $(sa+tb)$ of a and b.

Assume R is an integral domain and satisfies ①, ② ③ above. Prove that R is a P.I.D. (There will be an induction step in your proof, do it correctly.)

BIII) In class we constructed for each integral domain, R, its fraction field, $\mathrm{Frac}(R)$. Now assume we don't necessarily have a domain, just

suppose a commutative ring with unity — call it R, again. Inside R we have a subset, S, having 3 properties:

a) $1 \in S$

b) $0 \notin S$

c) If $s, t \in S$, then $st \in S$.

(Call such an S a multiplicative set. As an example, S might be all non-zero elts of R in the case when R is a domain, or if $x \in R$ and x^n is never 0, then S might be all the non-negative powers of x.) Our idea is to make a new ring, $S^{-1}R$, in which the elements of S become units. The construction mimics our construction of $\mathrm{Frac}(R)$, when R is a domain: We look at all pairs $\langle r, s\rangle$ where $r \in R$ and $s \in S$. We say $\langle r, s\rangle$ is equivalent to $\langle \rho, \sigma\rangle$ when and only when there is some $t \in S$ so that

$$t(r\sigma - \rho s) = 0.$$

This is an equiv. relation (check this mentally) and we write $\frac{r}{s}$ for the class containing $\langle r, s\rangle$. Define $+$ and $\cdot$ by

$$(\dagger)\begin{cases} \dfrac{r}{s} + \dfrac{\rho}{\sigma} = \dfrac{r\sigma + \rho s}{s\sigma} \\[2mm] \dfrac{r}{s} \cdot \dfrac{\rho}{\sigma} = \dfrac{r\rho}{s\sigma} \end{cases}$$

a) Show these operations are well-defined.

b) Let $S^{-1}R$ be the collection of all $\frac{r}{s}$, $r \in R$, $s \in S$, with the ring operations in $(\dagger)$ above. Show every $s \in S$ has an inverse in $S^{-1}R$.

c) There is a ring homomorphism $h : R \to S^{-1}R$, given by $h(r) = \frac{r}{1}$. (Check mentally that h is indeed a homomorphism.) What is $\ker(h)$ [remember: $\ker(h) = \{r \in R \mid h(r) = 0\}$] — explicit description please. When is h an injection, a surjection?

d) Say I is an ideal of R. Then $(S^{-1}R)I$, which is the set $\{qm \mid q \in S^{-1}R, m \in I\}$, is an ideal of $S^{-1}R$. When does $(S^{-1}R)I$ become the unit ideal (= everything) of $S^{-1}R$? Answer only in terms of S and I.

e) If $R = M[X]$, the polys in the variable X coeffs in the ring M, and if $S = \{X^n \mid n \geq 0,\ n \text{ an integer}\}$, describe explicitly the ring $S^{-1}R$. Which ideals of R, say J, become the unit ideal of $S^{-1}R$?

f) Let $R = \mathbb{Z}$, and let p be a prime number. Write S for the set of all integers relatively prime to p. It is a mult. subset of $\mathbb{Z}$. Show that $S^{-1}\mathbb{Z}$ is naturally a subring of $\mathbb{Q}$ ($= \mathrm{Frac}(\mathbb{Z})$). Exactly which fractions (in $\mathbb{Q}$) belong to $S^{-1}\mathbb{Z}$? Which ideals of $\mathbb{Z}$ become the unit ideal of $S^{-1}\mathbb{Z}$, and exactly which ideals of $\mathbb{Z}$ remain non-trivial ideals of $S^{-1}\mathbb{Z}$? List all the non-trivial ideals of $S^{-1}\mathbb{Z}$ [prove $S^{-1}\mathbb{Z}$ is a P.I.D., so you need only list the generators of the non-trivial ideals of $S^{-1}\mathbb{Z}$]. Find all the maximal ideals of $S^{-1}\mathbb{Z}$.