**Guidelines for laboratory/practical work**

Problem XVII.12. Prove that an R-module E is a generator if and only if it is balanced and ﬁnitely generated projective over EndR E.

Solution. Lang proves the (⇒) direction as Theorem 7.1, so it suﬃces to show that if E is balanced and ﬁnitely generated projective over EndR E, then R is a homomorphic image of a direct sum of E with itself.

Since E is ﬁnitely generated projective over EndR E, we have an isomorphism (EndR E)n = E ⊕ F for some EndR E-module F. Therefore we have the following isomorphisms of EndR E-modules:

∼

En = HomEndR E((EndR E)n,E) = HomEndR E(E ⊕ F,E) = HomEndR E(F,E) ⊕ EndEndR E(E).

∼ ∼

∼

If we deﬁne the operation of EndR E to be composition of mappings on the left, these become isomorphisms over R. Since E is balanced, EndEnd E(E) = R, so E is a generator.

∼

R

Problem X.9(a). Let A be an artinian commutative ring. Prove all prime ideals are maximal. [Hint: Given a prime ideal p, let x ∈ A, x ∈ p. Consider the descending chain (x) ⊃ (x2) ⊃ ....]

Solution. We show that any artinian domain is a ﬁeld. Let p be a prime ideal, so that A/p is a domain. Any quotient ring of an artinian ring is artinian (Proposition 7.1), so A/p is artinian. Let x ∈ A/p be nonzero. Then the descending chain (x) ⊃ (x2) ⊃ ... must terminate, so (xk) = (xk+1) for some integer k; therefore there exists a y ∈ A/p such that xk+1y = xk, which is to say xk(1 − xy) = 0, so xy = 1, and x ∈ (A/p)∗. Therefore A/p is a ﬁeld, so p is maximal.

Problem X.9(b). There is only a ﬁnite number of prime, or maximal, ideals. [Hint: Among all ﬁnite intersections of maximal ideals, pick a minimal one.]

Solution. Let S be the set of ﬁnite intersections of maximal ideals in A. This set is nonempty, so by Exercise XVII.2(c), there exists a minimal such intersection m1 ∩ ∩ mr. If m is any maximal ideal of A, then, m ∩ mi = mi so m ⊃ mi ⊃ m1m2 ...mr. A maximal ideal is prime, so m ⊃ mi for some i, but since

T T

i i

T

i

mi is maximal so m = mi.

Date: April 1, 2003.

XVII: 12 (ﬁrst sentence); X: 9, 10, 11.

1

2 JOHN VOIGHT

Problem X.9(c). The ideal N of nilpotent elements in A is nilpotent, that is there exists a positive integer k such that Nk = (0). [Hint: Let k be such that Nk = Nk+1. Let a = Nk. Let b be a minimal ideal such that ba = 0. Then b is principal and ba = b.]

Solution. Let k be such that Nk = Nk+1. Suppose that Nk = 0; let S be the set of ideals b of A such that bNk = 0. The set S is nonempty because Nk ∈ S, as NkNk = N2k = Nk = 0. Since A is artinian, S has a minimal element b. There is an element b ∈ b such that bNk = 0; therefore (b) ∈ S and (b) ⊂ b so by minimality (b) = b, in particular, b is ﬁnitely generated. But bNk ⊂ b and (bNk)Nk = bN2k = bNk, so again by minimality, bNk = b. But every element of Nk is nilpotent hence contained in every maximal ideal, so by Nakayama’s lemma, b = 0, a contradiction.

Problem X.9(d). A is noetherian.

Solution. Let k be an integer such that Nk = 0 as in part (c). Then Tp p = √0 = N, but by part (a) this implies N = mi. Let k be an integer such that Nk = 0. Then

T

i

T

Nk = 0 = ( imi)k ⊃ (m1 ...mr)k = mk ...mk.

r

1

Consider A as a module over itself; A is noetherian as an A-module if and only if A is noetherian as a ring. We have a ﬁltration

A ⊃ m1 ⊃ m1 ⊃ ⊃ m1 ...mr = 0

2

k k

of A. At the step E ⊃ Emi in the ﬁltration, E/Emi is a vector space over the ﬁeld A/mi which is ﬁnite-dimensional as A is artinian (as in Exercise XVII.2(a)). Therefore A has a ﬁnite simple ﬁltration, so by Proposition 7.2, A is noetherian as well as artinian.

Problem X.9(e). There exists an integer r such that

Y

A = A/mr m

∼

where the product is taken over all maximal ideals.

Solution. Let r be such that Nr = 0, and let mi be the maximal ideals of A. Since mi +mj = A for i = j, we also have mr +mr = A for i = j (otherwise, mr +mr ⊂ m for some maximal ideal m; then mr ⊂ m so mi ⊂ m, and similarly mj ⊂ m, a contradiction). By the Chinese remainder theorem, then,

i j i j

i

Y

A → A/mr m

i

T

i

is surjective. It is also injective, since mr = Nr = 0 (as in part (d)), therefore it is an isomorphism.

i

Problem X.9(f). We have A = YAp p

∼

where again the product is taken over all prime ideals p.

MATH 250B: HOMEWORK #7 3

Solution. It is enough to show that this map is an isomorphism considered as a map of A-modules. Let pi be the primes (maximal ideals) of A. Since localization preserves exact sequences (it is ﬂat), it is enough to show that the map A → Ap is an isomorphism after localization at every prime ideal p of A. But in this

Q

i

i

circumstance we have the map

Y Y

Ap → (Api )p = (Ap)pi . i i

Now Ap is artinian (descending chains of ideals of Ap are descending chains of ideals of A contained in p) and a local ring with maximal ideal pAp, so N = pAp and (pAp)r = 0. Then for p = pi, if xi ∈ p \ pi, xr = 0, so (Ap)p = 0 and the map is an isomorphism.

i

i

Problem X.10. Let A,B be local rings with maximal ideals mA,mB, respectively. Let f : A → B be a homomorphism. Suppose that f is local, i.e. f−1(mB) = mA. Assume that A,B are noetherian, and assume that:

(1) A/mA → B/mB is an isomorphism; (2) mA → mB/m2 is surjective;

B

(3) B is a ﬁnite A-module, via f.

Prove that f is surjective.

Solution. First, mB is a ﬁnitely generated B-module (since B is noetherian) and f(mA) is a ﬁnitely generated B-submodule of mB with mB = f(mA) + m2 by (2). By Nakayama’s lemma (X.4.2), f(mA) = mB.

B

Second, since B is ﬁnite over A and f(A) is a B-submodule with B = f(A)+mBB by (1), since A → B/mB is surjective. But mBB = mAB treating B as an A-module by f, so by Nakayama’s lemma, f(A) = B, so f is surjective.

Problem X.11. Let A be a commutative ring and M an A-module. Deﬁne the support of M by

Supp(M) = {p ∈ SpecA : Mp = 0}.

If M is ﬁnite over A, show that SuppM = V (Ann(M)), where V (a) = {p ∈ SpecA : p ⊃ a} and Ann(M) = {a ∈ A : aM = 0}.

Solution. Let p ∈ SpecA be so that Mp = 0. If aM = 0 then aMp = 0 so if a ∈ p then Mp = 0; hence Ann(M) ⊂ p.

Conversely, suppose Ann(M) ⊂ p. Let m1,...,mr generate M over A. Suppose that Mp = 0; then for all i there exists an ai ∈ p such that aimi = 0 ∈ M. Then a = i ai has aM = 0; therefore a ∈ p, a contradiction.

Q

Problem 12. Let K be a Galois extension of the Q with group G. Let B the integral closure of Z in K, and let α ∈ B be such that K = Q(α). Let f(X) be the irreducible polynomial for α over Q. Let p be a prime number, and assume that f remains irreducible modulo p over Z/pZ. What can you say about the Galois group G?

Solution. Let p be a prime above p in B. Then the decomposition group Gp is a subgroup of G; by Proposition 2.5, the extension B/p over Z/pZ is Galois with group cyclic of order n = [K : Q] = deg f. By proposition 2.8, Gp is isomorphic to this Galois group, so Z/nZ ⊂ G. Since both groups are ﬁnite of order n, G = Z/nZ, i.e. G is cyclic.

∼

Problem 13. Let A be an entire ring and K its quotient ﬁeld. Let t be transcendental over K. If A is integrally closed, show that A[t] is integrally closed.

Solution. Let x ∈ K(t) be integral over A[t]. Since K[t] is a UFD, it is integrally closed, so x ∈ K[t] (Proposition 1.7). Let x satisfy the integral equation

f(X) = Xn + an−1Xn−1 + + a0

with coeﬃcients ai ∈ A[t]. Write x = x(t) = cntn + + c0 with ci ∈ K. Substi-tuting these into f, looking at the coeﬃcients of each ti we see that the coeﬃcients ci are themselves integral over A, hence ci ∈ A, and x ∈ A[t].

Problem 14. Let L be a ﬁnite extension of Q and let OL be the ring of algebraic integers in L. Let σ1,...,σn be the distinct embeddings of L into the complex numbers. Embed OL into a Euclidean space by the map

α → (σ1α,...,σnα).

Show that in any bounded region of this Euclidean space, there is only a ﬁnite number of elements of OL. [Hint: The coeﬃcients in an integral equation for α are elementary symmetric functions of the conjugates of α and thus are bounded integers.] Use Exercise 5 of Chapter III to conclude that OL is a free Z-module of dimension ≤ n. In fact, show that the dimension is n, a basis of OL over Z also being a basis of L over Q.

Solution. Suppose α lies in the bounded region. Then the numbers σiα are all bounded; in particular, the coeﬃcients of an integral equation for α (being elemen-tary symmetric functions of the conjugates of α) are bounded integers. Since the

1

degree of an integral equation for α is also bounded (by the degree [L : Q]), there are only ﬁnitely many such integral equations, hence only ﬁnitely many α.

By Exercise III.5, OL is a free Z-module of rank ≤ n. Let α1,...,αn be a basis for L over Q. For each αi, there exists an integer ci ∈ Z>0 such that ciαi ∈ OL; therefore ciαi ∈ OL are Z-linearly independent, so OL contains a free Z-submodule of rank n, hence OL is itself free of rank n.

Problem 15. Let O be an entire ring which is noetherian, integrally closed, and such that every nonzero prime ideal is maximal. Deﬁne a fractional ideal a to be a nonzero O-submodule of the quotient ﬁeld K such that there exists c ∈ O, c = 0 for which ca ⊂ O. Prove that fractional ideals form a group under multiplication:

(a) Given an ideal a = 0 in O, there exists a product of prime ideals p1 ...pr ⊂ a.

(b) Every maximal ideal p is invertible, i.e. if we let p−1 be the set of elements x ∈ K such that xp ⊂ O, then p−1p = O.

(c) Every nonzero ideal is invertible, by a fractional ideal. [Use the noetherian property that if this is not true, there exists a maximal noninvertible ideal a and get a contradiction.]

Solution. For (a), consider the set of ideals which do not contain a product of primes. If the set is nonempty, since O is noetherian, there exists a maximal such ideal a. We cannot have a prime, therefore there exists x,y ∈ O such that xy ∈ a but x,y ∈ a. Since a is maximal, the ideals a + (x) and a + (y) contain a product of prime ideals: but

(a + (x))(a + (y)) ⊂ a

so a contains a product of primes, a contradiction.

For (b), it is clear that p−1p is an ideal of O, so since p is maximal, we must have either p−1p = p, or p−1p = O. Let a ∈ p be nonzero: then by (a) there exists a product of primes p1 ...pr ⊂ (a) ⊂ p. We may assume that p1 ...pr is a minimal such product (r taken as small as possible). Since every prime is maximal, we know p = pi for some i, so we may assume p = p1. Then p2 ...pr ⊂ (a), so there exists b ∈ p2 ...pr such that b ∈ (a). But bp ⊂ (a), so ba−1p ⊂ O, so ba−1 ∈ p−1. Since b ∈ aO, ba−1 ∈ O, so p−1 = O. This implies p−1p = O.

For (c), suppose that the set of nonzero noninvertible ideals is nonempty. Then since O is noetherian, there exists a maximal such noninvertible ideal a. If a is maximal, then by (b) it is invertible; otherwise, it is contained (properly) in a maximal ideal p, and

a ⊂ ap−1 ⊂ pp−1 = O.

We cannot have a = ap−1, so ap−1 is invertible. But then O = (ap−1)ap

implies that a is invertible, a contradiction.

To conclude, note that every fractional ideal a has ca ⊂ O for some c = 0: then (1/c)(ca)−1 is an inverse for a.

Problem 16. Let A be an entire ring, integrally closed. Let B be entire, integral over A. Let q1,q2 be prime ideals of B with q1 ⊃ q2 but q1 = q2. Let pi = qi ∩ A. Show that p1 = p2.

 3

Solution. Suppose p1 = p2 = p. Then the ring Ap is a local ring with maximal ideal pAp, and Bp is an integral extensions of Ap with qiBp ∩ Ap = pAp, so since the latter is maximal, so too is each qi. In particular, if q1 ⊂ q2, then q1 = q2, a contradiction.