Homework 4 Solutions

November 11, 2016

You were asked to do problems 3,4,7,9,10 in Chapter 7 of Lang.

Problem 3. Let A be an integral domain, integrally closed in its field of fractions K. Let L be a finite separable extension of K and let B be the integral closure of A in L. If A is Noetherian, show that B is a finitely generated A-module.

Solution.

Lemma 1 *If $x \in L$ then $tx \in B$ for some $t \in A$.*

Proof Since L/K is algebraic, x satisfies a polynomial

$$x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$$

with coefficients in K. Thus $y = tx$ satisfies the polynomial

$$y^n + b_{n-1}x^{n-1} + \ldots + b_0, \qquad b_{n-i} = t^i a_{n-i}.$$

Taking t to be the product of the denominators of the a_k written as fractions in A, we can arrange that the $b_k \in A$. Hence $tx \in B$. □

Lemma 2 *If $t \in B$ then $\mathrm{tr}(t) \in A$.*

Proof Since t is integral over A it is the root of a monic polynomial f with coefficients in A. The conjugates of t also satisfy this polynomial, so they are also integral over A. Thus the conjugates of t are in B. The trace $\mathrm{tr}(t)$ is the sum of the conjugates of t, so it is in B. However by Theorem VI.5.1 on page 285 of Lang, $\mathrm{tr}(t) \in K$. Since A is integrally closed $B \cap K = A$ and so $\mathrm{tr}(t) \in A$. □

Let $\omega_1, \cdots, \omega_n$ be a basis of L. By the Lemma, we may assume that $\omega_i \in B$. Now consider the trace bilinear form. By Theorem VI.5.2 on page 286 of Lang, this form identifies L with its dual space, so there is a dual basis ω_i' such that $\mathrm{tr}(\omega_i \omega_j') = \delta_{ij}$ (Kronecker delta).

Now consider the A-module M generated by ω_i'. Then $B \subseteq M$ because if $x \in B$ then we may write $x = \sum c_i \omega_i'$ and $\mathrm{tr}(c\omega_i) = \sum \mathrm{tr}(c_j \omega_j \omega_i') = c_i$. Thus $c_i \in A$ and $x \in M$. We see that B is a submodule of the finitely-generated module M. Because A is Noetherian, it follows that B is also finitely-generated.

Problem 4. Let L be a finite extension of $\mathbb{Q}$ and let $\mathfrak{o}_L$ be the ring of algebraic integers in L. Let $\sigma_1, \cdots, \sigma_n$ be the distinct embeddings of L into $\mathbb{C}$. Embed L into a Euclidean space by

$$\alpha \longmapsto (\alpha_1, \cdots, \alpha_n).$$

Show that any bounded region of space there are only a finite number of elements of $\mathfrak{o}_L$. Use Exercise 5 of Chapter III to conclude that $\mathfrak{o}_L$ is a free $\mathbb{Z}$-module of dimension $\leqslant n$. In fact, show that the dimension is n, a basis of $\mathfrak{o}_L$ over $\mathbb{Z}$ being also a basis of L over $\mathbb{Q}$.

Solution (following the hints in the book). Let e_i $(i \leqslant n)$ be the i-th elementary symmetric polynomial, so

$$e_i(x_1, \cdots, x_n) = \sum_{1 \leqslant k_1 < \cdots < k_i \leqslant n} x_{k_1} \cdots x_{k_n}.$$

If $\alpha \in \mathfrak{o}_L$, then α is a root of the polynomial

$$f(x) = 0, \qquad f(x) = x^n + a_{n-1}(\alpha) x^{n-1} + \ldots + a_0(\alpha)$$

where

$$a_{n-i}(\alpha) = (-1)^i e_i(\sigma_1 \alpha, \cdots, \sigma_n \alpha).$$

This formula shows that the coefficient a_{n-i}, regarded as a function of α, extends to a polynomial function on $\mathbb{C}^n$, namely the function $(-1)^i e_i$. For $\alpha \in \mathfrak{o}_L$, On the other hand, $a_{n-i}(\alpha)$ is integral over $\mathbb{Z}$ (since each $\sigma_i \alpha$ is integral) and they are invariant under the Galois group of the normal closure of L over $\mathbb{Q}$, and so $\alpha_{n-i}(\alpha) \in \mathbb{Q}$. Therefore $a_{n-i}(\alpha) \in \mathbb{Q} \cap \mathfrak{o}_L = \mathbb{Z}$.

So if K is a bounded region in $\mathbb{C}^n$, on the set K the function a_{n-i} takes bounded values. There are thus only a finite number of possible polynomials

$f(x) \in \mathbb{Z}[x]$ and therefore $\mathfrak{o}_L \cap K$ is finite. We see that $\mathfrak{o}_L$ is a discrete subgroup of a Euclidean space, hence it is finitely generated as an abelian group, and therefore free.

To see that the rank of $\mathfrak{o}_L$ is exactly n, it is sufficient to show that a basis of $\mathfrak{o}_L$ as a $\mathbb{Z}$-module is a basis of L as a vector space. This is similar to the arguments in the preceding exercise.

Problem 7 (Dedekind Domains). The usual definition of a Dedekind domain is a commutative domain that is Noetherian, integrally closed and of Krull dimension one which means that every nonzero prime ideal is maximal. These are rings that include principal ideal domains, and are "almost as good" as principal ideal domains. They come up frequently, for example, let K be an algebraic number field (a finite extension of $\mathbb{Q}$). Then the integral closure of $\mathbb{Z}$ in K is called the *ring of integers* and it is a Dedekind domain.

Assume that $\mathfrak{o}$ is Noetherian, integrally closed and of Krull dimension one which means that every nonzero prime ideal is maximal. Let K be its field of fractions.

(a) Given an ideal $\mathfrak{a}$ of $\mathfrak{o}$ prove that there exists a product of nonzero prime ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}$.

(b) Every maximal ideal $\mathfrak{p}$ is invertible by a fractional ideal. Thus if

$$\mathfrak{p}^{-1} = \{x \in K | x\mathfrak{p} \subseteq \mathfrak{o}\}$$

then $\mathfrak{p}^{-1}$ is a fractional ideal and $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{o}$.

(c) Every nonzero ideal is invertible.

Solution. (a) Since $\mathfrak{o}$ is Noetherian, any nonzero set of ideals has a maximal element. So we may assume that $\mathfrak{a}$ is an ideal that is maximal with respect to the assumption that it does not contain a product of nonzero ideals. Obviously $\mathfrak{a}$ cannot be prime, so find $x, y \in \mathfrak{o}$ such that $x, y \notin \mathfrak{a}$ but $xy \in \mathfrak{a}$. Then $\mathfrak{a} + \mathfrak{o}x$ is strictly larger than $\mathfrak{a}$ so it contains a product of prime ideals: $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a} + \mathfrak{o}x$. Similarly $\mathfrak{p}_{r+1} \cdots \mathfrak{p}_s \subseteq \mathfrak{a} + \mathfrak{o}y$. But then $\mathfrak{p}_1 \cdots \mathfrak{p}_r \cdot \mathfrak{p}_{r+1} \cdots \mathfrak{p}_s \subseteq (\mathfrak{a} + \mathfrak{o}x)(\mathfrak{a} + \mathfrak{o}y) \subseteq \mathfrak{a}$ since $xy \in \mathfrak{o}$. This is a contradiction.

(b) Clearly $\mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathfrak{o}$ so it is an ideal. If it is not equal to $\mathfrak{o}$ then it is a proper ideal. It contains $\mathfrak{p}$ since $1 \in \mathfrak{p}^{-1}$. Therefore we must have $\mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathfrak{p}$. Now if $x \in \mathfrak{p}^{-1}$ then $x\mathfrak{p} \subseteq \mathfrak{p}$ so $\mathfrak{p}$ is an $\mathfrak{o}[x]$-module that is faithful (since $\mathfrak{o}$ is a domain) and finitely generated as an $\mathfrak{o}$-module since $\mathfrak{o}$ is Noetherian. By INT3 on page 334, it follows that x is integral over $\mathfrak{o}$ and since $\mathfrak{o}$ is integrally

closed we must have $x \in \mathfrak{o}$. Thus we will have a contradiction if we can show $\mathfrak{p}^{-1} \not\subseteq \mathfrak{o}$.

Arguing by contradiction assume $\mathfrak{p}^{-1} \subseteq \mathfrak{o}$. Choose $y \in \mathfrak{p}$, $y \neq \mathfrak{o}$. By (a) we have a product $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{o}y$. Arguing by induction, assume r is as small as possible. One of the $\mathfrak{p}_i$ must equal $\mathfrak{p}$ because otherwise we could choose $x_i \in \mathfrak{p}_i - \mathfrak{p}$ and then $\prod x_i \in \prod \mathfrak{p}_i \subseteq \mathfrak{o}y \subseteq \mathfrak{p}$, which is a contradiction since $\mathfrak{p}$ is prime. So assume that $\mathfrak{p}_r = \mathfrak{p}$. Then

$$y^{-1}\mathfrak{p}_1 \cdots \mathfrak{p}_{r-1} \cdot \mathfrak{p} \subseteq \mathfrak{o} \qquad \Rightarrow \qquad y^{-1}\mathfrak{p}_1 \cdots \mathfrak{p}_{r-1} \subseteq \mathfrak{p}^{-1} \subseteq \mathfrak{o}.$$

So $\mathfrak{p}_1 \cdots \mathfrak{p}_{r-1} \subseteq \mathfrak{o}y$ which contradicts the minimality of r.

(c) Let $\mathfrak{a}$ be a nonzero ideal that is not invertible. Since $\mathfrak{o}$ is Noetherian, take $\mathfrak{a}$ to be maximal with this property, and let $\mathfrak{p}$ be a maximal ideal containing $\mathfrak{a}$. Then $\mathfrak{p} \subseteq \mathfrak{a}$ and so $\mathfrak{o} = \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathfrak{p}^{-1}\mathfrak{a}$. Therefore $\mathfrak{p}^{-1}\mathfrak{a}$ is an ideal. We claim that $\mathfrak{p}^{-1}\mathfrak{a}$ is strictly larger than $\mathfrak{a}$. If not, $\mathfrak{p}^{-1}\mathfrak{a} = \mathfrak{a}$ and so if $x \in \mathfrak{p}^{-1}$ then $\mathfrak{a}$ is a faithful $\mathfrak{o}[x]$ module that is finitely generated as an $\mathfrak{o}$-module so again by INT3, x is integral over the integrally closed ring $\mathfrak{o}$ proving $\mathfrak{p}^{-1} \subseteq \mathfrak{o}$. But we have already shown that this is not true in our proof of (b).

So $\mathfrak{p}^{-1}\mathfrak{a}$ is an ideal that is strictly larger than $\mathfrak{a}$ and by induction it is invertible. Thus $\mathfrak{a} = \mathfrak{p} \cdot \mathfrak{p}^{-1}\mathfrak{a}$ is invertible.

9. Let A be an integral domain. Let B be an integral domain that is integral over A. Let Q_1 and Q_2 be prime ideals of B with $Q_1 \supset Q_2$ and $Q_1 \neq Q_2$. Prove that if $P_i = Q_i \cap A$ then $P_1 \neq P_2$.

Note: Lang assumes that A is integrally closed but it appears that this assumption is unnecessary. Because Lang states an unnecessary hypothesis I am writing this up in greater detail than one usually would.

Solution. Assume that $P_1 = P_2$. Call this prime ideal P. Let $S = A - P$. Let us check that

$$S^{-1}Q_i \cap S^{-1}A = S^{-1}P.$$

If $q \in Q_i$ and $s \in S$ such that $q/s \in S^{-1}A$ then $q/s = a/t$ for $a \in A$ and $t \in T$. Then $qt = as \in A \cap Q_i$, that is $qt \in P$ and since $t \notin P$ and P is prime we have $q \in P$. So $q/s \in S^{-1}P$.

Now $S^{-1}P$ is the maximal ideal of the local ring $S^{-1}A$. Since $S^{-1}B$ is integral over $S^{-1}A$ (Proposition 1.8) we may invoke Proposition 1.11 (page 339) to conclude that $S^{-1}Q_2$ is maximal and so $S^{-1}Q_1 = S^{-1}Q_2$. Now let $q \in Q_1$. Then $q \in S^{-1}Q_2$ so $q = q_2/s$ for some $s \in S$ and therfore $qs \in Q_2$.

Now $s \notin P$ and so $s \notin Q_2$. Since Q_2 is prime it follos that $q \in Q_2$. We have proved $Q_1 \subseteq Q_2$ and so $Q_1 = Q_2$.

10. Let n be a positive integer and let ζ, ζ' be primitive n-th roots of unity.

(a) Show that $(1-\zeta)/(1-\zeta')$ is an algebraic integer.

(b) If $n \geqslant 6$ is divisible by at least two primes, show that $1-\zeta$ is a unit in the ring $\mathbb{Z}[\zeta]$.

For (b) I said to assume that $n = pq$ is a product of two distinct primes. This makes the problem slightly easier.

Solution. (a) Since ζ' is a primitive n-th root of unity, ζ is a power of ζ', that is, $\zeta = (\zeta')^m$ for some m. Now

$$\frac{1-\zeta}{1-\zeta'} = \frac{1-(\zeta')^m}{1-\zeta'} = 1 + \zeta' + (\zeta')^2 + \cdots (\zeta')^{m-1}.$$

Thus $\frac{1-\zeta}{1-\zeta'}$ is in the ring generated by ζ', and since ζ' is integral over $\mathbb{Z}$, so is this ratio. That is, it is an algebraic integer.

(b) We first prove, with $\zeta_m = e^{2\pi i/m}$ that

$$\prod_{i=1}^{m-1} \left(1 - \zeta_m^i\right) = m. \tag{1}$$

Indeed, the polynomial $X^m - 1$ has roots ζ_m^i for $i = 0, 1, \cdots, m-1$ and so

$$X^m - 1 = \prod_{i=0}^{m-1} (X - \zeta_m^i).$$

Dividing by the $i = 0$ factor

$$\prod_{i=1}^{m-1} (X - \zeta_m^i) = \frac{X^m - 1}{X - 1} = X^{m-1} + X^{m-2} + \ldots + 1$$

and substituting $X = 1$ gives (1).

Now we prove that

$$\prod_{\substack{i\,=\,1 \\ (p,\,i)\,=\,1 \\ (q,\,i)\,=\,1}}^{pq-1} (1 - \zeta_{pq}^i) = 1. \tag{2}$$

This equals

$$\frac{\prod_{i=1}^{pq}(1-\zeta_{pq}^{i})}{\left[\prod_{i=1}^{p}(1-\zeta_{pq}^{qi})\right]\left[\prod_{i=1}^{q}(1-\zeta_{pq}^{pi})\right]}$$

since the factors on the right that are not in the denominator are exactly those with i prime to both p and q. Recognizing that $\zeta_{pq}^{q}=\zeta_p$ this equals

$$\frac{\prod_{i=1}^{pq}(1-\zeta_{pq}^{i})}{\left[\prod_{i=1}^{p}(1-\zeta_{p}^{i})\right]\left[\prod_{i=1}^{q}(1-\zeta_{q}^{i})\right]}=\frac{pq}{p\cdot q}=1$$

where all three factors are evaluated using (1).

Now one of the factors in (2) is $1-\zeta$, and the others are in $\mathbb{Z}[\zeta]$, proving that $1-\zeta$ is a unit.