Math 210B: Homework 1 Solutions

Readings in Lang's *Algebra* for these problems: Sections 7.1 and 8.1; also Section 4.2 for Gauss' Lemma and Section 6.5 for norm and trace.

For the first two problems, let R be an integral domain, F its field of fractions, K/F a larger field. Let $\alpha \in K$. As we recall, α is defined to be integral over R if it satisfies a monic polynomial $f(\alpha) = 0$ where

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in R[x].$$

However in this definition we do not require f to be irreducible. So α is also a root of a monic polynomial

$$g(x) = x^m + b_{m-1}x^{m-1} + \ldots + b_0 \in F[x]$$

that is irreducible in $F[x]$. The first two exercises give conditions for $g \in R[x]$.

Problem 1. Suppose that R is a unique factorization domain. Use Gauss' Lemma to show that $g(x) \in R[x]$.

Solution: In the language of Section 4.2 in Lang's *Algebra* the *content* $\text{content}(f)$ of a polynomial $p \in R[x]$ is the greatest common divisor of the coefficients; it is only defined up to units. One version of Gauss' Lemma states that

$$\text{content}(pq) = \text{content}(p)\,\text{content}(q).$$

The content may be extended to $F[x]$ by multiplicativity.

We know that g generates the ideal $\{p \in F[x] | p(\alpha) = 0\}$, so g divides f in $F[x]$. Thus we may write $f = gh$ with $g, h \in F[x]$. Now $\text{content}(f) = 1$ since f is monic and has coefficients in $R[x]$. Therefore if $c = \text{content}(g)$ we may write $f = g_1 h_1$ with $g_1 = c^{-1}g$ and $h = ch$. Then g_1 has content 1 and by Gauss' Lemma h_1 also has content 1. Now the leading coefficient of f is 1, so the product of the leading coefficients of g_1 and h_1 are also 1, and so c is a unit. Therefore g has content 1, and in particular $g \in R[x]$.

The next problem requires some Galois theory.

Problem 2. Now suppose that R is integrally closed and $\text{char}(F) = 0$. Let $\alpha_1, \cdots, \alpha_m$ be the roots of g in a splitting field $E \supseteq K$. Thus $m = \deg(g)$. (a) Explain why the α_i are distinct and

$$g(x) = (x - \alpha_1) \cdots (x - \alpha_m).$$

(b) Prove that $b_i \in R$, so just as in Problem 1, $g \in R[x]$.

Solution. For (a), in characteristic zero the roots of the irreducible polynomial g are distinct by the criterion that g and its derivative g' are coprime in $F[x]$; this follows from the fact that g' is nonzero and of degree less than g, which is irreducible. Now $F(\alpha_1, \cdots, \alpha_m)$ is a Galois extension since it is the splitting field of a polynomial with distinct roots. The coefficients of

$$g_1(x) = (x - \alpha_1) \cdots (x - \alpha_m)$$

are in $F[x]$ because they are invariant under the Galois group. Thus $g | g_1$ but actually $g = g_1$ because every root of g_1 is a root of g.

For (b), each α_i is integral over R, since they are all roots of the monic polynomial $f \in R[x]$. Since the elements of E that are integral over R form a ring, it follows that each coefficient

$$b_{m-k} = (-1)^k \sum_{i_1 < \cdots < a_k} \alpha_{i_1} \cdots \alpha_{i_k}$$

is an element of F that is integral over R. Because R is integrally closed, $b_{m-k} \in R$ proving that $g \in R[x]$.

Problem 3. Let D be squarefree and consider $\alpha = a + b\sqrt{D} \in \mathbb{Q}\left(\sqrt{D}\right)$. Describe the norm and trace $\text{tr}(\alpha)$ and $N(\alpha)$. Prove that α is integral over $\mathbb{Z}$ if and only if $\text{tr}(\alpha)$ and $N(\alpha)$ are in $\mathbb{Z}$.

Solution: The conjugates of α over $\mathbb{Q}$ are α and $\beta = a - b\sqrt{D}$, so the norm and trace are:

$$\alpha + \beta = 2a, \qquad \alpha\beta = a^2 - Db^2.$$

Both α, β are integral over $\mathbb{Z}$ and so the norm and trace are elements of $\mathbb{Q}$ that are integral over $\mathbb{Z}$. But $\mathbb{Z}$ is integrally closed since it is a UFD. Thus

$\mathrm{tr}(\alpha)$, $N(\alpha) \in \mathbb{Z}$. Conversely, if $\mathrm{tr}(\alpha)$ and $N(\alpha)$ are in $\mathbb{Z}$ then α is a root of the monic polynomial:

$$x^2 - \mathrm{tr}(\alpha)x + N(\alpha) \in \mathbb{Z}[x].$$

Whether or not this polynomial is irreducible, this proves that α is integral over $\mathbb{Z}$.

Problem 4. Let p be a prime. Determine the integral closure of $\mathbb{Z}$ in $\mathbb{Q}\left(\sqrt{p}\right)$ and $\mathbb{Q}\left(\sqrt{-p}\right)$. The shape of the answer should depend on p mod 4.

Solution: We consider more generally $\mathbb{Q}\left(\sqrt{D}\right)$ with D squarefree. The condition that $a + b\sqrt{D}$ be integral is that $2a$ and $a^2 - Db^2$ be in $\mathbb{Z}$, by Problem 3. It follows that $4Db^2 = (2a)^2 - 4(a^2 - Db^2) \in \mathbb{Z}$ and since D is squarefree, this implies that $2b \in \mathbb{Z}$. Let $A = 2a$ and $B = 2b$. Then 4 divides $A^2 - DB^2$. The squares in $\mathbb{Z}/4\mathbb{Z}$ are 0 and 1, so A and B must both be even unless $D \equiv 1 \bmod 4$ in which case A and B may both be even or both odd.

From this we deduce that $a + b\sqrt{D} \in \mathbb{Z}\left[\sqrt{D}\right]$ (which is therefore the integral closure) except in the case where $D \equiv 1 \bmod 4$. If $D \equiv 1$, then we have proved that for $a + b\sqrt{D}$ to be integral over $\mathbb{Z}$ we so the integral closure of $\mathbb{Z}$ is

$$\left\{\tfrac{1}{2}(A + B\sqrt{D}) | A, B \in \mathbb{Z}, A, B \text{ both even or both odd}\right\}$$

which is the ring

$$\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right].$$

The generator $\frac{1+\sqrt{D}}{2}$ is itself a root of the polynomial $x^2 - x + \frac{1-D}{4} \in \mathbb{Z}[x]$.

Problem 5. Let $E \supset K \supset F$ fields. Prove that the transcendence degrees are additive:

$$\mathrm{tr}\,.\deg(E/F) = \mathrm{tr}\,.\deg(E/K) + \mathrm{tr}\,.\deg(K/F).$$

Solution: Let $\alpha_1, \cdots, \alpha_m$ be a transcendence basis of K/F and $\beta_1, \cdots, \beta_n$ be a transcendency basis of E/K. We claim $\alpha_1, \cdots, \alpha_m, \beta_1, \cdots, \beta_n$ are a transcendency basis of E/F. First note that E is algebraic over $K(\beta_1, \cdots, \beta_n)$ which in turn is algebraic over $F(\alpha_1, \cdots, \alpha_m, \beta_1, \cdots, \beta_n)$. Thus E is algebraic over $F(\alpha_1, \cdots, \alpha_m, \beta_1, \cdots, \beta_n)$.

It remains to be shown that the α_i, β_j are algebraically independent. If there is a relation of algebraic dependence:

$$\phi(\alpha_1, \cdots, \alpha_m, \beta_1, \cdots, \beta_n) = 0,$$

with $\phi(x_1, \cdots, x_m, y_1, \cdots, y_n) \in F[x_1, \cdots, x_m, y_1, \cdots, y_n]$ a polynomial in $m + n$ variables. This may be rearranged as a relation

$$\psi(\beta_1, \cdots, \beta_n) = 0$$

where

$$\psi(y_1, \cdots, y_n) = \sum_{\nu \in \mathbb{N}^n} c_{(\nu)}(\alpha_1, \cdots, \alpha_m) y_1^{\nu_1} \cdots y_n^{\nu_n}$$

and each $c_{(\nu)} \in F[y_1, \cdots, y_m]$. Now $c_{(\nu)}(\alpha_1, \cdots, \alpha_m) \in F(\alpha_1, \cdots, \alpha_m) \subseteq K$ and since $\beta_1, \cdots, \beta_n$ are algebraically independent over K, each $c_{(\nu)}(\alpha_1, \cdots, \alpha_m) = 0$. But since the α_i are algebraically independent over F, this means $c_{(\nu)} = 0$ as a polynomial in $F[y_1, \cdots, y_m]$ and therefore ϕ is the zero polynomial, proving the independence of the α_i, β_j.