Math 538: Commutative Algebra Problem Set

This problem set is for those who want to dig deeper. We may use some of those results in class, or only in problem sets.

Zorn's Lemma

DEFINITION. Let $\mathcal{F}$ be a set of sets. A *chain* in F is a subset $\mathcal{C} \subset \mathcal{F}$ such that for any $A, B \in \mathcal{C}$ either $A \subset B$ or $B \subset A$. An element $M \in \mathcal{F}$ is *maximal* if it is not contained in any other member.

AXIOM (Zorn's Lemma). *Let $\mathcal{F}$ be non-empty. Suppose that for any chain $\mathcal{C} \subset \mathcal{F}$ the set $\bigcup \mathcal{C} = \bigcup_{A \in \mathcal{C}} A$ also belongs to $\mathcal{F}$. Then $\mathcal{F}$ has maximal elements.*

1. Let F be a field, V a vector space over F. Let $\mathcal{F}$ be the family of linearly independent subsets of V. Show that $\mathcal{F}$ has maximal elements and conclude that V has a basis.

2. Let R be a ring (recall that rings here are commutative with identity), $I \subset R$ a proper ideal. Show that there exists a maximal ideal M of R containing I.

3. Let R be a ring, $S \subset R \setminus \{0\}$ a subset closed under multiplication. Show that there is a prime ideal P disjoint from S.

OPT Let $(X, \leq)$ be a partially ordered set (that is, $\leq$ is transitive and reflexive, and $x \leq y \wedge y \leq x \rightarrow x = y$). A *chain* in X is a subset $Y \subset X$ such that any two elements of Y are comparable (if $x, y \in Y$ then at least one of $x \leq y, y \leq x$ holds). An *upper bound* for a chain Y is an element $x \in X$ satisfying $y \leq x$ for all $y \in Y$. Show: suppose every chain in X has an upper bound. Then X has maximal elements.

Primes and Localization

Fix a commutative ring R. A *multiplicative subset* of R is a subset $S \subset R \setminus \{0\}$ closed under multiplication such that $1 \in S$. Fix such a subset.

4. Consider the following relation on $R \times S$: $(r,s) \sim (r',s') \iff \exists t \in S : t(s'r - sr') = 0$ (the intended interpretation of the pair (r,s) is as the fraction $\frac{r}{s}$).
   (a) Show that this is an equivalence relation, and that $(1,1) \not\sim (0,1)$.
   DEF Let $[r,s]$ (or $\frac{r}{s}$) denote the equivalence class of (r,s), and let $R[S^{-1}]$ denote the set of equivalence classes. Let $\iota\colon R \to R[S^{-1}]$ denote the map $\iota(r) = [r,1]$.
   (b) Define $[r,s] + [r',s'] = [rs' + r's, ss']$ and $[r,s] \cdot [r',s'] = [rr', ss']$. Show that this defines a ring structure on $R[S^{-1}]$ and that ι is a ring homomorphism such that $\iota(S) \subset R[S^{-1}]^{\times}$. Show that ι is injective iff S contains no zerodivisors.
   (c) Show that for any ring T and any homomorphism $\varphi\colon R \to T$ such that $\varphi(S) \subset T^{\times}$ there is a unique $\varphi'\colon R[S^{-1}] \to T$ such that $\varphi = \varphi' \circ \iota$.
   (d) Let $I \lhd R[S^{-1}]$ be a proper ideal. Show that $\iota^{-1}(I)$ is a proper ideal of R disjoint from S, and that I is the ideal of $R[S^{-1}]$ generated by $\iota(\iota^{-1}(I))$.
   (e) Conclude that when $S = R \setminus P$ for a prime ideal P (why is this closed under multiplication?) the ring $R[S^{-1}]$ is *local*: it has a unique maximal ideal (that being the ideal generated by the image of P).

DEFINITION. We call $R[S^{-1}]$ the *localization of R away from S.* If $S = R \setminus P$ for a prime ideal P we write R_P for $R[S^{-1}]$ and call it the localization of R *at* P.

5. Now let M be an R-module. On $M \times S$ define the relation $(m,s) \sim (m',s') \iff \exists t \in S : t(s'm - sm') = 0$ (with the interpretation $\frac{1}{s}m$).
   (a) Show that this is an equivalence relation, and that setting $[m,s] + [m',s'] = [s'm + sm', ss']$ and $[r,s] \cdot [m,s'] = [rm, ss']$ gives $M[S^{-1}]$, the set of equivalence classes, the structure of an $R[S^{-1}]$-module.
   (b) Let $\varphi \colon M \to N$ be a map of R-modules. Show that mapping $[m,s] \to [\varphi(m), s]$ gives a well-defined map $\varphi_{S^{-1}} \colon M[S^{-1}] \to N[S^{-1}]$ of $R[S^{-1}]$-modules.
   (c) Show that $\varphi_{S^{-1}}$ is surjective if φ is.
   (d) Show that $\operatorname{Ker} \varphi_{S^{-1}} = \left\{ [m,s] \in M[S^{-1}] \mid \exists t \in S : tm \in \operatorname{Ker} \varphi \right\}$.

6. (The key proposition)
   (a) Let M be a non-zero R-module. Show that there is a prime P (in fact, a maximal ideal) such that M_P is a non-zero R_P-module.
   (b) Let $M \subset N$ be R modules. Show that $M \neq N$ iff there is a prime P such that $M_P \neq N_P$.

7. (Examples)
   (a) Let R be an integral domain. Show that $K(R) = R_{(0)}$ is a field. This is known as the *fraction field* of R. Show that in this case $R[S^{-1}]$ is isomorphic to the subring of $K(R)$ genreated by the image of R and of the inverses of the elements of S.
   (b) Let p be a rational prime. Show that the $\mathbb{Z}_{(p)}$ is a *discrete valuation ring*: that for every $x \in \mathbb{Q}^\times$ at least one of x, x^{-1} belongs to $\mathbb{Z}_{(p)}$.
   (c) Let $\Lambda < \mathbb{Z}^d$ be a subgroup of finite index, and let $\iota \colon \Lambda \to \mathbb{Z}^d$ be the incusion map. Show that $\iota_{(p)} \colon \Lambda_{(p)} \to \left(\mathbb{Z}_{(p)}\right)^d$ is an isomorphism iff p does not divide the index.

Integrality in general: A tour in commutative algebra

DEFINITION. Let $A \subset B$ be an extension of rings. $\beta \in B$ is said to be *integral* over A if $p(\beta) = 0$ for some monic $p \in A[x]$.

8. (Basic properties)
   (a) $\beta \in B$ is integral over B iff $A[\beta]$ is a finitely generated A-module iff there is a finitely generated A-module $M \subset B$ such that $\alpha M \subset M$.
   (b) Let $\alpha, \beta \in B$ be integral over A. Then so is every element of $A[\alpha, \beta]$
   (c) The set of elements in B integral over A is a subring of B called the *integral closure* of A in B, and denoted $\bar{A}$. Say that A is *integrally closed in B* if $\bar{A} = A$ (say an integral domain is *integrally closed* if it is integrally closed in its field of fractions).

9. Let $A \subset B \subset C$ be a rings.
   (a) Suppose B is integral over A and $\gamma \in C$ is integral over B. Then γ is integral over A.
   COR Let $\gamma \in C$ be integral over the integral closure of A in B. Then it is integral over A.
   COR Suppose A is integrally closed in B and B is integrally closed in C. Then A is integrally closed in C.
   (b) Let L/K be an extension of number fields. Then $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L.

Hints

For 6a: Let $m \in M$ be non-zero. Check that $\mathrm{Ann}(m) = \{r \in R \mid rm = 0\}$ is a proper ideal and localize at a maximal ideal containing it.

For 6b: Localize at P so that $(N/M)_P \neq 0$.

CHAPTER 1

Number Fields and Algebraic Integers

DEFINITION 7. A *number field* is a finite extension of $\mathbb{Q}$.

Fix a number field K from now on. Let $n = [K : \mathbb{Q}]$.

1.1. Algebraic Integers

DEFINITION 8. An element $\alpha \in K$ is said to be an *algebraic integer* if $p(\alpha) = 0$ for some monic polynomial $p \in \mathbb{Z}[x]$. The set of algebraic integers in K is denoted $\mathcal{O}_K$ and called the "ring of integers" or the "maximal order".

LEMMA 9. *$\alpha \in K$ is an algebraic integer iff its minimal polynomial is in $\mathbb{Z}[x]$.*

PROOF. One direction is immediate. For the other, let $p \in \mathbb{Z}[x]$ be monic such that $p(\alpha) = 0$ and let $m \in \mathbb{Q}[x]$ be the minimal polynomial. Then m is an irreducible factor of p in $\mathbb{Q}[x]$, but by Gauss's Lemma every such divisor is in $\mathbb{Z}[x]$. □

EXAMPLE 10. $K = \mathbb{Q}$. The minimal polynomial of α is $x - \alpha$ so $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. This is the "rational root theorem".

EXAMPLE 11. $K = \mathbb{Q}(i)$. The minimal polynomial of $a + bi$ is $(x - a - bi)(x - a + bi) = (x - a)^2 + b^2 = x - (2a)x + (a^2 + b^2)$. This is $\mathbb{Z}[x]$ iff $2a, a^2 + b^2 \in \mathbb{Z}$. Thus $a \in \frac{1}{2}\mathbb{Z}$. If $a \in \mathbb{Z}$ then $b \in \mathbb{Q}$, $b^2 \in \mathbb{Z}$ so $b \in \mathbb{Z}$. If $a \notin \mathbb{Z}$ then $(2a)^2 + (2b)^2 \in 4\mathbb{Z}$ where $2a$ is an odd integer. This forces $(2b)^2$ to be an integer, hence $2b$ to be an integer, but then $(2b)^2$ is $0, 1$ mod 4 which is impossible since $(2a)^2 \equiv 1\,(4)$. Thus $a + bi$ is algebraic iff $a, b \in \mathbb{Z}$.

REMARK 12. Note that $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is a subring of K.

LEMMA 13. *$\beta \in \mathcal{O}_K$ iff $\mathbb{Z}[\beta]$ is a finitely generated Abelian group iff there is a finitely generated Abelian group $M \subset K$ such that $\alpha M \subset M$.*

PROOF. If $\beta \in \mathcal{O}_K$ then $\mathbb{Z}[\beta] = \mathbb{Z} \oplus \mathbb{Z}\beta \oplus \cdots \oplus \mathbb{Z}\beta^{n-1}$ where β has degree n. The last claim implies the first by Cayley–Hamilton. □

THEOREM 14. *Let $\alpha, \beta \in K$ be algebraic integers. Then so are $\alpha \pm \beta$, $\alpha\beta$.*

PROOF. Suppose that $\alpha M \subset M$, $\beta N \subset N$, where $M = \sum_{i=1}^{r} \mathbb{Z}x_i$, $N = \sum_{j=1}^{s} \mathbb{Z}y_j$. Then $MN = \sum_{i,j} \mathbb{Z}x_i y_j$ is invariant by α, β hence by $\mathbb{Z}[\alpha, \beta]$ which contains the requisite elements. □

COROLLARY 15. *$\mathcal{O}_K$ is a subring of K. If $\alpha \in \mathcal{O}_K$ then:*

(1) Every conjugate of α is integral over $\mathbb{Q}$;
(2) The minimal polynomial of α over $\mathbb{Q}$ is monic and belongs to $\mathbb{Z}[x]$;
(3) $\mathrm{Tr}^K_{\mathbb{Q}}(\alpha), N^K_{\mathbb{Q}}(\alpha) \in \mathbb{Z}$ and,
(4) $\alpha \in \mathcal{O}_K^\times$ iff $N^K_{\mathbb{Q}}\alpha \in \mathbb{Z}^\times = \{\pm 1\}$.