Math 676. Homework 3

1. A *lattice* in a finite-dimensional $\mathbf{R}$-vector space V is a discrete closed subgroup $\Lambda \subseteq V$ such that the quotient V/Λ with its (Hausdorff) quotient topology is compact.

(i) Prove that if G is a Hausdorff topological group and H is subgroup whose induced topology is discrete (we then say that H is a *discrete subgroup*), then H is automatically closed in G. Give a counterexample if G is not assumed to be Hausdorff.

(ii) Prove that a subgroup Λ in a finite-dimensional $\mathbf{R}$-vector space V is discrete if and only if Λ is a finite free $\mathbf{Z}$-module such that the natural map $\mathbf{R} \otimes_{\mathbf{Z}} \Lambda \to V$ is injective, and that Λ is a lattice if and only if Λ is a finitely generated $\mathbf{Z}$-module and the natural map $\mathbf{R} \otimes_{\mathbf{Z}} \Lambda \to V$ is an isomorphism. (That is, a $\mathbf{Z}$-basis of Λ is an $\mathbf{R}$-basis of V; in particular, the $\mathbf{Z}$-rank of Λ must equal the $\mathbf{R}$-rank of V.) Give an example of subgroup of $\mathbf{R}^2$ that is finite free of rank 2 over $\mathbf{Z}$ but is not a discrete subgroup.

(iii) Let K be a number field. Prove that $\mathscr{O}_K$ is a lattice in the Euclidean space $K \otimes_{\mathbf{Q}} \mathbf{R}$, and draw a picture of this lattice for $K = \mathbf{Q}(\alpha)$ in the cases $\alpha^2 = 2$ and $\alpha^2 = 5$, using the canonical isomorphism of $\mathbf{R}$-algebras $K \otimes_{\mathbf{Q}} \mathbf{R} \simeq \mathbf{R} \times \mathbf{R}$ with $\mathbf{R}$-factors labelled by the two embeddings of K into $\mathbf{R}$ (make sure to indicate the embedding associated to your axes).

(iv) Prove that in both pictures, the projection of the lattice onto either coordinate axis is a dense subgroup of $\mathbf{R}$. For any number field K with $r_1 + r_2 > 1$ (that is, $K \neq \mathbf{Q}$ and K not imaginary quadratic), make a topological conjecture concerning the image of $\mathscr{O}_K$ in the quotient of $K \otimes_{\mathbf{Q}} \mathbf{R}$ modulo a primitive idempotent; can you prove this conjecture? In the case $K = \mathbf{Q}(\zeta_5)$, how does this explain the winning strategy in the computer game "Lucy and Lilly" on Rick Schwarz' web site at the University of Maryland?

2. A pair of ideals I and J in a ring R are said to be *coprime* if $I + J = A$. For example, if I is a maximal ideal and J is not contained in I then I and J are coprime.

(i) If A is a PID, prove that nonzero ideals (a) and (a') are coprime if and only if a and a' share no common irreducible factor. Give a counterexample in a UFD that is not a PID. (Hint: $A = k[X, Y]$ for a field k.)

(ii) If I and J are coprime, prove that the inclusion $IJ \subseteq I \cap J$ is an equality.

(iii) If $I_1, \dots, I_k$ are ideals that are pairwise coprime with $k \geq 2$, prove that I_1 and $\prod_{j=2}^{k} I_j$ are coprime, and deduce by induction on k and (ii) that $\cap I_j = \prod I_j$.

(iv) Prove the *Chinese Remainder Theorem* for pairwise coprime ideals: if $I_1, \dots, I_k$ are pairwise coprime (with $k \geq 2$) then the natural map of rings $R/(\prod I_j) \to \prod R/I_j$ is an isomorphism, and so in particular the natural map $R \to \prod R/I_j$ is surjective. (Hint: induction)

3. (i) Let R be a domain whose underlying set is finite. Prove that R is a field.

(ii) Let F be a field and let A be an F-algebra that is finitely generated as an F-module. Prove that A is a domain if and only if it is a field. Can one relax module-finiteness to integrality?

4. Let $d \in \mathbf{Z}$ be a nonzero squarefree integer with $d \neq 1$. Let $K = \mathbf{Q}(\sqrt{d})$. Let $D = D_K = \mathrm{disc}(\mathscr{O}_K/\mathbf{Z})$ be the discriminant of K (so $D = 4d$ if $d \equiv 2, 3 \bmod 4$ and $D = d$ otherwise, so $D \equiv 0, 1 \bmod 4$ and $2|D$ if and only if $d \equiv 2, 3 \bmod 4$).

(i) Construct an isomorphism $\mathbf{Z}[X]/(X^2 - DX + (D^2 - D)/4) \simeq \mathscr{O}_K$, and be sure to give a careful proof that your map really is an isomorphism. (Hint: Prove that if R is any ring and $f \in R[X]$ is monic of degree $n \geq 1$, then $R[X]/(f)$ is a free R-module with R-basis $1, X, \dots, X^{n-1}$.)

(ii) Passing to the quotient modulo p, describe $\mathscr{O}_K/p\mathscr{O}_K$ as a quotient of $\mathbf{F}_p[X]$, and for odd p (resp. $p = 2$) deduce that $p\mathscr{O}_K$ is a prime ideal of $\mathscr{O}_K$ if and only if $p \nmid D$ and D is a nonsquare modulo p (resp. $D \equiv 5 \bmod 8$), in which case $\mathscr{O}_K/p\mathscr{O}_K$ is a finite field with size p^2. Prove that $\mathscr{O}_K/p\mathscr{O}_K \simeq \mathbf{F}_p[t]/(t^2)$ as rings if $p|D$ (so $\mathscr{O}_K/p\mathscr{O}_K$ has nonzero nilpotents in this case), and that if $p \nmid D$ but D is a square modulo p for odd p (resp. $D \equiv 1 \bmod 8$ for $p = 2$) then $\mathscr{O}_K/p\mathscr{O}_K \simeq \mathbf{F}_p \times \mathbf{F}_p$ as rings (so $\mathscr{O}_K/p\mathscr{O}_K$ has nontrivial idempotents in this case).

(iii) Let k be an algebraically closed field with $\mathrm{char}(k) \neq 2$, and let $f \in k[z]$ be a monic squarefree polynomial with degree n. Carry out analogues of (i) and (ii) for the extension $k[z] \to k[t, z]/(t^2 - f(z)) = k[t][\sqrt{f}]$. Relate the three cases in (ii) to the geometry of the projection $(t, z) \mapsto z$ of the plane curve

$t^2 = f(z)$ onto the z-axis, and in particular give a geometric interpretation of the zero locus of D. (In this final part, assume $k = \mathbf{C}$ if you prefer complex analysis to algebraic geometry.)

5. Let A be a domain and let M and N be torsion-free A-modules. The purpose of this exercise is to prove the final part, which gives some very important properties of $M \otimes_A N$ when A is Dedekind. *Our development of class groups will assume that you have done this exercise!*

(i) For any multiplicative set S in A, define $S^{-1}M$ in terms of "fractions", give it a natural structure of $S^{-1}A$-module, and prove that if $f : M \to N$ is a map between A-modules then there is a unique $S^{-1}A$-linear map $S^{-1}f : S^{-1}M \to S^{-1}N$ compatible with f and the natural maps $M \to S^{-1}M$ and $N \to S^{-1}N$. Prove also that the natural map $M \to S^{-1}M$ is injective and uniquely factors through an $S^{-1}A$-linear map $S^{-1}A \otimes_A M \to S^{-1}M$ that moreover is an isomorphism.

In the special case $S = A - \mathfrak{p}$ for a prime ideal $\mathfrak{p}$, we write $M_{\mathfrak{p}}$ to denote $S^{-1}M$.

(ii) Prove that a map $f : M \to N$ is surjective if and only if $f_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is surjective for all maximal ideals $\mathfrak{m}$ of A. (hint: Suppose there exists $n \in N$ not in the image of M, and let I be the set of $a \in A$ such that an is in the image of f. Prove that I is an ideal and $I \neq A$, and for a maximal ideal $\mathfrak{m}$ of A containing I (Zorn!) prove that $f_{\mathfrak{m}}$ is *not* surjective.)

(iii) Prove that the A-module $\mathrm{Hom}_A(M, N)$ is torsion-free, and construct a natural map

$$\theta_{S,M,N} : S^{-1}\mathrm{Hom}_A(M, N) \to \mathrm{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N)$$

for any multiplicative set S in A. Assuming that A is noetherian and M and N are finitely generated, prove that $\mathrm{Hom}_A(M, N)$ is finitely generated and that $\theta_{S,M,N}$ is an isomorphism. (Hint for second part: Treat the case when M is finite free, and then use a right-exact sequence

$$A^{\oplus n} \to A^{\oplus m} \to M \to 0$$

and *functoriality* in conjunction with exactness properties of $\mathrm{Hom}_A(\cdot, N)$ to reduce the general case to the case of finite free M.)

(iv) Assume that M and M' are finitely generated and torsion-free, and that A is noetherian. Let $\pi : M' \to M$ be a surjective linear map. A *section* of π is a linear map $s : M \to M'$ such that $\pi \circ s$ is the identity on M. Show that if s is a section then the natural map $\ker \pi \oplus s(M) \to M'$ is an isomorphism (so we may identify M with a direct summand of M'), and that a section exists if and only if the natural map of A-modules $\mathrm{Hom}_A(M, M') \to \mathrm{Hom}_A(M, M)$ (via composition with π) is surjective. Using (ii) and (iii), deduce the non-obvious fact that π admits an A-linear section if and only if $\pi_{\mathfrak{m}}$ admits an $A_{\mathfrak{m}}$-linear section for every maximal ideal $\mathfrak{m}$ of A!

(v) Finally, assume that A is a Dedekind domain. Using that $A_{\mathfrak{m}}$ is a PID for every maximal ideal $\mathfrak{m}$ of A, prove that every finitely generated torsion-free A-module M is a direct summand of a finite free A-module. Deduce that if N is a second finitely generated torsion-free A-module then $M \otimes_A N$ is finitely generated and *torsion-free* as an A-module, and that for any multiplicative set S in A there is a natural map

$$S^{-1}(M \otimes_A N) \to S^{-1}M \otimes_{S^{-1}A} S^{-1}N$$

that is moreover an *isomorphism*.