Math 129 Problem Set 6

Lev Kruglyak

March 29, 2022

I collaborated with Ignasi Vicente for this problem set.

Problem (Spec).

(a) Show that if $f : R \to S$ is any ring homomorphism (assuming $f(1) = 1$), there is an induced map of sets $\widetilde{f} : \operatorname{Spec}(S) \to \operatorname{Spec}(R)$.

(b) Find an example of a ring homomorphism that isn't an isomorphism of rings, but induces a bijection of spectrums.

(c) Describe $\widetilde{f} : \operatorname{Spec}(S) \to \operatorname{Spec}(R)$ when $R = \mathbb{C}[t]$ and $S = \mathbb{C}[t,s]/(s^2 - t)$, where $f : \mathbb{C}[t] \to \mathbb{C}[t,s]/(s^2 - t)$ is the natural inclusion.

(a) Let $\mathfrak{q} \subset S$ be a prime ideal, and let $\mathfrak{p} = f^{-1}(\mathfrak{q})$. We claim that $\mathfrak{p}$ is a prime ideal of R. To see this, let $ab \in \mathfrak{p}$. This means that $f(ab) = f(a)f(b) \in \mathfrak{q}$ so $f(a) \in \mathfrak{q}$ or $f(b) \in \mathfrak{q}$. This means that $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, so $\mathfrak{p}$ is a prime ideal. Thus, we can define $\widetilde{f} : \mathfrak{q} \mapsto f^{-1}(\mathfrak{q})$.

(b) Consider the natural reduction map from $\mathbb{Z}/4\mathbb{Z}$ to $\mathbb{Z}/2\mathbb{Z}$. The only prime ideal of $\mathbb{Z}/4\mathbb{Z}$ is (2) and the only prime ideal of $\mathbb{Z}/2\mathbb{Z}$ is (0). Thus the reduction map induces a bijection between $\{(0)\}$ and $\{(2)\}$.

(c) First we'll calculate $\operatorname{Spec}(\mathbb{C}[t])$. Note that $\mathbb{C}$ is a field so $\mathbb{C}[t]$ is a principal ideal domain. Thus every ideal is of the form $(f(t))$ for some polynomial $f(t) \in \mathbb{C}[t]$. Thus, the prime ideals in $\mathbb{C}[t]$ are $(x - a)$ for $a \in \mathbb{C}$.

Claim. Let R be a ring and I an ideal in R. Let $f : R \to R/I$ be the natural surjection. Then $\widetilde{f} : \operatorname{Spec}(R/I) \to \operatorname{Spec}(R)$ is an inclusion mapping prime ideals in $\operatorname{Spec}(R/A)$ to prime ideals in $\operatorname{Spec}(R)$ containing I.

Proof. This follows from the correspondence theorem and the third isomorphism; note that $\mathfrak{p} \subset R/I$ then $f^{-1}(\mathfrak{p})$ is an ideal of R containing I. Since $(R/I)/\mathfrak{p}$ is an integral domain, so is $R/f^{-1}(\mathfrak{p}) = R/(If^{-1}(\mathfrak{p}))$. $\square$

Since $\operatorname{Spec}(\mathbb{C}[t,s])$ consists of ideals $(t - a, s - b)$ for $a, b \in \mathbb{C}$, the claim implies that the spectrum $\operatorname{Spec}(\mathbb{C}[t,s]/(s^2 - t))$ consists of the prime ideals of the form $(s - a)$ for $a \in \mathbb{C}$. Note that $f^{-1}((s - a)) = (t - a^2)$, so $\widetilde{f}$ sends $(t - a)$ to $(t - a^2)$ and obviously (0) is sent to (0).

Problem 3.28. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, all $a_i \in \mathbb{Z}$, and let p be a prime divisor of a_0. Let p^r be the exact power of p dividing a_0, and suppose all a_i are all divisible by p^r. Assume moreover that f is irreducible over $\mathbb{Q}$ (which is automatic if $r = 1$) and let α be a root of f. Let $K = \mathbb{Q}[\alpha]$.

(a) Prove that $(p^r) = p^r\mathcal{O}_K$ is the n^{th} power of an ideal in $\mathcal{O}_K$.

(b) Show that if r is relatively prime to n, then (p) is the n^{th} power of an ideal in R. Conclude that in this case p is totally ramified in $\mathcal{O}_K$.

(c) Show that if r relatively prime to n, then Δ_K is divisible by p^{n-1}. What can you prove if $(n, r) = m > 1$?

(a) Since $f(\alpha) = 0$, we can write

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha - a_0 = p^r\left(-\frac{a_{n-1}}{p^r}\alpha^{n-1} - \cdots - \frac{a_1}{p^r}\alpha - \frac{a_0}{p^r}\right).$$

Let's call this last term β so that $\alpha^n = p^r\beta$. Note that all of the terms a_i/p^r are integers, and $p \nmid a_0/p^r$. Let $\beta_i = -a_i/p^r$, so that $\beta = \beta_{n-1}\alpha^{n-1} + \cdots + \beta_1\alpha + \beta_0$. Note that $p \nmid \beta$, since otherwise we would have some polynomial $g(x) \in \mathbb{Z}[x]$ with $g(\alpha) = 0$ and $\deg g < \deg f$, a contradiction to the irreducibility of f. So (p^r) is coprime to (β). Then since $(\alpha)^n = (p^r)(\beta)$, it follows that $(p^r) = I^n$ for some ideal $I \subset \mathcal{O}_K$.

(b) Write $(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}$ for $\mathfrak{p}_i$ prime. Then $(p^r) = (p)^r = \mathfrak{p}_1^{re_1} \cdots \mathfrak{p}_k^{re_k}$. Since $(p^r) = I^n$ for some ideal by (a), it follows that $n \mid re_i$ for all i. Since $(n, r) = 1$, we have $n \mid e_i$ for all i. Thus (p) is an n-th power of an ideal of $\mathcal{O}_K$. By the decomposition equation $\sum_{i=1}^k e_i f_i = n$ yet $n \mid e_i$ so $e_i \geq n$. This means that $k = 1$, $e_1 = n$, and $f_1 = 1$. Thus $p\mathcal{O}_K = \mathfrak{p}_1^n$ so p is totally ramified.

(c) We'll address the case when r is relatively prime to n first. By (b), $p\mathcal{O}_K = \mathfrak{p}^n$ for a prime $\mathfrak{p} \subset \mathcal{O}_K$. By the decomposition equation we have $f(\mathfrak{p} \mid p) = 1$. By Problem 3.21b, Δ_K is divisible by p^k for $k = n - f(\mathfrak{q} \mid p) = n - 1$. So if r is relatively prime to n then $p^{n-1} \mid \Delta_K$.

In the case when $(n, r) = m > 1$, let $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}$. Then $n \mid e_i r$ so e_i is a multiple of n/m. By the decomposition equation $e_1 f_1 + \cdots + e_k f_k = n$. Then $\sum_i f_i \leq m$, and this maximum is achieved when all $e_i = n/m$. Then by Problem 3.21b, we have $p^{n-m} \mid \Delta_K$.

Problem 4.1. Show that $E(\mathfrak{q} \mid \mathfrak{p})$ is a normal subgroup of $D(\mathfrak{q} \mid \mathfrak{p})$ directly from the definition of these groups.

Let $\sigma \in E(\mathfrak{q} \mid \mathfrak{p})$ be some automorphism. By definition of the inertia group we have $\sigma(\alpha) - \alpha \in \mathfrak{q}$ for all $\alpha \in \mathcal{O}_L$. Then for any $\zeta \in D(\mathfrak{q} \mid \mathfrak{p})$ since $\zeta^{-1} \in \text{Gal}(L/K)$, it follows that $\zeta^{-1}(\alpha) \in \mathcal{O}_L$ so $\zeta(\sigma^{-1}(\alpha)) - \sigma^{-1}(\alpha) \in \mathfrak{q}$. Since ζ preserves the prime $\mathfrak{q}$, we have $\zeta(\sigma(\zeta^{-1}(\alpha)) - \sigma^{-1}(\alpha)) = \zeta\sigma\zeta^{-1}(\alpha) - \alpha$. Thus $\zeta\sigma\zeta^{-1} \in E(\mathfrak{q} \mid \mathfrak{p})$. This proves the normality of $E(\mathfrak{q} \mid \mathfrak{p})$ in $D(\mathfrak{q} \mid \mathfrak{p})$.

Problem 4.2. Suppose $D(\mathfrak{q} \mid \mathfrak{p})$ is a normal subgroup of $\text{Gal}(L/K)$. Then $\mathfrak{p}$ splits into r distinct primes in $L_{D(\mathfrak{q}|\mathfrak{p})}$. If $E(\mathfrak{q} \mid \mathfrak{p})$ is also normal in $\text{Gal}(L/K)$, then each of them remains prime (is "inert") in $L_{E(\mathfrak{q}|\mathfrak{p})}$. Finally, each one becomes an e^{th} power in L.

If $D(\mathfrak{q} \mid \mathfrak{p})$ is normal in $\mathrm{Gal}(L/K)$, then by the fundamental theorem of Galois theory, $L_{D(\mathfrak{q}|\mathfrak{p})}$ is a normal extension of K. We know that $\mathfrak{q}_{D(\mathfrak{q}|\mathfrak{p})}$ has ramification index and inertial degree 1 over $\mathfrak{p}$, hence so does every prime $\mathfrak{p}'$ in $L_{D(\mathfrak{q}|\mathfrak{p})}$ lying over $\mathfrak{p}$. So there must be exactly r such primes. It follows that there are exactly r primes in $L_{E(\mathfrak{q}|\mathfrak{p})}$ lying over $\mathfrak{p}$ since this is true in both $L_{D(\mathfrak{q}|\mathfrak{p})}$ and L. This implies that each $\mathfrak{p}$ lies under a unique primes $\mathfrak{p}''$ in $L_{E(\mathfrak{q}|\mathfrak{p})}$; however $\mathfrak{p}''$ might be ramified over $\mathfrak{p}'$. If $E(\mathfrak{q} \mid \mathfrak{p})$ is normal in $\mathrm{Gal}(L/K)$, then $e(\mathfrak{p}'' \mid \mathfrak{p}) = e(\mathfrak{q}_{E(\mathfrak{q}|\mathfrak{p})}) = 1$ hence $e(\mathfrak{p}'' \mid \mathfrak{p}') = 1$. This proves that $\mathfrak{p}'$ is inert in $L_{E(\mathfrak{q}|\mathfrak{p})}$, i.e. $\mathfrak{p}'' = \mathfrak{p}'(\mathcal{O}_L)_{E(\mathfrak{q}|\mathfrak{p})}$.

We claim that $\mathfrak{p}''$ becomes an e^{th} power in L. Let $\mathfrak{q}''$ be a prime of L lying over $\mathfrak{p}''$. By transitivity, $\mathfrak{q}''$ lies over $\mathfrak{p}$ so we have $e = e(\mathfrak{q}'' \mid \mathfrak{p}) = e(\mathfrak{q}'' \mid \mathfrak{p}'')e(\mathfrak{p}'' \mid \mathfrak{p}')e(\mathfrak{p}' \mid \mathfrak{p})$. Earlier, we showed that $e(\mathfrak{p}'' \mid \mathfrak{p}') = e(\mathfrak{p}' \mid \mathfrak{p}) = 1$; thus $e = e(\mathfrak{q}'' \mid \mathfrak{p}'')$. So $\mathfrak{p}''\mathcal{O}_L = (\mathfrak{q}_1 \cdots \mathfrak{q}_k)^e$ where $\mathfrak{q}_i$ are the primes of L lying over $\mathfrak{p}''$. Hence $\mathfrak{p}''$ is an e^{th} power in L.

Problem 4.10. Let K be a number field, and let L and M be two finite extensions of K. Assume that M is normal over K. Then the composite field LM is normal over L and the Galois group $\mathrm{Gal}(LM/L)$ is embedded in $\mathrm{Gal}(M/K)$ by restricting automorphisms to M. Let $\mathfrak{p} \subset \mathcal{O}_K, \mathfrak{n} \subset \mathcal{O}_L, \mathfrak{m} \subset \mathcal{O}_M$, and $\mathfrak{q} \subset \mathcal{O}_{LM}$ be primes such that $\mathfrak{n}$ lies over $\mathfrak{q}$ and $\mathfrak{m}$ and $\mathfrak{q}$ and $\mathfrak{m}$ lie over p.

(a) Prove that $D(\mathfrak{q} \mid \mathfrak{n})$ is embedded in $D(\mathfrak{m} \mid \mathfrak{p})$ by restricting automorphisms.

(b) Prove that $E(\mathfrak{q} \mid \mathfrak{n})$ is embedded in $E(\mathfrak{m} \mid \mathfrak{p})$ by restricting automorphisms.

(c) Prove that if $\mathfrak{p}$ is unramified in M, then every prime of L lying over $\mathfrak{p}$ is unramified in LM.

(a) Firstly if $\sigma \in D(\mathfrak{q} \mid \mathfrak{n})$, then by definition $\sigma(\mathfrak{q}) = \mathfrak{q}$. Let $\overline{\sigma} \in \mathrm{Gal}(M/K)$ be the restriction of σ to $M \subset LM$. Then $\overline{\sigma}(\mathfrak{q} \cap M) = \mathfrak{q} \cap M$ however $\mathfrak{q} \cap M = \mathfrak{m}$ so $\overline{\sigma}(\mathfrak{m}) = \mathfrak{m}$. This gives us a well defined map $D(\mathfrak{q} \mid \mathfrak{n}) \to D(\mathfrak{m} \mid \mathfrak{p})$. To prove that this map is injective, suppose $\overline{\sigma}$ is the identity on M, then σ is the identity on M. Similarly, σ is the identity on L so it must be the identity on the composite field LM. Thus there is an imbedding $D(\mathfrak{q} \mid \mathfrak{n}) \hookrightarrow D(\mathfrak{m} \mid \mathfrak{p})$.

(b) By (a), the natural restriction map $\mathrm{Gal}(LM/L)$ to $\mathrm{Gal}(M/K)$ is an injective homomorphism, so it suffices to show that the image of $E(\mathfrak{q} \mid \mathfrak{n})$ under this map is $E(\mathfrak{m} \mid \mathfrak{p})$. Let $\sigma \in E(\mathfrak{q} \mid \mathfrak{n})$. Then if $\sigma(\alpha) - \alpha \in \mathfrak{q}$ for all $\alpha \in \mathcal{O}_{LM}$, then for all $\alpha \in \mathcal{O}_M \subset \mathcal{O}_{LM}$ we have $\sigma(\alpha) - \alpha \in \mathfrak{q} \cap M = \mathfrak{m}$. Thus $\overline{\sigma} \in E(\mathfrak{m} \mid \mathfrak{p})$, and we have our embedding.

(c) Suppose $\mathfrak{p}$ is unramified in M. Let $\mathfrak{n}$ be a prime of $\mathcal{O}_L$ lying over $\mathfrak{p}$, and let $\mathfrak{q}$ be a prime of $\mathcal{O}_{LM}$ lying over $\mathfrak{n}$. Since M is Galois, Theorem 4.28 gives us the degree relation $e(\mathfrak{m} \mid \mathfrak{p}) = e(\mathfrak{m} \mid \mathfrak{m}_{E(\mathfrak{m}|\mathfrak{p})}) = [M : M_{E(\mathfrak{m}|\mathfrak{p})}]$ where $\mathfrak{m} = \mathfrak{q} \cap \mathcal{O}_M$. Since $\mathfrak{p}$ is unramified, $e(\mathfrak{m} \mid \mathfrak{p}) = 1$ so $[M : M_{E(\mathfrak{m}|\mathfrak{p})}] = |E(\mathfrak{m} \mid \mathfrak{p})| = 1$. By (b), $|E(\mathfrak{q} \mid \mathfrak{n})| \leq |E(\mathfrak{m} \mid \mathfrak{p})| = 1$ so $e(\mathfrak{q} \mid \mathfrak{n}) = 1$. Since LM is Galois over L, applying Theorem 4.28 gives us $e(\mathfrak{q} \mid \mathfrak{n}) = [LM : (LM)_{E(\mathfrak{q}|\mathfrak{n})}] = |E(\mathfrak{q} \mid \mathfrak{n})| = 1$. This proves that $\mathfrak{n}$ is unramified in LM.