Math 418, Spring 2024 – Practice Problems for Final Exam

8.2.2 *Prove that any two nonzero elements of a P.I.D. have a least common multiple*

Solution. Let I be the set of common multiples of a and b, and note that this forms an ideal, which is nonempty since $ab \in I$. I is principal, $I = (m)$, so m is a common multiple of a and b of which every other common multiple is in turn a multiple i.e. $m = lcm(a, b)$.

9.4.11 *Prove that $x^2 + y^2 - 1$ is irreducible in $\mathbb{Q}[x, y]$.*

Solution. If x^2+y^2-1 is reducible, it is the product of two linear factors $f = ax+by+c$ and $g = rx+sy+t$. We have $x^2+y^2-1 = arx^2+bsy^2+(as+br)xy+(at+cr)x+(bt+cs)y+ct$, so $ar = 1, bs = 1, ct = -1, as = -br, at = -cr$. The first three equations show that none of a, b, c, r, s, t can be 0, and the first, second, and fourth equations say that $ab^{-1} = -a^{-1}b$, which is impossible. [Note that since $\mathbb{Q}[x, y]$ is a UFD, this means that $(x^2 + y^2 - 1)$ is a prime ideal.]

13.2.15 *A field F is said to be* formally real *if -1 is not expressible as a sum of squares in F. Let F be a formally real field, let $f(x) \in F[x]$ be an irreducible polynomial of odd degree and let α be a root of $f(x)$. Prove that $F(\alpha)$ is also formally real.*

Solution. Suppose otherwise, and a counterexample α such that the degree of α over F is the minimum possible. Then $-1 = \beta_1^2 + \cdots + \beta_m^2$ for some choice of $\beta_i \in F(\alpha)$, Let the coset $p_i(x)+(f(x))$ be the image of β_i under the (inverse of the) isomorphism given in Theorem 6, and we choose the representatives p_i to have $\deg p_i < \deg f$ (otherwise, divide with remainder). Then we have

$$-1 + (f) = p_1^2 + \cdots + p_m^2,$$

where we have collected copies of the ideal (f). Pulling this back to the polynomial ring $F[x]$, we see that

$$-1 + f(x)g(x) = p_1^2 + \cdots + p_m^2 \tag{1}$$

for some polynomial $g \in F[x]$. Since the degree of the right side of (1) is even and less that $2 \deg f$, so must be the degree of the left side, so $\deg g$ is odd and less than $\deg f$.

Now, g may not be irreducible, but at least one of its irreducible factors must have odd degree. Let β be a root of such a factor $h(x)$; then β has odd degree over F. Under the maps $F[x] \to F[x]/(h) \to F(\beta)$, (1) becomes

$$-1 = \gamma_1^2 + \cdots \gamma_m^2$$

for elements $\gamma_i \in F(\beta)$. This means that $F(\beta)$ is also not formally real, and since $\deg \beta < \deg \alpha$, this contradicts the minimality of α.

13.5.8 *Prove that $f(x)^p = f(x^p)$ for any polynomial $f(x) \in \mathbb{F}_p[x]$.*

Solution. Recall the Frobenius endomorphism $a \mapsto a^p$. Since this is an endomorphism, we have $(a+b)^p = a^p + b^p$ in $\mathbb{F}_p$. Therefore, if $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$,

$$\begin{aligned} f(x)^p &= (a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0)^p \\ &= (a_n x^n)^p + \cdots + (a_1 x)^p + a_0^p \\ &= a_n x^p + \cdots + a_1 x^p + a_0 \\ &= f(x^p). \end{aligned}$$

14.1.6 *Let k be a field. Show that the automorphisms of $k[t]$ that fix k are precisely the maps $\phi(f(t)) = f(at+b)$, for $a, b \in k, a \neq 0$*

Solution. First let $a, b \in k, a \neq 0$, and let $\phi(f(t)) = f(at+b)$. ϕ is a homomorphism since $(f+g)(at+b) = f(at+b)+g(at+b)$, $fg(at+b) = f(at+b)g(at+b)$ (all evaluation maps are homomorphisms). ϕ is an isomorphism since its inverse is $f(t) \mapsto f((t-b)/a)$ and $a \neq 0$.

Conversely, let ϕ be any automorphism of $k[t]$ fixing k. ϕ is determined by the value $\phi(t) = f(t)$ (this is the action on the element $t \in k[t]$, which is sent to another polynomial, $f(t) \in k[t]$). Let $g(t) = \phi^{-1}(t)$. Then since ϕ is a homomorphism, we have

$$t = \phi(g(t)) = g(\phi(t)) = g(f(t)),$$

so since t is degree on, f and g must be degree one also.

14.2.23 *Let K be a Galois extension of F with cyclic Galois group of order n generated by σ. Suppose $\alpha \in K$ has $N_{K/F}(\alpha) = 1$. Prove that α is of the form $\alpha = \frac{\beta}{\sigma\beta}$ for some nonzero $\beta \in K$.*

Solution. As in the hint, choose $\theta \in K$ and let

$$\beta = \theta + \alpha\sigma(\theta) + \alpha\sigma(\alpha)\sigma^2(\theta) + \cdots + \alpha\sigma(\alpha)\cdots\sigma^{n-2}(\alpha)\sigma^{n-1}(\theta).$$

Then,

$$\sigma(\beta) = \sigma(\theta) + \sigma(\alpha)\sigma^2(\theta) + \sigma(\alpha)\sigma^2(\alpha)\sigma^3(\theta) + \cdots + \sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^{n-1}(\alpha)\theta,$$

so

$$\alpha\sigma(\beta) = \alpha\sigma(\theta) + \alpha\sigma(\alpha)\sigma^2(\theta) + \alpha\sigma(\alpha)\sigma^2(\alpha)\sigma^3(\theta) + \cdots + \theta = \beta,$$

noting that the product of all the Galois conjugates of α is $N_{K/F}(\alpha) = 1$.

This means that $\alpha = \frac{\beta}{\sigma(\beta)}$ as long as $\beta \neq 0$. By the linear independence of characters, $1, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ are linearly independent, so the character

$$\chi := 1 + \alpha\sigma + \alpha\sigma(\alpha)\sigma^2 + \cdots + \alpha\sigma(\alpha)\cdots\sigma^{n-2}(\alpha)\sigma^{n-1} \neq 0.$$

This means there exists some $\theta \in K$ such that $\beta := \chi(\theta) \neq 0$, and the above shows that $\alpha = \frac{\beta}{\sigma(\beta)}$.

15.2.8 *Suppose the prime ideal P contains the ideal I. Prove that P contains the radical of I.*

Solution. At least two ways to think about this. First, prime ideals are radical and radicals are inclusion-preserving, so $\sqrt{I} \subseteq \sqrt{P} = P$.

More directly, let $a \in \sqrt{I}$. Then $a^n \in I \subseteq P$ for some I, so $a \cdot a \cdots a \in P$. Since P is a prime ideal, whenever a (finite) product lives in P, one of its factors must live in P. In this case every factor is a, so $a \in P$.

CLO-8.3.1 (a) *Show that $I = (x^2y - x^3)$ is a homogeneous ideal in $k[x, y]$* **Solution.** Since I is principal, $f \in I$ is of the form $f = g(x^2y - x^3)$, $g \in k[x, y]$. Let f_i (resp. g_i) be the degree-i homogeneous component of f (resp. g), and then $f_0 = f_1 = 0 \in I$, and for $i \geq 2$, $f_i = g_{i-2}(x^2y - x^3) \in I$. Thus, I is a homogeneous ideal.

(b) *Show that $(f) \subseteq k[x_0, \ldots, x_n]$ is a homogeneous ideal if and only if f is a homogeneous polynomial* **Solution.** Similar argument to the first part. If f is homogeneous i.e. $f = f_m$ for some m, then if $g \in (f)$, $g = fh$, $g_i = 0$ for all $i < m$ and for $i \geq m$, $g_i = fh_{i-m} \in I$. Conversely, if f is not homogeneous, let f_m be the lowest nonzero homogeneous component of f. Since f is not homogeneous, $m < degf$, but every element g of (f) is a multiple of f and therefore $m < degf \leq degg$, so $f_m \notin (f)$, and so (f) is not a homogeneous ideal.

G-C *Galois correspondence for the following polynomials* [Note: below, we'll assume over $\mathbb{Q}$. Over a finite field, the extension degree of the splitting field is just the degree of the largest irreducible factor, and the Galois group is the cyclic group of the appropriate size. Try to think about how this works and how the roots of each irreducible factor get permuted.]

(a) $x^9 - 1$ **Solution.** Cyclotomic extension $\mathbb{Q}(\zeta_9)/\mathbb{Q}$. $G = (\mathbb{Z}/9\mathbb{Z})^\times$, which is abelian of order 6, so it must be $C_6 = \langle\sigma\rangle$, where $\sigma : \zeta \mapsto \zeta^2$. Subgroups are $1, \langle\sigma^3\rangle, \langle\sigma^2\rangle$, and G. The middle two don't contain each other. To compute the fixed fields, try periods. $\mathrm{Fix}\langle\sigma^3\rangle = \mathbb{Q}(\zeta_9 + \sigma^3\zeta_9) = \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$. Check degrees: the minimal polynomial of ζ_9 over this field is $x^2 - (\zeta_9 + \zeta_9^{-1})x + 1$, so the degree is correct. On the other hand, for the other subgroup, $\zeta_9 + \sigma^2\zeta_9 + \sigma^4\zeta_9) = \zeta_9 + \zeta_9^4 + \zeta_9^7 \in \mathrm{Fix}\langle\sigma^3\rangle$ but this doesn't help because it's 0: $\zeta_9 + \zeta_9^4 + \zeta_9^7 = \zeta_9(1 + \zeta_3 + \zeta_3^2) = 0$. So we want to find any element of degree 2 in $\mathbb{Q}(\zeta_9)$ since there's only one intermediate field of this degree. One such element is ζ_3 since $\sigma^2(\zeta_3) = \sigma^2(\zeta_9)^3 = \zeta_9^3 = \zeta_3$. (This shouldn't be surprising, since cube roots are 9th roots, so $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_3) \subseteq \mathbb{Q}(\zeta_9)$. Since G is abelian, every subgroup is normal, so every subextension is Galois.

(b) $x^6 - 2$ **Solution.** Irreducible by Eisenstein with prime 2. Here, $K = \mathbb{Q}(\zeta_6, \sqrt{2})$. Only 1 and 5 are less than and coprime to 6. and so $\Phi_6(x) = (x - \zeta_6)(x - \zeta_6^{-1})$. Since $\zeta_6 \notin \mathbb{R}$, $K/\mathbb{Q}$ is degree 4 and $G = C_2 \times C_2$, with nonidentity elements

$\sigma : \sqrt{2} \mapsto -\sqrt{2}, \zeta_6 \mapsto \zeta_6$, $\tau : \sqrt{2} \mapsto \sqrt{2}, \zeta_6 \mapsto -\zeta_6$ $\sigma\tau : \sqrt{2} \mapsto -\sqrt{2}, \zeta_6 \mapsto -\zeta_6$. Subgroups are the identity, G, and the order-2 subgroups generated by each nonidentity element. Each of these subgroups fixes exactly one of $\sqrt{2}, \zeta_6, \zeta_6\sqrt{2}$. Again, G is abelian, so everything in sight is normal/Galois.

(c) $x^3 + x + 1$ **Solution.** Irreducible since no root modulo 2. Discriminant is $D = -4 \cdot 1^2 - 27 \cdot 1^2 = -31$, which is not a square in $\mathbb{Q}$, so $G = S_3$. We don't know the roots directly unless you use Cardano's formula, so call them α, β, γ. Without loss of generality, $\langle(12)\rangle$ has fixed field $\mathbb{Q}(\gamma)$, $\langle(13)\rangle$ has fixed field $\mathbb{Q}(\beta)$, and $\langle(23)\rangle$ has fixed field $\mathbb{Q}(\alpha)$. $A_3 = \langle(123)\rangle$ has fixed field $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{-31})$. The trivial subgroup fixes K and G fixes only $\mathbb{Q}$. Of the proper nontrivial subgroups of G, only A_3 is normal, so $\mathbb{Q}(\sqrt{-31})/\mathbb{Q}$ is Galois, but $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\beta)$, and $\mathbb{Q}(\gamma)$ are not Galois over $\mathbb{Q}$.

(d) $(x^2 - x - 1)(x^2 - 5)$ **Solution.** K is a composite extension of the splitting fields of these two factors. Since they're both degree 2, their splitting fields are either identical or intersect in $\mathbb{Q}$. By the quadratic formula, $x^2 - x - 1$ has roots $\frac{1 \pm \sqrt{5}}{2}$, so its splitting field is actually $\mathbb{Q}(\sqrt{5})$, the same as the splitting field of $x^2 - 5$. Therefore, $K = \mathbb{Q}(\sqrt{5})$, $G = C_2$, and there are no proper nontrivial subgroups or intermediate fields.

(In general, for a composite extension like this one, you may need to use the method in Problem 2 of Homework 9.)