Math 418, Spring 2025 – 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 $I = (x^2 y - x^3)$ is a homogeneous ideal in $k[x, y]$*
Solution. Since I is principal, $f \in I$ is of the form $f = g(x^2 y - x^3)$, $g \in k[x, y]$. Let f_i (resp. g_i) be the degree-i homogeneous component of f (resp. g), and then $f_0 = f_1 = f_2 = 0 \in I$, and for $i \geq 3$, $f_i = g_{i-3}(x^2 y - x^3) \in I$. 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 $i \geq m$, $g_i = f h_{i-m} \in I$. Conversely, if f is not homogeneous, let f_m be the lowest nonzero homogeneous component of f. Since f is not homogeneous, $m < deg f$, but every element g of (f) is a multiple of f and therefore $m < deg f \leq deg g$, so $f_m \notin (f)$, and so (f) is not a homogeneous ideal.

Scheme Describe the scheme Spec $\mathbb{Z}$ to the level discussed in class. That is, say what the set of points is, what the functions on Spec $\mathbb{Z}$ are, how to evaluate a function at a point of Spec $\mathbb{Z}$, and what the sets of functions are on each of the sets $D(f)$.

Solution. The set of points in Spec $\mathbb{Z}$ is just the set of prime ideals of $\mathbb{Z}$, which is (p) for p a positive prime number, and (0). The functions on Spec $\mathbb{Z}$ are by definition the elements of $\mathbb{Z}$, and given some $f \in \mathbb{Z}$ and some $I \in$ Spec $\mathbb{Z}$, we have $f(I) = f$ mod $p \in \mathbb{F}_p$ if $I = (p)$, and $f(I) = 0$ if $I = (0)$.

Let $f \in \mathbb{Z}$; then $D(f)$ is the set of points I of Spec $\mathbb{Z}$ such that $f(I) \neq 0$. This is exactly the set of prime ideals (p) such that f is not a multiple of p. The functions on $D(f)$ are rational numbers $\frac{a}{b}$ such that b is a power of f. Since a can cancel some factors from f, we can refine this description to the following: the functions on $D(f)$ are rational numbers $\frac{a}{b}$ such that every prime factor of b is a prime factor of f. (Note that we will only evaluate $\frac{a}{b}$ on $D(f)$, meaning in finite fields F_p such that p doesn't divide b.)

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. The splitting field is $K = \mathbb{Q}(\zeta_6, \sqrt[6]{2})$. Since ζ_6 has degree 2 over $\mathbb{Q}$ and $\sqrt[6]{2}$ has degree 6 over $\mathbb{Q}$. $6 \le [K : \mathbb{Q}]2 \cdot 6$. But $\mathbb{Q}(\sqrt[6]{2} \subseteq \mathbb{R}$ and $\zeta_6 \notin \mathbb{R}$, so $[K : \mathbb{Q}] = 12$. Let $\sigma(\sqrt[6]{2})\zeta_6\sqrt[6]{2}, \sigma(\zeta_6) = \zeta_6$ and $\tau(\sqrt[6]{2}) = \sqrt[6]{2}, \tau(\zeta_6) = \zeta_6^{-1}$. Then σ has order 6 and τ has order 2. We also have $\tau\sigma(\sqrt[6]{2}) = \tau(\zeta_6\sqrt[6]{2}) = \zeta_6^{-1}\sqrt[6]{2}, \tau\sigma(\zeta_6) = \tau(\zeta_6) = \zeta_6^{-1}$ and $\sigma^a\tau(\sqrt[6]{2}) = \sigma^a(\sqrt[6]{2}) = \zeta_6^a\sqrt[6]{2}, \sigma^a\tau(\zeta_6) = \sigma^a(\zeta_6^{-1}) = \zeta_6^{-1}$, so we have $\tau\sigma = \sigma^5\tau$.

As a consequence of these relations, we have a group of order 12, which therefore must be all of G. Precisely,

$$G = \langle \sigma, \tau \rangle = \{\sigma^a\tau^b | 0 \le a < 6, 0 \le b < 2\}.$$

G is isomorphic to the dihedral group D_{12}.

G has 16 subgroups, so we won't consider them all (see here for all subgroups). For any a, $(\sigma^a\tau)^2 = \sigma^a\tau\sigma^a\tau = \sigma^a\sigma^{-a}\tau\tau = 1$, so every element that is not in $\langle \sigma \rangle$ has order 2. This allows us to construct all the subgroups, by taking subgroups of $\langle \sigma \rangle$ along with elements of $G \setminus \langle \sigma \rangle$.

Let's do a couple of examples. Let $H_1 = \langle \sigma^2 \rangle$. $\sigma^2(\sqrt[6]{2}) = \zeta_6^2\sqrt[6]{2}$, so $\sigma^2(\sqrt{2}) = \zeta_6^6\sqrt{2} = \sqrt{2}$, and we have $Fix\langle \sigma^2 \rangle = \mathbb{Q}(\sqrt{2}, \zeta_6)$. H_1 is normal since $\tau\sigma^2\tau^{-1} = \sigma^{-2} \in H_1$, so $\mathbb{Q}(\sqrt{2}, \zeta_6)$ is Galois over $\mathbb{Q}$.

As a second example, let $H_2 = \langle \sigma\tau, \sigma^4\tau \rangle = \{1, \sigma\tau, \sigma^4\tau, \sigma^3\}$. From the previous example, we might guess at the element $\sqrt[3]{2}$; however, $\sigma\tau(\sqrt[3]{2}) = \zeta_6^2\sqrt[3]{2}$. So let's try another cube root of 2: $\sigma\tau(\zeta_6^4\sqrt[3]{2}) = \sigma(\zeta_6^2\sqrt[3]{2}) = \zeta_6^4\sqrt[3]{2}$. In addition, $\sigma^3(\zeta_6^4\sqrt[3]{2}) = \zeta_6^4\sqrt[3]{2}$, and for good measure, $\sigma^4\tau(\zeta_6^4\sqrt[3]{2}) = \sigma^4(\zeta_6^2\sqrt[3]{2}) = \zeta_6^4\sqrt[3]{2}$. H_2 is not normal since $\tau\sigma\tau\tau^{-1} = \sigma^5\tau \notin H_2$, so (as we knew), $\mathbb{Q}(\zeta_6^4)/\mathbb{Q}$ is not a Galois extension.

(c) $x^3 + x + 1$

Solution. Irreducible since no root modulo 2. Discriminant is $D = -4 \cdot 1^2 -$

4

$27 \cdot 1^2 = -31$, 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.)