Questions

Hui Sun

August 5, 2025

Problem 0.1. To see whether a polynomial is irreducible over $\mathbb{Q}$, is it sufficient to test whether $f \mod p$ is irreducible over any prime p?

For example, $x^5 - 5x^3 + 1$.

Proof. Yes. The converse is not true, consider the minimal polynomial for $\sqrt{2} + \sqrt{3}$. □

Problem 0.2. In the above example, how do we know that the Galois group contains an element of order 5? (It is clear why it contains a transposition because there exists complex roots).

Proof. This is because the Galois group G acts transitively on the set of roots, by the Orbit stabilizer theorem, we know

$$|G| = |\text{Orbit}(\alpha)| \cdot |\text{Stab}(\alpha)| = 5 \cdot |\text{Stab}(\alpha)|$$

i.e., 5 divides $|G|$. By Cauchy's theorem, there exists an element of order 5 in G, i.e., a 5-cycle. □

Problem 0.3. The Galois action on the set of roots implies for any root r of the irreducible polynomial (where G is the splitting field of), we must have

$$\text{Orbit}(r) = \{ \text{ set of all roots} \}$$

Proof. Yes, by defiition of a transitive action. □

Problem 0.4. Is it true that if I, J are ideals of a ring R, then

$$\frac{R}{I} \otimes_R \frac{R}{J} = \frac{R}{(I+J)}$$

in the case where $R = \mathbb{Q}[x]$, and I, J are irreducible polynomials, we have

$$\frac{R}{(f)} \otimes_R \frac{R}{(g)} = \frac{R}{(f)+(g)} = \frac{R}{\gcd(f,g)}$$

Problem 0.5. Fall 2014 Q2, $\text{Hom}_R(M, N)$.

Problem 0.6. $\mathbb{Z}/55\mathbb{Z}$.

Proof. We have $n_{11} = 1$, and we can write G as a semidirect product

$$G = \frac{\mathbb{Z}}{11\mathbb{Z}} \rtimes_\theta \frac{\mathbb{Z}}{5\mathbb{Z}}$$

where $\theta : \frac{\mathbb{Z}}{5\mathbb{Z}} \to \left(\frac{\mathbb{Z}}{11\mathbb{Z}}\right)^\times$. We know $\theta(1)$ needs to be sent to an elemennt of order 5, which includes $3, 4$.

$$G = \langle g, h : g^{11} = h^5 = e, hgh^{-1} = g^3 \rangle$$

and

$$G = \langle g, h : g^{11} = h^5 = e, hgh^{-1} = g^4 \rangle$$

□

Problem 0.7. Is cyclotomic extension cyclic.

Proof. No, consider $\mathbb{Q}(\zeta_8)$, then the Galois group is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. □

Problem 0.8. If an intermediate field extension of a Galois extension has order a, $k \subset E \subset K$ has $[E : k] = a$, then the subgroup that fixes E has index a.

Problem 0.9. Find all intermediate fields when the Galois group is $\mathbb{Q}(\zeta_9)$.

Problem 0.10. Find all the intermediate fields when the Galois group is D_8.

Problem 0.11. S2013-Q6(b)(c), S2016-Q3

Problem 0.12. Solvable by radicals, f2014-Q1 (polynomial), f2006-Q2 (field)

Problem 0.13. F2010-Q3

Problem 0.14. Review orbit-stabilizer theorem.

Problem 0.15. Map S_4 onto S_3 first for the irreducible rep.

Proof. Can only do it for the 2 dimensional irred character. □

Problem 0.16. Relationship between abelianization and $z(G)$. Why is p^3 nonabelian group has $[G, G] = p$.

Proof. Find the smallest normal subgroup H such that G/H is abelian. The smallest in this case is $Z(G)$. □

Problem 0.17. Irreducible rep of a cyclic group over $\mathbb{R}$ is ≤ 2.

Proof. □

Problem 0.18. Schur's lemma on simple modules over a semisimple ring.

$$\mathrm{End}_A(S) \cong \mathbb{C}$$

where S is a simple module. also like, irreducible, simple.

Problem 0.19. S2003-Q3, S2011-Q4

Problem 0.20. Isomorphism class of groups of order 360, page 238 aluffi.

Problem 0.21. Can I write all free R-modules as R^n

Problem 0.22. columns of the character table, sums of squares is $|G|/[(c)]$?

Problem 0.23. $\frac{K[t]}{(f(t))}$ is simple? is equal to $k(\alpha)$ for some α s.t. $f(\alpha) = 0$.

Problem 0.24. since ext $k(\alpha)$ always factors over k? is $k(\alpha)$ be the splitting field for all α s.t. $f(\alpha) = 0$ is a root? no. nononono.

Problem 0.25. Theorem 5.1

Problem 0.26. $x^4 + 1$ is reducible over all $\mathbb{F}_p$ for any p

Problem 0.27. relationship between D_n, A_n, galois

Problem 0.28. Degree p irred polynomial, what is the degree of the splitting field? $p!$?

Problem 0.29. normal basis theorem: connection w galois theory and linear alg

Chapter 1

Aluffi

Chapter VII: Fields.
Section 1: 5, 11, 14, 23
not done yet: 5

Chapter 2

Random Facts

Proposition 2.1. If $R \subset F$ is a subring of a field, then R is an integal domain. Moreover, if $k \subset R \subset F$ where F/k is an algebraic extension, then R is a subfield.

Proposition 2.2. $\mathbb{F}_4$ embeds into $\mathbb{F}_{16}$, more generally, if the order allows (as a vector space over $\mathbb{F}_2$), then it embeds.

Proposition 2.3. $\mathbb{F}_8/\mathbb{F}_2$ is a Galois extension and the Galois group is generated by the Frobenius transformation $\sigma : a \mapsto a^2$, $\{e, \sigma, \sigma^2\}$.

Recall the equivalent defn of Galois: let $k \subset E$ be a field extension, if $[E : k] = |\mathrm{Aut}_k(E)|$, then the extension is Galois.

Proposition 2.4. You tend to forget Cayley-Hamilton. Let p be the characteristic polynomial of some linear transformation T, then

$$p(T) = 0$$

Proposition 2.5. Let $I, J \subset R$ be ideals, then

$$J + I \subset R/I$$

is also an ideal. For example, one could use this to show that if R is Noetherian, then R/I is also Noetherian.

Proposition 2.6. Let V be a finite dimensional vector space, let $T, S : V \to V$ be diagonalizable operators, if

$$TS = ST$$

then T, S can be simultaneously diagonalized: in other words, V has a basis containing eigenvectors of both T and S.

Proposition 2.7. Every ideal/element in a nonzero ring is contained in some maximal ideal $\mathfrak{m}$.

Proposition 2.8. Each group has two interesting actions on itself: left-multiplcation and conjugation. Try both if needed!