Prelim Workshop
Summer 2018

Algebra Worksheet 3: Rings II

Fields and field extensions (6.12.14, 6.12.15)

- Degree of a field extension, multiplicativity of degree, transcendental extensions (6.12.16)
- Frobenius endomorphism (6.12.10)
- Algebraic closure: of a finite field? Of $\mathbb{Q}$? Of $\mathbb{R}$?
- Finite subgroup of multiplicative group of a field is cyclic (6.12.5, 6.12.22)
- Automorphisms of $\mathbb{F}_{p^n}^k$ (6.12.19)

Number theory

- Euler's function: multiplicativity, as order of $(\mathbb{Z}/n\mathbb{Z})^*$. (6.13.20)
- Solving congruences modulo n by working in the group of units modulo n. Euler's theorem. Check cases. (6.13.8, 6.13.17)

6.12.5 • Prove that a finite subgroup of the multiplicative group of a field is cyclic.

6.12.10 • Let F be a field of characteristic $p > 0$, $p \neq 3$. If α is a zero of the polynomial $f(x) = x^p - x + 3$ in an extension field of F, show that $f(x)$ has p distinct zeros in the field $F(\alpha)$.

6.12.14 • Exhibit infinitely many pairwise nonisomorphic quadratic extensions of $\mathbb{Q}$ and show they are pairwise nonisomorphic.

6.12.15 • Let $\mathbb{Q}$ be the field of rational numbers. For θ a real number, let $F_\theta = \mathbb{Q}(\sin\theta)$ and $E_\theta = \mathbb{Q}(\sin\frac{\theta}{3})$. Show that E_θ is an extension field of F_θ and determine all possibilities for $\dim_{F_\theta} E_\theta$. (Use trigonometric identities.)

6.12.16 • Show that the field $\mathbb{Q}(t_1, ..., t_n)$ of rational functions in n variables over the rational numbers is isomorphic to a subfield of $\mathbb{R}$.

6.12.19 • Let $\mathbb{F}$ be a finite field of cardinality p^n, with p prime and $n > 0$, and let G be the group of invertible 2×2 matrices with coefficients in $\mathbb{F}$. (1) Prove that G has order $(p^{2n} - 1)(p^{2n} - p^n)$. (2) Show that any p-Sylow subgroup of G is isomorphic to the additive group of F.

6.12.22 • Let p be a prime and $\mathbb{F}_p$ the field of p elements. How many elements of $\mathbb{F}_p$ have square roots in $\mathbb{F}_p$? Cube roots? (You may separate into cases for p.)

6.13.8 • Let $n \geq 2$ be an integer such that $2^n + n^2$ is prime. Prove that

$$n \equiv 3 \mod 6.$$

6.13.17 • Determine the rightmost decimal digit of

$$A = 17^{17^{17}}.$$

6.13.20 • Let ϕ be Euler's function. Let a and k be two integers, with $a > 1, k > 0$. Prove that k divides $\phi(a^k - 1)$.