Fields and Polynomials. HW #1.

Prof. D. Shapiro   Ross Program 2015.

Review the definitions of the following terms:
commutative ring, integral domain, field, vector space, dimension.

If R is a domain, and $p \in R$, what does it mean to say that p is irreducible? That p is prime?

P1. PODASIP. Let $f(x) = x^2 - 5$.
(1) f is irreducible over $\mathbb{Q}$ but not over $\mathbb{R}$.
(2) f is irreducible over $\mathbb{Q}(\sqrt{d})$ for every integer d coprime to 5.
(3) If p is prime let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, the field of p elements. f is irreducible over $\mathbb{F}_3, \mathbb{F}_7$ and $\mathbb{F}_{13}$ but not over $\mathbb{F}_{11}$ or $\mathbb{F}_{19}$. For which p is f is irreducible over $\mathbb{F}_p$?

P2. Lemma. A polynomial of degree n in $R[x]$ has at most n zeros in R.
True if R is a domain, but $x^2 + x$ has more more than 2 zeros in $\mathbb{Z}/6\mathbb{Z}$.
Let R is a commutative ring. PODASIP: If every monic polynomial of degree 2 in $R[x]$ has at most 2 zeros in R, then R must be an integral domain. [Answer: R is a domain, $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{F}_2[x]/(x^2)$.]

P3. PODASIP. Suppose $K \subseteq L$ are fields. Then,
Every $\theta \in L$ has degree ≤ 2 over $K \Rightarrow [L : K] = 2$.

P4. $\zeta = e^{2\pi i/5}$ is a zero of $x^5 = 1$. The zeros of $x^4 + x^3 + x^2 + x + 1$ are ζ, ζ^2, ζ^3 and ζ^4.
(1) Let $\alpha = \zeta + \zeta^{-1} = 2\cos(2\pi/5) = 2\cos(72°)$. Then $\alpha^2 = \zeta^2 + 2 + \zeta^{-2}$.
Since $\zeta^2 + \zeta + 1 + \zeta^{-1} + \zeta^{-2} = 0$, deduce: $\alpha^2 + \alpha - 1 = 0$ and $\alpha = \frac{-1+\sqrt{5}}{2}$.
(2) Then $\cos(2\pi/5) = \frac{-1+\sqrt{5}}{4}$, $\quad \sin(2\pi/5) = \sqrt{\frac{5+\sqrt{5}}{4}}$, $\quad \tan(2\pi/5) = \sqrt{5 + 2\sqrt{5}}$.
(3) Express $\sqrt{5}$ as a linear combination $c_1\zeta + c_2\zeta^2 + c_3\zeta^3 + c_4\zeta^4$, for some $c_j \in \mathbb{Q}$.
[Note: $\sqrt{5} = 2\alpha + 1 = 2(\zeta + \zeta^{-1}) + 1$.]

P5. Cubic Formula says: $x^3 + px + q$ has a zero $\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$.

Since $x^3 + 6x - 20$ has $x = 2$ as its the only real solution we find:

$$\sqrt[3]{6\sqrt{3} + 10} - \sqrt[3]{6\sqrt{3} - 10} = 2.$$

- Is $10 + 6\sqrt{3}$ a cube in $\mathbb{Q}(\sqrt{3})$?

Check other numerical examples like $(20 + 14\sqrt{2})^{\frac{1}{3}} + (20 - 14\sqrt{2})^{\frac{1}{3}} = 4$, and $(\sqrt{5} + 2)^{\frac{1}{3}} - (\sqrt{5} - 2)^{\frac{1}{3}} = 1$.

- Do those terms turn out to be perfect cubes as well?

Fields and Polynomials. HW #2.

Prof. D. Shapiro Ross Program 2015.

Supply details to prove the following results.

Proposition. *For a commutative ring R, let $f(x) \in R[x]$ and $c \in R$.*
(0) There exist $q(x) \in R[x]$ such that $f(x) = (x - c)q(x) + f(c)$.
(1) If $c_1, \ldots, c_k \in R$ have unit differences (every $c_i - c_j \in R^\times$), then:

$$f(c_j) = 0 \text{ for every } j \implies (x - c_1) \cdots (x - c_k) \mid f(x) \text{ in } R[x].$$

(2) A polynomial of degree n in $R[x]$ has at most n zeros in R, provided R is a domain.

Definition. *Suppose D is an integral domain, and $p, a, b \in D$.*
D is a factorial domain *or a UFD (unique factorization domain) if every nonzero $d \in D$ can be expressed as $d = up_1 \ldots p_r$ where $u \in R^\times$ is a unit, and each p_i is irreducible in D; and such an expression is unique up to unit multiples and permutation of the factors.*

Exercise 1. *(1) Suppose D is a Euclidean domain, that is, D admits a division algorithm.*
[Definition: There is $\delta : D \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ with the property:
for nonzero $a, b \in D$ there exists $q \in D$ such that either $a - bq = 0$ or $\delta(a - bq) < \delta(b)$.]
Then every ideal of D is principal. That is: D is a principal ideal domain, or PID.

(2) If D is a PID then D is factorial.

(3) Every prime is irreducible.
If D is factorial, then every irreducible is prime.

Find a domain containing an irreducible that is not prime.

(4) If D is a domain in which every irreducible is prime, must D be factorial?

Exercise 2. *Suppose domain D contains a element that is not zero, not a unit, not irreducible, and cannot be expressed as a product of irreducibles. Show:*
There exists an infinite ascending chain of principal ideals $J_1 \subset J_2 \subset \cdots$ in D.
If every ideal of D is finitely generated, then D has is no infinite ascending chain of ideals.

For nonzero a, b in a factorial domain D, define their *greatest common divisor* $\gcd(a, b)$. Explain why the GCD is "really" an element of $D/D^\times$. Does it follow that $\gcd(da, db) = d \gcd(a, b)$? We say that a list $a_1, \ldots, a_n$ is coprime if $\gcd(a_1, \ldots, a_n) = 1$.

Let K be the field of fractions of the factorial domain D. (Definition?) Every $a \in K^\times$ c is a fraction $a = r/s$ where $r, s \in D$ are coprime and $s \neq 0$. Extend definitions to make sense of $\gcd(a_1, \ldots, a_r)$ when the $a_j \in K^\times$. Is this GCD really in $K^\times/D^\times$?

Definition. *Suppose D is a factorial domain with $K = Frac(D)$. Polynomial $f(x) \in K[x]$ is called* primitive *if its coefficients form a caprime set in D.*

Lemma. *Suppose $0 \neq f(x) \in K[x]$, for D and K as above. Then there exists $c \in K^\times$ such that $f(x) = cf_1(x)$ and $f_1 \in D[x]$ is primitive. The values $c = c(f)$ and f_1 are uniquely determined, up to a multiplied factor in $D^\times$.* *$c(f)$ is called the* content *of f.*

Gauss's Lemma:

Lemma. *A product of primitive polynomials is primitive. If $f, g \in K[x]$ are nonzero then:*

$$c(fg) = c(f)c(g) \qquad \text{in } K^\times/D^\times.$$

Exercise 3. *Suppose $D \subseteq L$ where D is a factorial domain and L is a field. Suppose $f, g \in D[x]$ are primitive and $f = gh$ in $L[x]$. Then $h \in D[x]$ is primitive.*

Exercise 4. *Prove: An irreducible element of $\mathbb{Z}[x]$ is either a prime number $p \in \mathbb{Z}^+$ or is a primitive polynomial $\pi(x) \in \mathbb{Z}[x]$ that is irreducible in $\mathbb{Q}[x]$. Does this generalize to any factorial domain?*

Theorem. *If D is a factorial domain then $D[x]$ is also a factorial domain.*

For example, $\mathbb{Z}[x, y]$ and $\mathbb{R}[x_1, \ldots, x_n]$ are factorial domains.

Exercise 5 (Eisenstein.)**.** *(1) Suppose $f \in \mathbb{Z}[x]$ and $f \equiv x^n \pmod p$ for some prime p. If $f(0)$ is not a multiple of p^2, then f is irreducible in $\mathbb{Q}[x]$.*

(2) Suppose $c \in \mathbb{Z}$ with prime factor p such that $p^2 \nmid c$. Every n, $x^n - c$ is irreducible in $\mathbb{Q}[x]$.

(3) If p is prime then $\Phi_p(x) = x^{p-1} + \cdots + x + 1 = \frac{x^p - 1}{x - 1}$ is irreducible in $\mathbb{Q}[x]$.

Fields and Polynomials. HW #3.

Prof. D. Shapiro   Ross Program 2015.

P1. Lemma Suppose $K \subseteq L$ are fields and $\alpha \in L$. The following are equivalent:

1. α is algebraic over K.
2. $K[\alpha]$ is finite dimensional as a K-vector space.
3. There exists a finite extension field L/K with $\alpha \in L$.
4. $K[\alpha]$ is a field.

P2. (New Rings from Old.) An element c in a commutative ring R is "regular" if it can be canceled: $cr = cs \;\Rightarrow\; r = s$. Equivalently: c is not a zero-divisor. Suppose $S \subseteq R$ is a subset of regular elements. Explain how to define a new ring $S^{-1}R$ that consists of all fractions r/s where $r \in R$ and $s \in S$. Desired properties are:

(1) $R \subseteq S^{-1}R$ is a subring.

(2) Every $s \in S$ has in inverse in $S^{-1}R$.

(3) If a ring homomorphism $\varphi : R \to A$ has $\varphi(S) \subseteq A^{\times}$ (i.e. every $\varphi(s)$ is invertible in A), then φ extends to a ring homomorphism $\widehat{\varphi} : S^{-1}R \to A$.

If D is a domain, then its *field of fractions* $K = Frac(D)$ is formed as $S^{-1}D$ where $S = D \setminus \{0\}$.

P3. Suppose K is a field containing the p roots of $X^p - 1$. Here, p is a prime number.

- If $c \in K$ and $x^p - c$ has no root in K, then it is irreducible in $K[x]$.

Does this result generalize to non-prime exponents? [Hint: Look at $x^4 + 4$.]

P5. Euclidean tools. We allow geometric constructions using a compass and an unmarked straightedge, with a unit-length segment given. If a segment of length r can be constructed using those tools, then we say that r and $-r$ are *constructible number*. Let Co be the set of all constructible numbers.
Show: Co is a subfield of $\mathbb{R}$ and: If $a > 0$ is in Co then $\sqrt{a} \in Co$.

Moreover, if $\alpha \in Co$ then $\mathbb{Q}(\alpha) \subseteq K$ for some field extension $K/\mathbb{Q}$ that is the top of a tower of quadratic extensions. In particular, $\deg(\alpha) = 2^m$ for some m.

Deduce that a line segment of length $\sqrt[3]{2}$ is not a constructible.

P6. Find the degree of the algebraic number $\beta_n = \cos(2\pi/n)$.
[Assume the famous theorem: The cyclotomic polynomial $\Phi_n(X)$ is irreducible in $\mathbb{Q}[X]$.]

Which regular n-gons are constructible with Euclidean tools?

Fields and Polynomials. HW #4.

Prof. D. Shapiro   Ross Program 2015.

P1. Suppose K is a field that contains a root ω of $X^2 + X + 1$.
If d in K is not a cube, let $L = K(\theta)$ where $\theta^3 = d$. The minimal polynomial $m_\theta(X) = X^3 - d$ has zeros $\theta, \omega\theta, \omega^2\theta$ in L. There is a K-automorphism $\sigma : L \to L$ with $\sigma(\theta) = \omega\theta$. If $\alpha = x + y\theta + z\theta^2$, then $\sigma(\alpha) = x + y\omega\theta + z\omega^2\theta^2$, and:

$$Tr_{L/K}(\alpha) = 3x, \quad \text{and} \quad N_{L/K}(\alpha) = x^3 + dy^3 + d^2z^3 - 6xyzd.$$

P2. (1) For $a, b \in \mathbb{Q}^*$, find all the quadratic subfields of $\mathbb{Q}(\sqrt{a}, \sqrt{b}\,)$.
(2) For which $d \in \mathbb{Q}$ does $\sqrt[3]{d} \in \mathbb{Q}(\sqrt[3]{2})$?
(3) What pure cube roots $\sqrt[3]{c}$ lie in the field $\mathbb{Q}(\sqrt[3]{5}, \sqrt[3]{6})$?
[Clue: If $\sqrt{d} \in L$ for some non-square $d \in \mathbb{Q}$, does $Tr_{L/\mathbb{Q}}(\sqrt{d}) = 0$?]

P3. Show that the square roots of the primes are linearly independent over $\mathbb{Q}$.
Let p_n be the n^{th} prime number and $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \ldots, \sqrt{p_n})$. Does $[K : \mathbb{Q}] = 2^n$?
If $a_j \in K$ and $L = K(\sqrt{a_1}, \ldots, \sqrt{a_n})$, when does it follow that $[L : K] = 2^n$?

P5. Assume: The cyclotomic polynomial $\Phi_n(x)$ is irreducible over $\mathbb{Q}$.
Then for $\zeta = e^{2\pi i/n}$ and $K = \mathbb{Q}(\zeta)$, then $[K : \mathbb{Q}] = \varphi(n)$.
Compute $N_{K/\mathbb{Q}}(\zeta)$ and $Tr_{K/\mathbb{Q}}(\zeta)$.

P6. $f \in \mathbb{R}[X]$ is *positive semi-definite* (PSD) if $f(c) \geq 0$ for every c in $\mathbb{R}^n$.
(0) If $f(x) \in \mathbb{R}[x]$ (one variable) is PSD then f is a sum of two squares in $\mathbb{R}[x]$.
[Start with $ax^2 + bx + c$.]

Define $M(x, y) = x^4y^2 + x^2y^4 + 1 - 3x^2y^2$.
(1) Motzkin's M is PSD. When does $M(c) = 0$?
(2) M is not expressible as a sum of squares in $\mathbb{R}[x, y]$.
(3) M is a sum of squares in $\mathbb{R}(x, y)$. [Observe: $M(x, y) = \frac{x^2y^2(x^2+y^2+1)(x^2+y^2-2)^2+(x^2-y^2)^2}{(x^2+y^2)^2}$.]

P7. Suppose P is an ordering of a field K.
(1) If $c \in K$ then $c^2 \in P$. Then $\Sigma K^2 \subseteq P$, and in particular, $1 \in P$.
(2) If $c \in P$ and $c \neq 0$ then $c^{-1} \in P$.
(3) $-1 \notin P$. [Note: Every $c \in K$ can be expressed as $c = u^2 - v^2$, using hypothesis $2 \neq 0$.]
(4) $P \cap (-P) = (0)$
(5) K has characteristic 0.
(6) $P^\times \leq K^\times$ is a subgroup of index 2.
(7) If P' is an ordering of K and $P \subseteq P'$, then $P = P'$.

P8. Find all orderings on the field $\mathbb{R}(x)$. [Rational functions in one variable.]

Fields and Polynomials. HW #5.

Prof. D. Shapiro   Ross Program 2015.

Unfortunately the file for Homework set # 5 has been lost.

This leads us toward the philosophical question:

Did it ever exist?

Fields and Polynomials. HW #6.

Prof. D. Shapiro   Ross Program 2015.

Supply details to prove the following results.

P1. Suppose K is a field and $X = (x_1, \dots, x_n)$ indeterminates. If $c = (c_1, \dots, c_n) \in K^n$, let $M_c = \mathcal{I}(\{c\}) = (x_1 - c_1, \dots, x_n - c_n)K[X]$.
Suppose $J \subseteq K[X]$ is an ideal and $A = K[X]/J = A[\theta_1, \dots, \theta_n]$, where, $\theta_j = Class(x_j)$. Explain why the following are equivalent ideas.

(1) There is a K-algebra homomorphism $\psi : A \to K$.
(2) There is a K-algebra homomorphism $\varphi : K[X] \to K$ with $\varphi(J) = (0)$.
(3) $J \subseteq M_c$ for some $c \in K^n$.
(4) $\mathcal{Z}(J)$ contains a point in K^n.

P2. (a) For a field K (assuming $2 \neq 0$), prove:
Lemma. Suppose $n = 2^m$ and $c_j \in K$ for $j = 1, \dots, n$. Then there exists an $n \times n$ matrix C having first row $(c_1, c_2, \dots, c_n)$ and satisfying:

$$C^{\mathsf{T}}C = CC^{\mathsf{T}} = (c_1^2 + c_2^2 + \cdots + c_n^2)I_n.$$

[Idea: Let $c = \sum c_j^2$ and write $c = a + b$ where a, b are sums of 2^{m-1} terms. By WOP there exist matrices A, B for a, b. If $a \neq 0$, define $C = \begin{bmatrix} A & B \\ \diamondsuit & A^{\mathsf{T}} \end{bmatrix}$, and fill in the entry $\diamondsuit$ to make the equation true. What if $a = 0$?]

(b) $D_K(2^m)$ is a group.
[If $c, d \in D_K(2^m)$, obtain matrices C, D as in lemma, and set $A = CD^{\mathsf{T}}$. Then $A^{\mathsf{T}}A = cdI_n$.]

(c) There is an identity $(x_1^2 + \cdots + x_n^2) \cdot (y_1^2 + \cdots + y_n^2) = z_1^2 + \cdots + z_n^2$, where each z_k is linear in Y with coefficients in the field $K(X)$. Moreover, we can arrange $z_1 = x_1y_1 + \cdots + x_ny_n$.

P3. Let K be a field in which $2 \neq 0$, and write $D(n)$ for $D_K(n)$.
Then $D(3)D(3) \subseteq D(4)$. Is that an equality?
Does $D(4)D(5) = D(8)$?
Show that $D(3)D(5) \subseteq D(7)$. Is that an equality?
Challenge: Investigate the smallest value n for which $D(r)D(s) \subseteq D(n)$.
[There is a "composition" $r \circ s$ satisfying: For every field K, $D_K(r)D_K(s) = D_K(r \circ s)$.]

Fields and Polynomials. HW #7.

Prof. D. Shapiro Ross Program 2015.

P1. An ordered field (K, P) contains $\mathbb{Q}$. Let $\mathcal{O}$ be the set of finite elements, and $\mathfrak{m}$ the set of infinitesimals. That is:

$\mathcal{O} = \{\theta \in K : |\theta| < n \text{ for some } n \in \mathbb{Z}^+\}$, and

$\mathfrak{m} = \{\alpha \in K : |\alpha| < 1/m \text{ for every } m \in \mathbb{Z}^+\}$.

Then $\mathcal{O}$ is a valuation ring of K with unique maximal ideal $\mathfrak{m}$, and the residue field $\overline{K} = \mathcal{O}/\mathfrak{m}$ inherits an ordering $\overline{P}$. Moreover, $\overline{P}$ is archimedean so $\overline{K} \hookrightarrow \mathbb{R}$. The 'value group" is $\Gamma = K^\times/\mathcal{O}^\times$, an ordered abelian group.

[A domain R is a *valuation ring* if it has ideal M such that: $r \in R \Rightarrow r \in M$ or $1/r \in M$.]

P2. Define field K to be *euclidean* if K^2 is an ordering of K. That is: (K, P) is an ordered field and every positive element is a square.

Field L is *2-closed* (or *quadratically closed*) if $L = L^2$. That is, L has no quadratic extensions.

Equivalent statements:

(1) K is euclidean.

(2) K is formally real and every quadratic extension is nonreal.

(3) $-1 \notin K^2$ and $K(\sqrt{-1})$ is 2-closed.

(4) There exists a quadratic extension $L \supset K$ that is 2-closed.

P3. For field K, let $K^{(2)}$ be its 2-closure: a 2-closed, algebraic extension of K.

Is it unique up to isomorphism?

Is there an analogue to Artin-Schreier's result:

If K is not 2-closed and not euclidean, then must $[K^{(2)} : K]$ be infinite?

P4. If J is an ideal in commutative ring R, define the *radical*

$$\sqrt{J} = \{r \in R : r^m \in J \text{ for some } m \geq 1\}.$$

(1) $\sqrt{(0)} = nil(R)$, the set of nilpotent elements of R. Moreover, $\sqrt{J}/J = nil(R/J)$.

(2) If J is an ideal then $\sqrt{J}$ is also an ideal.

(3) Does $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$? $\sqrt{I + J} = \sqrt{I} + \sqrt{J}$? $\sqrt{IJ} = \sqrt{I \cap J}$?

(4) If $J \subseteq K[X]$ is an ideal, then $\mathcal{Z}(\sqrt{J}\,) = \mathcal{Z}(J)$.

(5)* $\sqrt{J} = \bigcap_{P \supseteq J} P$, the intersection of all prime ideals containing J.