Math 210B Discussion Week 1

Matthew Gherman

January 6, 2022

Definition 1. A *left ideal* in a ring R is a subset $I \subset R$ that is an additive subgroup such that for all $r \in R$ and $a \in I$, $ra \in I$. Similarly, a *right ideal* satisfies $ar \in I$ for all $r \in R$ and $a \in I$.

Definition 2. A subset S of R is *finitely generated as a left R-module* if there are elements $\{x_1, \ldots, x_k\}$ of R such that each $s \in S$ can be written $s = \sum_{i=1}^{k} r_i x_i$ for some $r_i \in R$.

Fall 2014 Problem 8. Let A be a ring. Assume there is an infinite chain of left ideals $I_0 \subset I_1 \subset \cdots \subset A$ with $I_i \neq I_{i+1}$ for $i \geqslant 0$. Show that A has a left ideal that is not finitely generated as a left A-module.

Define $I := \bigcup_{i=0}^{\infty} I_i$. We will show that I is a proper ideal. Let $a, b \in I$. Then $a \in I_k$ for some k and $b \in I_\ell$ for some ℓ. Without loss of generality, assume $k \geqslant \ell$. Then $a, b \in I_k$. Since I_k is an ideal, $a + b \in I_k$ so $a + b \in I$. Similarly, let $r \in A$ and $a \in I$. Then $a \in I_k$ for some k and $ra \in I_k$ since I_k is an ideal. Thus $ra \in I$ and I is an ideal of A. If $1 \in I$, then $1 \in I_k$ for some k. We would have $I_k = I_{k+1} = \cdots = A$, a contradiction. Therefore, I is a proper ideal of A.

Assume for the sake of contradiction that I is finitely generated as a left A-module. Let $\{x_1, \ldots, x_n\}$ be the generating set. Each $x_i \in I_{k_i}$ for some k_i. Define $k := \max_{i=1}^{n} k_i$, then $x_i \in I_k$ for all i. This would imply that $I_k = I_{k+1} = \cdots = A$, a contradiction. Thus I is an ideal of A that is not finitely generated as a left A-module.

Definition 3. Let R and S be rings with multiplicative identities 1_R and 1_S respectively. A *ring homomorphism* $f : R \to S$ is a function that satisfies:

(1) $f(1_R) = 1_S$,

(2) $f(a + b) = f(a) + f(b)$,

(3) $f(ab) = f(a)f(b)$.

A *ring endomorphism* of R is a ring homomorphism $f : R \to R$.

Definition 4. Let R be a commutative ring. A *unit* $r \in R$ is such that there is some $s \in R$ for which $rs = 1_R$. Note that if $ab = 1_R$, then $f(ab) = f(a)f(b) = 1_S$. A ring homomorphism takes units of R to units of S.

Spring 2015 Problem 7. Determine the ring endomorphisms of $\mathbb{F}_2[t, t^{-1}]$, where t is an indeterminate.

Let $R := \mathbb{F}_2[t, t^{-1}]$. For a ring endomorphism $f : R \to R$, we have $f(1) = 1$ so f fixes the base field $\mathbb{F}_2$. Let $a \in R^\times$. We note $1 = f(1) = f(aa^{-1}) = f(a)f(a^{-1}) = f(a^{-1})f(a)$ so f will send units to units with $f(a^{-1}) = f(a)^{-1}$. Each endomorphism of R is thus determined by the image of t since $f(t^{-1}) = f(t)^{-1}$. Take a non-zero $p \in R$. Then there is some $k \in \mathbb{Z}$ such that $t^k p \in \mathbb{F}_2[t]$ and $t^k p$ has a non-zero constant term. If $p \in R^\times$, then $t^k p \in R^\times$ via $(t^k p)(p^{-1}t^{-k}) = 1$. If $t^k p \in R^\times$, then the product of two units $t^{-k}(t^k p) = p$ is also an element of $R^\times$. Thus $t^k p$ is a unit of R if and only if p is a unit of R so it is sufficient to classify $(\mathbb{F}_2[t])^\times$. We show below that $(\mathbb{F}_2[t])^\times = \{1\}$. Thus $R^\times = \{t^k\}$ for $k \in \mathbb{Z}$, and a ring endomorphism $f : R \to R$ will always be defined by $f(t) = t^k$ for some $k \in \mathbb{Z}$.

Let $p(t) = a_0 + \cdots + a_n t^n \in (\mathbb{F}_2[t])^\times$ with $a_n \neq 0$. Then there is some $q(t) = b_0 + \cdots + b_m t^m \in \mathbb{F}_2[t]$ such that $q(t)p(t) = 1$. Distributing the product, the constant term $a_0 b_0 = 1$ so $a_0, b_0 \in \mathbb{F}_2^\times$. Looking at the highest degree term, $a_n b_m = 0$ so $b_m = 0$ since $\mathbb{F}_2$ is an integral domain. Then the next largest term in the expansion yields $a_n b_{m-1} = 0$ so $b_{m-1} = 0$. We can continue this argument to show that $b_i = 0$ for all $i \geqslant 1$. Then $b_0(a_0 + \cdots + a_n t^n) = 1$ implies $n = 0$. In $\mathbb{F}_2[t]$, the set of units is $\{1\}$.

Remark 1. The more general result is $f = a_0 + \cdots + a_n t^n \in R[t]$ is a unit if and only if $a_0 \in R^\times$ and a_i is nilpotent for all $i \geqslant 1$.

Definition 5. An *integral domain* R is a ring for which $ab = 0$ implies $a = 0$ or $b = 0$ for $a, b \in R$.

Definition 6. A non-zero, non-unit r in an integral domain R is *irreducible* if it is not a product of two non-units. Equivalently, every factorization of r contains at least one unit.

Definition 7. A *unique factorization domain* is an integral domain R for which every non-zero element of R can be written as a product of irreducible elements and a unit. The factorization is unique up to rearrangement and multiplication by a unit.

Definition 8. A *principal ideal* I in a ring R is generated by one element $x \in R$. In other words, every element $a \in I$ satisfies $a = rx$ for some $r \in R$. We write $I = (x)$.

A *principal ideal domain* is an integral domain R for which each ideal is principal.

Example 1. Every PID is a UFD.

Definition 9. A proper ideal $\mathfrak{p}$ in a commutative ring R is *prime* if $ab \in \mathfrak{p}$ implies that $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

An element $p \in R$ is *prime* if the principal ideal (p) is a prime ideal of R.

Example 2. Every prime element of a commutative ring is irreducible. In a UFD, the converse also holds.

Example 3. As an application of Gauss's Lemma, we can prove that $R[x]$ is a UFD when R is a UFD.

Spring 2016 Problem 1.

(a) Give an example of a unique factorization domain A that is not a PID. You need not show that A is a UFD (assuming it is), but please show that your example is not a PID.

Let $A := \mathbb{Z}[x]$. We know that A is a UFD via an application of Gauss's Lemma. Let $I := (2, x)$ and we claim that I is not a principal ideal. We will first show that I is a proper ideal of A. For

$$1 = 2a + bx,$$

we would need $b = 0$. Then there are no possibilities for a since $1 \notin 2\mathbb{Z}$. Thus $1 \notin I$ and I is a proper ideal.

Assume $I = (p)$ for some $p \in A$. Then there is an $r \in A$ such that $rp = 2$. Since $\mathbb{Z}$ is an integral domain, $0 = \deg(rp) = \deg(r) + \deg(p)$ so $\deg(p) = 0$. Thus $p \in \mathbb{Z}$ and the only integer divisors of 2 are $\pm 1, \pm 2$. Since I is a proper ideal, $p = \pm 2$. We note $(2) = (-2)$ so take $p = 2$. Now there is some $s \in A$ such that $sp = x$. However, $2s = x$ cannot occur. We conclude that I is not principal.

(b) Let R be a UFD. Let $\mathfrak{p}$ be a prime ideal such that $0 \neq \mathfrak{p}$ and there is no prime ideal strictly between 0 and $\mathfrak{p}$. Show that $\mathfrak{p}$ is principal.

Let $a \in \mathfrak{p}$ be some nonzero element. Since R is a UFD, we can factor a as a product of irreducible elements $a = \prod_{i=1}^{n} p_i^{k^i}$. In a UFD, irreducible implies prime so each p_i is prime in R. Since $a \in \mathfrak{p}$ and $\mathfrak{p}$ is a prime ideal, one of the $p_i \in \mathfrak{p}$. Thus $(p_i) \subset \mathfrak{p}$. Since (p_i) is a prime ideal, we must have $(p_i) = \mathfrak{p}$ and $\mathfrak{p}$ is principal.

Spring 2019 Problem 3. Let $d > 2$ be a square-free integer. Show that the integer 2 in $\mathbb{Z}[\sqrt{-d}]$ is irreducible but the ideal (2) in $\mathbb{Z}[\sqrt{-d}]$ is not a prime ideal.

Define the norm $N : \mathbb{Z}[\sqrt{-d}] \to \mathbb{Z}_{\geqslant 0}$ as $N(a + b\sqrt{-d}) = (a + b\sqrt{-d})(a - b\sqrt{-d}) = a^2 + b^2 d$. We can show algebraically that the norm is multiplicative. Further, we will show $N(a + b\sqrt{-d}) = 1$ if and only if $a + b\sqrt{-d}$ is a unit in $\mathbb{Z}[\sqrt{-1}]$. ($\Rightarrow$) Assume $N(a + b\sqrt{-d}) = 1$. Then $(a + b\sqrt{-d})(a - b\sqrt{-d}) = 1$ and $a + b\sqrt{-d}$ is a unit. ($\Leftarrow$) Assume $a + b\sqrt{-d}$ is a unit. Then there is some element $a' + b'\sqrt{-d}$ for which $(a + b\sqrt{-d})(a' + b'\sqrt{-d}) = 1$. By multiplicativity of the norm, $N(a + b\sqrt{-d})$ divides $N(1) = 1$. We conclude that $N(a + b\sqrt{-d}) = 1$.

We will first show that 2 is irreducible in $\mathbb{Z}[\sqrt{-d}]$. Let $a + b\sqrt{-d}$ be a non-unit factor of 2. Then $N(a + b\sqrt{-d}) = a^2 + b^2 d$ divides $N(2) = 4$. If $N(a + b\sqrt{-d}) = 1$ or $N(a + b\sqrt{-d}) = 4$, the factorization of 2 includes a unit. Thus $N(a + b\sqrt{-d}) = 2$ or $a^2 + b^2 d = 2$. Since $d > 2$, we must have $b = 0$. Then $a^2 = 2$ for integer a, which is not possible. No such non-trivial factor of 2 exists.

We will now show that (2) is not prime in $\mathbb{Z}[\sqrt{-d}]$. If d is even, 2 divides $-d$ but 2 does not divide either factor in $-d = \sqrt{-d} \cdot \sqrt{-d}$. If d is odd, 2 divides $1 + d$ but 2 does not divide either factor of $1 + d = (1 + \sqrt{-d})(1 - \sqrt{-d})$. Thus (2) is not a prime ideal. Note that this argument proves that $\mathbb{Z}[\sqrt{-d}]$ is not a UFD since irreducible and prime are equivalent notions in a UFD.

Definition 10. Let $I \subset R$ be an ideal of a commutative ring R. We define an equivalence relation $a \sim b$ if and only if $a - b \in I$. The quotient ring R/I is the set of equivalence classes of R via $\sim$ under the operations:

(1) $(a + I) + (b + I) = (a + b) + I$,

(2) $(a + I)(b + I) = ab + I$.

Lemma (Ideal correspondence)**.** Let R be a ring with ideal $I \subset R$. Then there is a one-to-one correspondence between the ideals of R/I and the ideals of R containing I.

Theorem (Hilbert Nullstellensatz)**.** Let F be an algebraically closed field (e.g. $\mathbb{C}$). Then the maximal ideals of $F[x_1, \ldots, x_n]$ are of the form $(x_1 - a_1, \ldots, x_n - a_n)$ for $a_i \in F$.

Fall 2019 Problem 3. Let I be the ideal $(x^2 - y^2 + z^2, (xy + 1)^2 - z, z^3)$ of $R = \mathbb{C}[x, y, z]$. Find the maximal ideals of R/I, as well as all of the points on the variety

$$V(I) = \{(a, b, c) \in \mathbb{C}^3 : f(a, b, c) = 0 \text{ for all } f \in I\}.$$

By ideal correspondence, the maximal ideals of R/I are in bijection with the ideals of R containing I. Hilbert Nullstellensatz reveals that the maximal ideals of R are of the form $(x - a, y - b, z - c)$ for $a, b, c \in \mathbb{C}$. Let $\mathfrak{m}$ be a maximal ideal. Since $\mathfrak{m}$ contains z^3, it must contain z. We reduce the other relations to $x^2 - y^2$ and $(xy + 1)^2$. If $\mathfrak{m}$ contains $x^2 - y^2$, then it contains either $x - y$ or $x + y$. If $\mathfrak{m}$ contains $(xy + 1)^2$, then it contains $xy + 1$. Case 1: Assume $\mathfrak{m}$ contains $x - y$. Multiply by $-y$ to obtain $-xy + y^2$ in $\mathfrak{m}$. Then $y^2 + 1$ is in $\mathfrak{m}$ so either $y + i$ or $y - i$ is in $\mathfrak{m}$. Case 2: Assume $\mathfrak{m}$ contains $x + y$. Then $-xy - y^2$ is in $\mathfrak{m}$ and so is $1 - y^2$. Thus either $y + 1$ or $y - 1$ is in $\mathfrak{m}$. The maximal ideals of R containing I are $(x - 1, y + 1, z)$, $(x + 1, y - 1, z)$, $(x - i, y - i, z)$, and $(x + i, y + i, z)$ which correspond to the points $(1, -1, 0)$, $(-1, 1, 0)$, $(i, i, 0)$, and $(-i, -i, 0)$ in the variety.

Math 210B Discussion Week 2

Matthew Gherman

January 13, 2022

Spring 2015 Problem 4. Let $M = \mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z}$ and $N = \mathbb{Q}/\mathbb{Z}$, where $\mathbb{Z}\left[\frac{1}{p}\right] \subset \mathbb{Q}$ is the subring generated by $\frac{1}{p}$ for a prime p.

(a) Show that M is an Artinian module but not a Noetherian module.

Let $I_k := \left(\frac{1}{p^k}\right)$ be $\mathbb{Z}$-submodules of M. If $I_k = I_{k+1}$, then there is some $r \in \mathbb{Z}$ such that $\frac{r}{p^k} = \frac{1}{p^{k+1}}$. Equivalently, $rp^{k+1} - p^k = p^k(rp-1) = 0$. Since $\mathbb{Z}$ is an integral domain, this cannot occur. We have an ascending chain $I_1 \subset I_2 \subset \dots$ that does not terminate so M is not Noetherian.

Let $A \subset M$ be a proper $\mathbb{Z}$-submodule. Then there is a maximum $k \in \mathbb{N}$ for which $\frac{a}{p^k} \in A$ for $a \in \mathbb{Z}$ and $\gcd(a,p) = 1$. In this case, $\gcd(a,p^k) = 1$ so there are integers ℓ, m such that $ma + \ell p^k = 1$. Then $m\frac{a}{p^k} = \frac{1-\ell p^k}{p^k} = \frac{1}{p^k} \in A$. Thus $\frac{b}{p^i} \in A$ for all $b \in \mathbb{Z}$ and $i \leqslant k$. In other words, $A = \left(\frac{1}{p^k}\right)$. Take a strict descending chain $A_1 \supset A_2 \supset \dots$ of $\mathbb{Z}$-submodules of M. Then $A_1 = \left(\frac{1}{p^k}\right)$ for some $k \in \mathbb{N}$. Then $\frac{1}{p^j} \notin A_2$ for all natural numbers $j \geqslant k$. Thus $A_2 = \left(\frac{1}{p^i}\right)$ for $i < k$. Continuing this argument, the descending chain must terminate. Thus M is Artinian.

(b) Show that N is neither Noetherian nor Artinian.

The counterexample in (a) proves that N is not Noetherian.

Order the prime numbers $\{p_i\}_{i\in\mathbb{N}}$. Define N_i as the $\mathbb{Z}$-submodule of N generated by $\left\{\frac{1}{p_i}, \frac{1}{p_{i+1}}, \dots\right\}$. Since the $p_i \in Z$ are prime, $\frac{1}{p_{i-1}} \notin N_i$ for each natural number $i \geqslant 2$. Then we can construct a descending chain $N_1 \supset N_2 \supset \dots$ that does not terminate. We conclude that N is not Artinian.

Fall 2015 Problem 3. Let k be a field and define $A = k[X,Y]/(X^2, XY, Y^2)$.

(a) What are the principal ideals of A?

Let R be a commutative ring. We will prove that the sum of a unit r and a nilpotent element a is a unit. Let $a^k = 0$. To show the element $r + a$ is a unit is equivalent to showing $1 + r^{-1}a$ is a unit. Then

$$(1 + r^{-1}a)\left(\sum_{i=0}^{k-1}(-1)^i(r^{-1}a)^i\right) = 1 + (-1)^{k-1}(r^{-1}a)^k = 1.$$

We conclude that $r + a$ is a unit of R.

Take a polynomial with coefficients in k. We can reduce all terms of degree greater than or equal to 2. Thus a general representative of an element of A is $aX + bY + c$ for $a, b, c \in k$. Clearly (0) and $(1) = A$ are principal ideals. A non-trivial principal ideal will have some element $aX + bY + c$.

Case 1: Assume $c = 0$. Then

$$(aX + bY)^2 = a^2X^2 + 2abXY + b^2Y^2 = 0$$

in A so $aX + bY$ is nilpotent for any choice of $a, b \in k$. Each of $(aX + bY)$ is a principal ideal for $a, b \in k$.

Case 2: Assume $c \neq 0$. Since c is a unit and $aX + bY$ is nilpotent, the element $aX + bY + c$ is a unit of A. Then $(aX + bY + c) = A$.

Thus all principal ideals have one of the following forms $\{(0), A, (aX + bY)\}$ for $a, b \in k$. We can further simplify this by breaking into cases $a = 0$ and $a \neq 0$. If $a = 0$, we have $(aX + bY) = (bY) = Y$ for $b \neq 0$. If $a \neq 0$, then $(aX + bY) = (X + a^{-1}bY)$. All principal ideals have one of the following forms $\{(0), (X + cY), (Y), A\}$ for $c \in k$.

(b) What are the ideals of A?

Let $I \subset A$ be a non-trivial, proper ideal. Then by part (a), I contains some $aX + bY$ for $a, b \in k$. If $I = (aX + bY)$, then we are in the case of part (a). Assume that $(aX + bY)$ is not all of I. Then there is some $cx + dY$ in I that is not in $(aX + bY)$. If $a = 0$, then $b^{-1}(bY) = Y \in I$. Since $cX + dY$ was chosen so as not to be contained in I, we have $c \neq 0$. Then $c^{-1}((cX + dY) - dY) = X \in I$ and $(X, Y) \subset I$. A similar argument holds if $c = 0$.

Assume that $a \neq 0$ and $c \neq 0$. The elements $X + a^{-1}bY$ and $X + c^{-1}dY$ are contained in I so

$$(X + a^{-1}bY) - (X + c^{-1}dY) = (a^{-1}b - c^{-1}d)Y$$

is an element of I. Since $cX + dY$ was chosen to not be in $(aX + bY)$, we conclude that $a^{-1}b - c^{-1}d \neq 0$. Then multiplying by its inverse in k, we obtain $Y \in I$. Further, $X \in I$ and $(X, Y) \subset I$.

Since $A/(X, Y) \simeq k$ is a field, we conclude that (X, Y) is a maximal ideal. Thus I proper implies $I = (X, Y)$ in the above cases. We conclude that the ideals of A are $\{(0), (X + cY), (Y), (X, Y), A\}$ for $c \in k$.

Fall 2020 Problem 8. Consider $R = \mathbb{C}[X, Y]/(X^2, XY)$. Determine the prime ideals P of R.

By the prime ideal correspondence, the prime ideals of R are in bijection with the prime ideals of $\mathbb{C}[X, Y]$ that contain (X^2, XY). Let $\mathfrak{p}$ be a prime ideal of $\mathbb{C}[X, Y]$ that contains (X^2, XY). Then $X^2 \in \mathfrak{p}$ and $\mathfrak{p}$ prime implies $(X) \subset \mathfrak{p}$. The quotient $\mathbb{C}[X, Y]/\mathfrak{p}$ factors through $\mathbb{C}[Y]/\mathfrak{p}'$ for some prime ideal $\mathfrak{p}'$ of $\mathbb{C}[Y]$. Since $\mathbb{C}[Y]$ is a PID, we conclude that $\mathfrak{p}' = (p(Y))$ for an irreducible polynomial $p(Y) \in \mathbb{C}[Y]$. Thus $\mathfrak{p} = (X)$ or $\mathfrak{p} = (X, p(Y))$. The collection $\{(\overline{X}), (\overline{X}, \overline{p(Y)})\}$ is all the prime ideals of R for $p(Y)$ irreducible in $\mathbb{C}[Y]$.

Spring 2016 Problem 3. Let R be a ring which is left Artinian (that is, Artinian with respect to left ideals). Suppose that R is a domain, meaning that $1 \neq 0$ in R and $ab = 0$ implies $a = 0$ or $b = 0$ in R. Show that R is a division ring.

Let the ring homomorphism $f : R \to R$ be right multiplication by some nonzero $a \in R$. Then $f(b) = 0$ implies $ba = 0$ so $a = 0$ or $b = 0$ by R a domain. Since $a \neq 0$, we have $b = 0$ and f is injective. Note that this further implies that f^k is injective for all $k \in \mathbb{N}$. We have the chain of decreasing left R-modules,

$$\mathrm{im}(f) \supset \mathrm{im}(f^2) \supset \dots$$

Since R is Artinian, the chain terminates so $\mathrm{im}(f^k) = \mathrm{im}(f^{k+1})$ for some $k \in \mathbb{N}$. Let $b \in R$ be any element. Then $f^k(b) \in \mathrm{im}(f^k)$ so there is some $c \in R$ such that $f^{k+1}(c) = f^k(b)$. Rearranging, $f^k(f(c) - b) = 0$ and $f(c) = b$ by injectivity of f^k. We conclude that f is surjective. Then $f(b) = 1$ for some $b \in R$ which implies $ba = 1$. We have shown that every nonzero element $a \in R$ has a left inverse b. Further, b has a left inverse, which we denote $c \in R$. Then

$$a = (cb)a = c(ba) = c$$

and every nonzero $a \in R$ is invertible. We conclude R is a division ring.

Definition. We say that B is *finitely generated as an A-algebra* if each element $b \in B$ can be written as a polynomial of elements $\{x_1, \dots, x_k\} \subset B$ with coefficients in A.

Proposition. Let B be a finitely generated A-algebra. If A is Noetherian, then B is Noetherian.

Proof. Let $\{x_1, \dots, x_k\}$ generate B as an A-algebra. Then there is a surjective ring homomorphism

$$\varphi : A[x_1, \dots, x_n] \to B.$$

Thus B is isomorphic to a quotient of $A[x_1, \dots, x_n]$, a Noetherian ring by Hilbert Basis Theorem. We conclude that B is Noetherian as a ring. □

Fall 2017 Problem 4. Let R be a commutative Noetherian ring and A a finitely generated R-algebra (not necessarily commutative). Let B be an R-subalgebra of the center $Z(A)$. Assume A is a finitely generated B-module. Show that B is a finitely generated R-algebra.

Let $\{x_1, \ldots, x_m\}$ generate A as a C-algebra and $\{y_1, \ldots, y_n\}$ generated A as a B-module. Then $x_i = \sum_{j=1}^{n} b_{ij} y_j$ and $y_i y_j = \sum_{k=1}^{n} b_{ijk} y_k$ for some $b_{ij}, b_{ijk} \in B$. Let B_0 be the R-algebra generated by the set $\{b_{ij}, b_{ijk}\}$. Since R is Noetherian and B_0 is finitely generated as an R-algebra, B_0 is Noetherian as a ring. Every element of C is a polynomial in the x_i, which we can write in terms of the y_j. Then $B \subset Z(A)$ and $y_i y_j = \sum_{k=1}^{n} b_{ijk} y_k$ allow us to reduce this expression to a linear combination of the y_j with coefficients in B_0. Thus A is a finitely generated B_0-module, which implies A is a Noetherian B_0-module. Initially, B is an R-subalgebra of A and $B_0 \subset B$ so B has the structure of a B_0-submodule of A. Thus B is finitely generated as a B_0-module and B_0 is finitely generated as an R-algebra so B is finitely generated as an R-algebra.

This proof is based on that of Proposition 7.8 in Atiyah MacDonald.

Math 210B Discussion Week 3

Matthew Gherman

January 20, 2022

Spring 2017 Problem 5. Let S be a multiplicatively closed subset of a commutative ring R. For a prime ideal I in R with $I \cap S = \varnothing$, show that the ideal $I \cdot S^{-1}R$ in the localized ring $S^{-1}R$ is prime. Also, show that sending I to $I \cdot S^{-1}R$ gives a bijection between the prime ideals in R that do not meet S and the prime ideals in the localized ring $S^{-1}R$.

We will first prove that the ideals of $S^{-1}R$ are in one-to-one correspondence with the ideals of R that are disjoint from S. Let $I \subset R$ be an ideal. Since I is a proper ideal R, $S^{-1}I = S^{-1}R$ implies I contains some element of S. Thus $S^{-1}I$ is a proper subset of $S^{-1}R$ when $I \cap S = \varnothing$. For $\frac{a}{s}, \frac{b}{t} \in S^{-1}I$, we have $\frac{ta+sb}{st} \in S^{-1}I$ since $ta + sb \in I$ and $st \in S$. For $\frac{r}{t} \in S^{-1}R$ and $\frac{a}{s} \in S^{-1}R$, we have $\frac{ra}{st} \in S^{-1}I$ since $ra \in I$ and $st \in S$. Given an ideal $J \subset S^{-1}R$, define $I := \{a \in R : \frac{a}{1} \in J\}$. If $\frac{a}{s} \in J$, then $\frac{s}{1}\frac{a}{s} = \frac{a}{1} \in J$ so I is the set of all numerators of J. If $J \subset S^{-1}R$ is a proper ideal, then $\frac{1}{1} \notin J$ so $1 \notin I$ and I is a proper subset of R. Now $ra \in I$ for all $a \in I$ and $r \in R$ since $\frac{r}{1}\frac{a}{1} = \frac{ra}{1} \in J$. For $a, b \in I$ we have $\frac{a}{1} + \frac{b}{1} = \frac{a+b}{1} \in J$ so $a + b \in I$. We conclude that $I \subset R$ is a proper ideal.

We want to show further that a prime ideal of R maps to a prime ideal of $S^{-1}R$ for S a multiplicatively closed subset of $R\backslash\{0\}$ with $1 \in S$ under this correspondence. Let $\mathfrak{p} \subset R$ be a prime ideal with $\frac{a}{s}\frac{b}{t} = \frac{ab}{st} \in S^{-1}\mathfrak{p}$. Then $ab \in \mathfrak{p}$ so $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ since $\mathfrak{p}$ is prime. Thus $\frac{a}{s} \in S^{-1}\mathfrak{p}$ or $\frac{b}{t} \in S^{-1}\mathfrak{p}$ and $S^{-1}\mathfrak{p}$ is a prime ideal of $S^{-1}R$. Given a prime ideal $\mathfrak{q} \subset S^{-1}R$, define the corresponding ideal $\mathfrak{p} = \{a \in R : \frac{a}{1} \in \mathfrak{q}\}$. If $ab \in \mathfrak{p}$, then $\frac{ab}{1} \in \mathfrak{q}$ so $\frac{a}{1}$ or $\frac{b}{1}$ is in $\mathfrak{q}$. We conclude that a or b is in p.

Spring 2016 Problem 4(a). Let A be a commutative ring, S a multiplicatively closed subset of A, $A \to S^{-1}A$ the localization. Which elements of A map to zero in $S^{-1}A$?

An element $a \in A$ maps to $\frac{a}{1} \in S^{-1}A$. If $\frac{a}{1} = 0$, then there is some $s \in S$ such that $sa = 0$. Let $Sa = \{sa : s \in S\}$ and $0 \in Sa$ when a maps to 0. Conversely, an element $a \in A$ such that $0 \in Sa$ maps to zero in the localization. If S contains some zero divisor of A, then it will send some non-trivial element of A to zero in $S^{-1}A$.

Fall 2015 Problem 2. Let R be a principal ideal domain with field of fractions K.

(a) Let S be a non-empty multiplicatively closed subset of $R\backslash\{0\}$. Show that $S^{-1}R$ is a principal ideal domain.

Let $J \subset S^{-1}R$ be an ideal. Then the ideal $I \subset R$ of all numerators of J is principal. Let $I = (a)$ for $a \in R$. Then we claim that $J = \left(\frac{a}{1}\right)$. Certainly $J \supset \left(\frac{a}{1}\right)$. Let $\frac{j}{s} \in J$. Then $j = ra$ for some $r \in R$ and $\frac{r}{s}\frac{a}{1} = \frac{ra}{s} = \frac{j}{s}$. We conclude $J = \left(\frac{a}{1}\right)$ and $S^{-1}R$ is a principal ideal domain.

(b) Show that any subring of K containing R is $S^{-1}R$ for some multiplicatively closed subset S of $R\backslash\{0\}$.

Let $R \subset T \subset K$ be a subring. Define $S := \{s \in R\backslash\{0\} : \frac{1}{s} \in T\}$. Since $\frac{1}{1} \in T$ we have $1 \in S$. Given $s, t \in S$, we have $\frac{1}{s}\frac{1}{t} = \frac{1}{st} \in T$ so $st \in S$. Thus S is a multiplicatively closed subset of R and $T \supset S^{-1}R$. Let $\frac{a}{s} \in T$ and we want to show $\frac{a}{s} \in S^{-1}R$. We can assume $\gcd(a, s) = 1$ since R is a UFD. In the PID R, Bezout's identity implies there are elements $k, \ell \in R$ such that $ka + \ell s = 1$. Thus $\frac{k}{1}\frac{a}{s} + \frac{s}{s}\frac{\ell}{1} = \frac{ka+\ell s}{s} = \frac{1}{s} \in T$ so $\frac{a}{s} \in S^{-1}R$. We conclude $T = S^{-1}R$ for a multiplicatively closed set S of $R\backslash\{0\}$.

Proposition. Let R be a ring and S a multiplicatively closed subset of R that does not contain 0. Let I be an ideal of R. Then $S^{-1}R/S^{-1}I$ is isomorphic to $\overline{S}^{-1}(R/I)$ where $\overline{S}$ is the image of S in R/I.

Proof. Let $T = S^{-1}R/S^{-1}I$. Then define a ring homomorphism $g : R \to S^{-1}R \to T$ so that $g(r)$ is the class of $\frac{r}{1}$ in T. The kernel of g is I so g descends to a ring homomorphism $g : R/I \to T$. Further, the elements $\overline{S}$ map to units in T. By the universal property of localization, there is a unique homomorphism $h : \overline{S}^{-1}(R/I) \to T$ such that $g = h \circ f$ for $f : R/I \to \overline{S}^{-1}(R/I)$ the usual inclusion. One can check that h is an isomorphism. □

Fall 2020 Problem 8. Consider $R = \mathbb{C}[X,Y]/(X^2, XY)$. Determine the prime ideals P of R. Which of the localizations R_P are integral domains?

By the prime ideal correspondence, the prime ideals of R are in bijection with the prime ideals of $\mathbb{C}[X,Y]$ that contain (X^2, XY). Let $\mathfrak{p}$ be a prime ideal of $\mathbb{C}[X,Y]$ that contains (X^2, XY). Then $X^2 \in \mathfrak{p}$ and $\mathfrak{p}$ prime implies $(X) \subset \mathfrak{p}$. The quotient $\mathbb{C}[X,Y]/\mathfrak{p}$ factors through $\mathbb{C}[Y]/\mathfrak{p}'$ for some prime ideal $\mathfrak{p}'$ of $\mathbb{C}[Y]$. Since $\mathbb{C}[Y]$ is a PID, we conclude that $\mathfrak{p}' = (p(Y))$ for an irreducible polynomial $p(Y) \in \mathbb{C}[Y]$. Thus $\mathfrak{p} = (X)$ or $\mathfrak{p} = (X, p(Y))$. The collection $\{(\overline{X}), (\overline{X}, \overline{p(Y)})\}$ is all the prime ideals of R for $p(Y)$ irreducible in $\mathbb{C}[Y]$.

Let $I = (X^2, XY)$ be an ideal of $\mathbb{C}[X,Y]$. Since localization commutes with quotients, the ring $R_\mathfrak{p}$ for a prime ideal $\mathfrak{p}$ in R is isomorphic to $S^{-1}\mathbb{C}[X,Y]/S^{-1}I$ for a multiplicatively closed set $S \subset \mathbb{C}[X,Y]$ for which the image of S in R is $R\backslash\mathfrak{p}$. Assume $\overline{Y} \notin \mathfrak{p}$. Then $\overline{Y}$ is invertible in $R_\mathfrak{p}$. We conclude that $S^{-1}I = S^{-1}(X^2, XY) = (X)$ in $\mathbb{C}[X,Y]$. Then $S^{-1}\mathbb{C}[X,Y]/S^{-1}I$ is isomorphic to a localization of the integral domain $\mathbb{C}[Y]$ so $R_\mathfrak{p}$ is an integral domain. If $\overline{Y} \in \mathfrak{p}$, then $\mathfrak{p} = (\overline{X}, \overline{Y})$. The localization at the prime ideal $\mathfrak{p}$ will not be an integral domain since $\overline{X}$ is nilpotent.

Definition. The *nilradical* of a commutative ring R is the ideal of R containing all nilpotent elements of R. Equivalently, the *nilradical* is the intersection of all prime ideals of R. There are analogues of the nilradical for non-commutative rings, but the situation is more complicated.

Definition. The *Jacobson radical* is the set of all $r \in R$ such that $rM = 0$ for all simple R-modules M. One can show that the Jacobson radical is a two-sided ideal. The *Jacobson radical* of a commutative ring R is equivalently the intersection of all maximal ideals of the ring R.

Fall 2015 Problem 9(b). Let R be a ring. Is an element in the Jacobson radical of R always nilpotent? Is a nilpotent element of R always in the Jacobson radical? Justify your answers.

An element of the Jacobson radical is not always nilpotent. In commutative rings, the nilradical, the set of all nilpotent elements, is the intersection of all prime ideals of the ring. The Jacobson radical is the intersection of all maximal ideals of R. The ring $\mathbb{Z}[x]$ has maximal ideal $(2,x)$. Let $R = \mathbb{Z}[x]_{(2,x)}$ be the localization of $\mathbb{Z}[x]$ with $S = \mathbb{Z}[x]\backslash(2,x)$. Then R is local with $J(R) = S^{-1}(2,x)$. Note $\mathbb{Z}[x]/(2) \simeq (\mathbb{Z}/2\mathbb{Z})[x]$, which is an integral domain. Thus (2) is a prime ideal of $\mathbb{Z}[x]$. Similarly, $\mathbb{Z}[x]/(x) \simeq \mathbb{Z}$ is an integral domain and (x) is a prime ideal of $\mathbb{Z}[x]$. By the argument above, $S^{-1}(2)$ and $S^{-1}(x)$ are prime ideals of R. We see that $S^{-1}(2) \cap S^{-1}(x)$ is strictly contained in the Jacobson radical $S^{-1}(2,x)$. Take for instance $\frac{2+x}{1} \in J(R)$ but $\frac{2+x}{1}$ is not nilpotent.

A nilpotent element is not always in the Jacobson radical of a ring R. Let $R = \mathrm{M}_2(\mathbb{C})$ and $A := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in \mathrm{M}_2(\mathbb{C})$. It is clear that A^2 is the zero matrix so A is nilpotent. The matrix ring R has no non-trivial two-sided ideals so A is a nilpotent element that is not in the Jacobson radical of R.

Spring 2019 Problem 9(a) Find a domain R and two nonzero elements $a, b \in R$ such that R is equal to the intersection of the localizations $R[1/a]$ and $R[1/b]$ (in the quotient field of R) and $aR + bR \neq R$.

Let $R = \mathbb{Z}[x]$ with $a = 2$ and $b = x$. Then $(2,x)$ is a proper ideal of R so $2R + xR \neq R$. We want to show that $R = R[1/2] \cap R[1/x]$ in the quotient field. Let $\frac{r}{s}$ be in the intersection. Then $\frac{r}{s} = \frac{c}{2^k} = \frac{d}{x^\ell}$ where we can assume without loss of generality that the fractions are reduced. We have $s(cx^\ell - d2^k) = 0$ in R which only has non-trivial solutions when $k = \ell = 0$ since R is an integral domain. Thus $R = R[1/2] \cap R[1/x]$ as desired.

Spring 2020 Problem 3. Prove that a noetherian commutative ring A is a finite ring if the following two conditions are satisfied:

(a) the nilradical of A vanishes,

(b) localization at every maximal ideal is a finite ring.

Let $\mathfrak{p}$ be a prime ideal of A. Let $\mathfrak{m}$ be a maximal ideal of A for which $\mathfrak{p} \subset \mathfrak{m}$. We note that $A/\mathfrak{p}$ and the localization of $A/\mathfrak{p}$ at $\mathfrak{m}/\mathfrak{p}$ are integral domains. The localization $(A/\mathfrak{p})_{\mathfrak{m}/\mathfrak{p}}$ is isomorphic to $A_\mathfrak{m}/\mathfrak{p}_\mathfrak{m}$ so, by assumption (b), $(A/\mathfrak{p})_{\mathfrak{m}/\mathfrak{p}}$ is finite. A finite integral domain is a field so $\mathfrak{p}_\mathfrak{m}$ is a maximal ideal of $A_\mathfrak{m}$. Since $A_\mathfrak{m}$ is a local ring with unique maximal ideal $\mathfrak{m}$, we conclude that $\mathfrak{p} = \mathfrak{m}$ and every prime ideal of A is maximal. Since A

is Noetherian, A will have finitely many minimal prime ideals. Each maximal ideal in A is also minimal so there are finitely many maximal ideals of A.

Let $\mathfrak{n}$ be the nilradical or the intersection of all prime ideals of A. By the above argument, $\mathfrak{n}$ is equivalently the intersection of all maximal ideals of A. In general, we can define a ring homomorphism f from A to $\prod_{i\in I} A/\mathfrak{m}_i$ by $f(a) = (a+\mathfrak{m}_i)_{i\in I}$ for $\{\mathfrak{m}_i\}_{i\in I}$ the collection of all maximal ideals of A. The kernel of f is $\mathfrak{n}$ so assumption (a) implies f is injective. In our case, we can use Chinese Remainder Theorem to prove that the map is an isomorphism. Each component $A/\mathfrak{m}_i$ is finite since $(A/\mathfrak{m}_i)_{\mathfrak{m}_i/\mathfrak{m}_i} \simeq A_{\mathfrak{m}_i}/(\mathfrak{m}_i)_{\mathfrak{m}_i}$ is isomorphic to $A/\mathfrak{m}_i$. There are finitely many maximal ideals m_i so the codomain of f is finite. Thus A is finite.

Math 210B Discussion Week 4

Matthew Gherman

January 27, 2022

Proposition. Let R be a left Artinian ring. Then any injective R-module homomorphism is surjective.

Proof. Let $f : M \to N$ be an injective homomorphism of left R-modules. We can construct the descending chain $\text{im}(f) \supset \text{im}(f^2) \supset \dots$ of left R-modules. (Note that each $\text{im}(f^i)$ is finitely generated because they are submodules of a finitely generated module over a left Noetherian ring R.) Then the descending chain terminates and $\text{im}(f^k) = \text{im}(f^{k+1})$ for some k. Take $b \in R$. Then $f^k(b) \in \text{im}(f^k) = \text{im}(f^{k+1})$ so there is some $c \in R$ such that $f^{k+1}(c) = f^k(b)$. Then $f^k(b - f(c)) = 0$ and f^k injective implies $b = f(c)$. Thus f is surjective. □

Spring 2015 Problem 3. Let R be a ring. Show that R is a division ring if and only if all R-modules are free.

($\Rightarrow$) Assume that R is a division ring and let M be a left R-module. Let S be the set of all possible linearly independent sets of M ordered by inclusion. The set S is not empty since the empty set is linearly independent. Let $\{x_i\}_{i\in I_0} \subset \{x_i\}_{i\in I_1} \subset \dots$ be an increasing chain of elements of S. Then $X := \bigcup_{j=1}^{\infty} \{x_i\}_{i\in I_j}$ is a linearly independent set of M since any linear dependence occurs with the elements from some I_j. By Zorn's Lemma, there is a maximal element $\{x_i\}_{i\in I}$ of S. If $\{x_i\}_{i\in I}$ is a generating set, we are done.

Let $x \in M$. Then $\{x_i\}_{i\in I} \cup \{x\}$ is a linearly dependent set by maximality. For $x = x_{i_0}$, we have

$$\sum_{j=1}^{k} r_i x_{i_j} = 0$$

for all $r_i \neq 0$. Since R is a division ring,

$$x = -r_0^{-1} \left(\sum_{j=0}^{k} r_i x_{i_j} \right).$$

Thus x is in the span of $\{x_i\}_{i\in I}$ and $\{x_i\}_{i\in I}$ is a generating set of M. We conclude that all left R-modules are free. We make the same argument for right R-modules.

($\Leftarrow$) Assume that all R-modules are free. Thus all R-modules are projective and R is semisimple. Then R is left Artinian. Right multiplication $f : R \to R$ by some $a \in R$ is a left R-module homomorphism. Since Ra is free as a left R-module, f is an injective R-module homomorphism. By Proposition, f is a surjective left R-module homomorphism. There is some $b \in R$ such that $f(b) = ba = 1$. We conclude that every element $a \in R$ has a left inverse. Let c be the left inverse of b. Then $c = c(ba) = (cb)a = a$ and each element of R has an inverse. We conclude R is a division ring.

Lemma (Nakayama's Lemma)**.** Let R be a commutative ring with identity. Let I be an ideal of R and M a finitely-generated R-module. If $IM = M$, then there exists some $r \equiv 1 \pmod{I}$ such that $rM = 0$.

Corollary. Let R be a commutative ring with identity. Let M is a finitely-generated R-module with $J(R)$ the Jacobson radical of R. If $J(R)M = M$, then $M = 0$.

Proof. Nakayama's Lemma implies that $r - 1$ is in the Jacobson radical. Thus r is invertible. □

Spring 2019 Problem 4. Let R be a commutative local ring and P a finitely generated projective R-module. Prove that P is R-free.

Let $\{x_i\}_{i=1}^k$ be a minimal set of generators for P as an R-module. Then we have a surjection $f : R^k \to P$ and the short exact sequence

$$0 \to \ker(f) \to R^k \to P \to 0.$$

Since P is projective, the short exact sequence splits and $R^k \simeq P \oplus \ker(f)$. Let $N = \ker(f)$. We will show that N is trivial.

Let $\mathfrak{m}$ be the unique maximal ideal of R. Then $M/\mathfrak{m}M$ is a vector space over $R/\mathfrak{m}$ of the same dimension as $(R/\mathfrak{m})^k$. Thus $M/\mathfrak{m}M \simeq (R/\mathfrak{m})^k$ as $R/\mathfrak{m}$-vector spaces and $N = \mathfrak{m}N$. Since R is a commutative local ring, the Jacobson radical $J(R) = \mathfrak{m}$. By the second version of Nakayama's Lemma, $N = 0$ as desired.

Spring 2020 Problem 10. Let R be a commutative ring and M a left R-module. Let $f : M \to M$ be a surjective R-linear endomorphism. [Hint: Let $R[X]$ act on M via f.]

(a) Suppose that M is finitely generated. Show that f is an isomorphism and that f^{-1} can be described as a polynomial in f.

Let $R[X]$ act on M via $X \cdot m = f(m)$ and extend linearly. Let $I = (X) \subset R[X]$. Then f surjective gives $M = IM$. Nakayama's Lemma provides some $r \in R[X]$ for which $r \equiv 1 \pmod{(X)}$ and $rM = 0$. In other words, $r = 1 - Xp(X)$ for $p(X) \in R[X]$ and

$$\begin{aligned} r \cdot m &= 0 \\ (1 - Xp(X)) \cdot m &= 0 \\ m &= Xp(X) \cdot m. \end{aligned}$$

We conclude that $p(f)$ is the inverse of f.

(b) Show that this fails if M is not finitely generated.

Let M be the free module of countably many copies of R. Define $f : M \to M$ as

$$f(r_1, r_2 \ldots, r_k, \ldots) = (r_2, \ldots, r_k, \ldots).$$

Then f is surjective with kernel isomorphic to R.

Spring 2018 Problem 9. Let $f : M \to N$ and $g : N \to M$ be two R-linear homomorphisms of R-modules such that $\mathrm{id}_M - gf$ is invertible. Show that $\mathrm{id}_N - fg$ is invertible as well and give a formula for its inverse. [Hint: You may use Analysis to make a guess.]

Since $\mathrm{id}_M - gf : M \to M$ is invertible, there is some R-module homomorphism $c : M \to M$ such that $c(\mathrm{id}_M - gf) = \mathrm{id}_M = (\mathrm{id}_M - gf)c$. Note that $cgf = c - \mathrm{id}_M$ and $gfc = c - \mathrm{id}_M$. We claim the R-module homomorphism $\mathrm{id}_N + fcg : N \to N$ is the inverse of $\mathrm{id}_N - fg : N \to N$.

$$\begin{aligned} (\mathrm{id}_N + fcg)(\mathrm{id}_N - fg) &= \mathrm{id}_N - fg + fcg - f(cgf)g \\ &= \mathrm{id}_N - fg + fcg - f(c - \mathrm{id}_M)g \\ &= \mathrm{id}_N - fg + fcg - fcg + fg \\ &= \mathrm{id}_N \\ (\mathrm{id}_N - fg)(\mathrm{id}_N + fcg) &= \mathrm{id}_N + fcg - fg - f(gfc)g \\ &= \mathrm{id}_N + fcg - fg - f(c - \mathrm{id}_M)g \\ &= \mathrm{id}_N + fcg - fg - fcg + g \\ &= \mathrm{id}_N. \end{aligned}$$

Fall 2014 Problem 9. Let A be a ring and let $i, j \in A$ such that $i^2 = i$ and $j^2 = j$. Show that the left A-modules Ai and Aj are isomorphic if and only if there are $a, b \in A$ such that $i = ab$ and $j = ba$.

($\Rightarrow$) Assume Ai and Aj are isomorphic. Let $\phi : Ai \to Aj$ be such an isomorphism with inverse $\psi : Aj \to Ai$. Then $\phi(i) = cj$ and $\psi(j) = di$ for some $c, d \in A$. Note that $\phi(i) = \phi(i^2) = i\phi(i) = icj$ and $\psi(j) = \psi(j^2) = j\psi(j) = jdi$. Let $a := icj$ and $b := jdi$. Then

$$ab = (icj)(jdi) = icjdi = ic\psi(j) = \psi(icj) = \psi(\phi(i)) = i$$
$$ba = (jdi)(icj) = jdicj = jd\phi(i) = \phi(jdi) = \phi(\psi(j)) = j$$

as desired.

($\Leftarrow$) Assume $i = ab$ and $j = ba$ for some $a, b \in A$. Then we can define a left A-module homomorphism $\phi : Ai \to Aj$ by $\phi(i) = ia = aj$. Extend ϕ A-linearly. We can also define an A-module homomorphism $\psi : Aj \to Ai$ by extending $\psi(j) = jb = bi$ A-linearly. Let $r \in A$. Then

$$\psi(\phi(ri)) = \psi(r\phi(i)) = \psi(ria) = \psi(raj) = ra\psi(j) = rajb = rabi = ri^2 = ri$$
$$\phi(\psi(rj)) = \phi(r\psi(j)) = \phi(rjb) = \phi(rbi) = rb\phi(i) = rbia = rbaj = rj^2 = rj.$$

We conclude that ϕ is an isomorphism.

Fall 2020 Problem 4. Let M be a left R-module. Show that M is a projective R-module if and only if there exist $m_i \in M$ and R-homomorphisms $f_i : M \to R$ for each $i \in I$ such that the sets $\{m_i : i \in I\}$ and $\{f_i : i \in I\}$ satisfy:

(a) If $m \in M$, then $f_i(m) = 0$ for all but finitely many $i \in I$.

(b) If $m \in M$, then $m = \sum_{i \in I} f_i(m)m_i$.

($\Rightarrow$) Assume M is projective. Then M is a direct summand of a free R-module. There is a surjection $g : R^{|I|} \to M$. Define m_i as $g(e_i)$ for $(e_i)_{i \in I}$ the standard basis of $R^{|I|}$. Further, define f_i as the composition of the inclusion of M into $R^{|I|}$ and the projection onto the ith component.

($\Leftarrow$) The set $\{m_i : i \in I\}$ is a generating set of M. There is a surjection $g : R^{|I|} \to M$ given by $g(r_i) = r_i m_i$ where r_i is an element of the ith component of $R^{|I|}$. Define a splitting $f : M \to R^{|I|}$ as $f(m) = (f_i(m))_i$. Then $f(g(m)) = \sum_{i \in I} f_i(m)m_i = m$ by assumption (b). Since M is a direct summand of a free R-module, M is projective.

Math 210B Discussion Week 5

Matthew Gherman

February 3, 2022

Definition 1. Let F be a field. A *field extension* E of F is a field for which $F \subset E$. We can view E as a vector space over F and the *degree* of E over F is $[E : F] = \dim_F(E)$. A *finite* field extension is one in which the degree is finite.

Definition 2. An *algebraic field extension* E of F is one for which any element $a \in E$ is the root of some polynomial in $F[x]$. A field extension that is not algebraic is called *transcendental*.

Proposition. If E/F is a finite field extension, then it is algebraic.

Proposition. Let $E/L/F$ be a tower of finite field extensions. Then $[E : F] = [E : L][L : F]$.

Definition 3. Let K and L be two algebraic field extensions of F. Then the product KL is defined as the smallest field extension of F containing both K and L.

Proposition. Let K and L be two finite field extensions of F. If $[K : F]$ and $[L : F]$ are relatively prime and $K \cap L = F$, then $[KL : F] = [K : F][L : F]$.

Definition 4. Let E/F be an algebraic field extension. For some $\alpha \in E$, the minimal polynomial of α is the unique monic irreducible polynomial $p \in F[x]$ of lowest degree for which α is a root.

Definition 5. Let E be a field. Then a non-constant $f \in E[x]$ splits if it factors into linear terms.

Let E be a field extension of F. We say that E is the *splitting field* of some $f \in F[X]$ if f splits in $E[x]$ and $E = F[\alpha_1, \ldots, \alpha_n]$ for $\{\alpha_i\}$ the roots of f. A field extension E/F is *normal* if E is the splitting field of some polynomial $f \in F[x]$.

We say that f is *separable* if the linear factors of f in a splitting field are distinct. A *separable field extension* E/F is one in which the minimal polynomial of each element $\alpha \in E$ is separable.

Proposition. If F has $\mathrm{char}(F) = 0$ or F is finite, then every algebraic field extension of F is separable.

Definition 6. A *Galois extension* of F is the splitting field E of a separable polynomial $f \in F[x]$. In other words, the extension is normal and separable. The *Galois group* $\mathrm{Gal}(E/F)$ is the group of field automorphisms of E that fix all elements of F.

Proposition. If E/F is a finite Galois extension, then $|\mathrm{Gal}(E/F)| = [E : F]$.

Theorem (Galois correspondence)**.** Let E/F be a Galois extension. Let H be a subgroup of $\mathrm{Gal}(E/F)$. Define E^H to be the elements of E fixed by all automorphisms of H. There is a one-to-one correspondence between subgroups of $\mathrm{Gal}(E/F)$ and intermediate fields $E/L/F$ via $H \mapsto E^H$. The correspondence is inclusion reversing and $|H| = [E : E^H]$. Finally, E^H is a normal extension of F if and only if H is a normal subgroup of $\mathrm{Gal}(E/F)$.

Fall 2014 Problem 3. Pick a non-zero rational number x. Determine all possibilities for the Galois group G of the normal closure of $\mathbb{Q}[\sqrt[4]{x}]$ over $\mathbb{Q}$, where $\sqrt[4]{x}$ is the root of $X^4 - x$ with maximal degree over $\mathbb{Q}$.

Note that $\mathrm{char}(\mathbb{Q}) = 0$ so all finite extensions of $\mathbb{Q}$ are separable.

Case 1: Assume $x = y^4$ for some $y \in \mathbb{Q}$, then the roots of $X^4 - x$ are $\{\pm y, \pm yi\}$. A root of maximal degree is yi, and $\mathbb{Q}[yi] = \mathbb{Q}[i]$ is the splitting field of the irreducible polynomial $X^2 + 1$ over $\mathbb{Q}$. Thus $\mathbb{Q}[i]/\mathbb{Q}$ is a Galois extension of degree 2. The only group of order 2 is $\mathbb{Z}/2\mathbb{Z}$ so

$$\mathrm{Gal}(\mathbb{Q}[i]/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}.$$

Case 2: Assume $x = y^2$ for some $y \in \mathbb{Q}$ and $x \neq z^4$ for all $z \in \mathbb{Q}$. Then the roots of $X^4 - x$ are $\{\pm\sqrt{y}, \pm\sqrt{y}i\}$ for $\sqrt{y} \in \mathbb{R}$ and $X^4 - x = (X^2 - y)(X^2 + y)$. The two polynomials $X^2 - y$ and $X^2 + y$ are irreducible over $\mathbb{Q}$ since they do not have roots over $\mathbb{Q}$. Thus all of the roots have degree 2 so we can take $\sqrt[4]{x} = \sqrt{y}$. Then $\mathbb{Q}[\sqrt{y}]$ is the splitting field of $X^2 - y$ over $\mathbb{Q}$ and $\mathbb{Q}[\sqrt{y}]/\mathbb{Q}$ is Galois. Once again, the Galois group is order 2 so

$$\mathrm{Gal}(\mathbb{Q}[\sqrt{y}]/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}.$$

Case 3: Assume $x = -y^2$ for some $y \in \mathbb{Q}$ and $x \neq z^4$ for all $z \in \mathbb{Q}$. Then the roots of $X^4 - x$ are $\{\sqrt{y}\xi_8^j\}$ for ξ_8 a primitive eighth root of unity and $j = 1, 3, 5, 7$. Note that $\xi_8 = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$. These roots are not rational so $X^4 - x$ can only factor as a product of quadratics.

If $2y$ is the square of a rational number, then

$$(X - \sqrt{y}\xi_8)(X - \sqrt{y}\xi_8^7) = X^2 - \sqrt{2y}X + y$$
$$(X - \sqrt{y}\xi_8^3)(X - \sqrt{y}\xi_8^5) = X^2 - \sqrt{2y}X + y$$

The normal closure K is a degree 2 extension of $\mathbb{Q}$ and

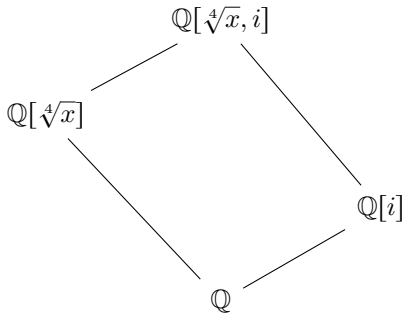
$$\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}.$$

In all other cases, none of the possible pairings of roots yields a quadratic with coefficients in $\mathbb{Q}$. Thus $X^4 - x$ is irreducible and the normal closure K is the splitting field of $X^4 - x$. It is clear that $K \subset \mathbb{Q}[\sqrt{2y}, i]$. Continuing, $\sqrt[4]{x}\xi_8 = \frac{\sqrt{2y}}{2} + \frac{\sqrt{2y}}{2}i$. We see that $2\sqrt[4]{x}\xi_8 + \sqrt[4]{x}\xi_8 = \sqrt{2y} \in K$. Then $\frac{2}{y}(\sqrt{2y}\sqrt[4]{x}\xi_8 - \frac{y}{2}) = i \in K$ as well. We conclude $K = \mathbb{Q}[\sqrt{2y}, i]$. Note the polynomials $X^2 - 2y$ and $X^2 + 1$ are irreducible so $\mathbb{Q}[\sqrt{2y}]/\mathbb{Q}$ and $\mathbb{Q}[i]/\mathbb{Q}$ are degree 2 Galois extensions with $\mathbb{Q}[\sqrt{2y}] \cap \mathbb{Q}[i] = \mathbb{Q}$ since $\mathbb{Q}[\sqrt{2y}] \subset \mathbb{R}$. Then

$$\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}[\sqrt{2y}]/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}[i]/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Case 4: Assume $x \neq y^2$ for all $y \in \mathbb{Q}$ and $x > 0$. The roots are $\{\pm\sqrt[4]{x}, \pm\sqrt[4]{x}i\}$ where we take $\sqrt[4]{x}$ to be the real fourth root of x. By assumption, $X^4 - x$ has no roots in $\mathbb{Q}$. None of the possible pairings of $(x - \alpha)$ for α a root of $X^4 - x$ gives a quadratic with coefficients in $\mathbb{Q}$. Thus $X^4 - x$ is irreducible and all the roots have degree 4, justifying the choice of $\sqrt[4]{x}$ as the real fourth root. Let K be the normal closure of $\mathbb{Q}[\sqrt[4]{x}]/\mathbb{Q}$. Since $X^4 - x$ is irreducible, K will be the splitting field of $X^4 - x$. We note that $K \subset \mathbb{Q}[\sqrt[4]{x}, i]$ since $X^4 - x$ splits in $\mathbb{Q}[\sqrt[4]{x}, i]$. Additionally, $\sqrt[4]{x} \in K$ and $\frac{1}{x}(\sqrt[4]{x})^3(\sqrt[4]{x}i) = i \in K$ so $K = \mathbb{Q}[\sqrt[4]{x}, i]$.

We build the tower of field extensions below. We know that $[\mathbb{Q}[\sqrt[4]{x}] : \mathbb{Q}] = 4$ and $[\mathbb{Q}[i] : \mathbb{Q}] = 2$. Since $\mathbb{Q}[\sqrt[4]{x}] \subset \mathbb{R}$, we have $\mathbb{Q}[\sqrt[4]{x}] \cap \mathbb{Q}[i] = \mathbb{Q}$ and $[\mathbb{Q}[\sqrt[4]{x}, i] : \mathbb{Q}] = 8$, as a result. Note that $\mathbb{Q}[\sqrt[4]{x}]/\mathbb{Q}$ is not a normal extension so $\mathbb{Q}[\sqrt[4]{x}, i]/\mathbb{Q}$ is not an abelian extension. Thus $\mathrm{Gal}(\mathbb{Q}[\sqrt[4]{x}, i]/\mathbb{Q})$ is a non-abelian group of order 8. This leaves the quaternion group or the dihedral group.



Complex conjugation τ is an order 2 automorphism. In both D_4 and Q_8, there is an element of order 4. Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ be such an element. If $\sigma(\sqrt[4]{x}) = -\sqrt[4]{x}$, then $\sigma(\sqrt[4]{x}i) = \sqrt[4]{x}i$ or $\sigma(\sqrt[4]{x}i) = -\sqrt[4]{x}i$. In either case, σ^2 is the identity, a contradiction. Thus $\sigma(\sqrt[4]{x}) = \pm\sqrt[4]{x}i$. The argument will work for either choice so assume $\sigma(\sqrt[4]{x}) = \sqrt[4]{x}i$. We see that $\sigma\tau(\sqrt[4]{x}) = \sigma(\sqrt[4]{x}) = \sqrt[4]{x}i$ and $\tau\sigma(\sqrt[4]{x}) = \tau(\sqrt[4]{x}i) = -\sqrt[4]{x}i$. Thus σ and τ do not commute. The order 2 element -1 in the quaternion group commutes with the order 4 elements. We conclude

$$\mathrm{Gal}(\mathbb{Q}[\sqrt[4]{x}, i]/\mathbb{Q}) \simeq D_4.$$

Case 5: Assume $x \neq y^2$ for all $y \in \mathbb{Q}$ and $x < 0$. Let $z = |x|$. Then the roots of $X^4 - x$ are $\{\sqrt[4]{z}\xi_8^i\}$ for $\sqrt[4]{z}$ the real fourth root and $i \in \{1, 3, 5, 7\}$. The roots are not contained in $\mathbb{Q}$ and none of the possible pairings of roots

yields a quadratic with coefficients in $\mathbb{Q}$. Thus $X^4 - x$ is irreducible and the normal closure K is the splitting field of $X^4 - x$. It is clear that $K \subset \mathbb{Q}[\sqrt[4]{4z}, i]$ since $\sqrt[4]{z}\xi_8 = \sqrt[4]{z}(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i)$. But, $\sqrt[4]{z}\xi_8 + \sqrt[4]{z}\xi_8^7 = \sqrt[4]{z}\sqrt{2} = \sqrt[4]{4z} \in K$ and $\sqrt[4]{z}\xi_8^3 + \sqrt[4]{z}\xi_8^5 = \sqrt[4]{z}\sqrt{2}i = \sqrt[4]{4z}i \in K$. Then $(\frac{1}{4z})(\sqrt[4]{4z})^3(\sqrt[4]{4z}i) = i \in K$. We conclude that $K = \mathbb{Q}[\sqrt[4]{4z}, i]$. This is Case 4 since $4z \in \mathbb{Q}$ so

$$\mathrm{Gal}(K/\mathbb{Q}) \simeq D_4.$$

Dedekind Domains

Matthew Gherman

February 3, 2022

Definition 1. The following are equivalent definitions of a *Dedekind domain*.

(a) A *Dedekind domain* is an integral domain in which each non-zero proper ideal factors into a product of prime ideals. This factorization can be shown to be unique up to reordering of the factors.

(b) A *Dedekind domain* is an integrally closed, Noetherian domain in which each prime ideal is maximal.

(c) A *Dedekind domain* is Noetherian and the localization at each maximal ideal is a DVR.

Proposition. A Dedekind domain is a PID if and only if it is a UFD.

Proof. We need only prove that every ideal in a Dedekind domain R with unique factorization is principal. Further, unique factorization of prime ideals means it is sufficient to prove each prime ideal is principal. Let $\mathfrak{p}$ be a non-zero prime ideal of R with $a \in \mathfrak{p}$. Let $a = p_1 \cdots p_k$ be a unique factorization of a into prime elements of R. Then $\mathfrak{p}$ divides $(a) = (p_1) \cdots (p_k)$ so $\mathfrak{p}$ contains some prime ideal (p_i). Since R has dimension one, $\mathfrak{p} = (p_i)$ and $\mathfrak{p}$ is principal. □

Example 1. The ring $R = \mathbb{R}[x, y]/(x^2 + y^2 - 1)$ is a Dedekind domain that is not a PID and, thus, not a UFD.

Definition 2. Let R be an integral domain and K its field of fractions. A *fractional ideal* is an R-submodule of K for which there is some $r \in R$ such that $rI \subset R$. We think of r as clearing denominators in I.

Definition 3. A fractional ideal I of R is *invertible* if there is another fractional ideal J of R for which $IJ = R$.

Definition 4. A *Dedekind domain* is, equivalently, an integral domain for which each fractional ideal is invertible. The inverse of a fractional ideal I is given by $\{x \in K : xI \subset R\}$.

Spring 2017 Problem 4. Show that the ring $R = \mathbb{C}[x, y]/(y^2 - x^3 + 1)$ is a Dedekind domain. (Hint: Compare R with the subring $\mathbb{C}[x]$.)

The ring R is a quotient of the Noetherian ring $\mathbb{C}[x, y]$ so R is Noetherian. The polynomial $y^2 - x^3 + 1$ would have to factor in $\mathbb{C}[x, y]$ as a product of two degree one polynomials in y. By inspection, the polynomial is irreducible in $\mathbb{C}[x, y]$. Thus $(y^2 - x^3 + 1)$ is a prime ideal in $\mathbb{C}[x, y]$ so R is an integral domain. Further, $\mathbb{C}[x, y]$ has Krull dimension two so, by the prime ideal correspondence, R has Krull dimension one.

It is thus sufficient to show that R is the integral closure of the subring $\mathbb{C}[x]$ in the fraction field of R, which is $K = \mathbb{C}(x)[y]/(y^2 - (x^3 - 1))$. Let $\alpha \in \mathbb{C}(x)[y]/(y^2 - (x^3 - 1))$ be integral over $\mathbb{C}[x]$. The set $\{1, y\}$ is a basis for $\mathbb{C}(x)[y]/(y^2 - (x^3 - 1))$ as a $\mathbb{C}(x)$-vector space. Thus $\alpha = p + qy$ for $p, q \in \mathbb{C}(x)$. If $q = 0$, $\alpha \in \mathbb{C}[x] \subset R$ so we may assume $q \neq 0$. Let $m = T^2 - 2pT + (p^2 + q^2(x^3 - 1)) \in \mathbb{C}(x)[T]$ be the minimal polynomial of α over $\mathbb{C}(x)$. Since $\mathbb{C}[x]$ is a UFD, Gauss's Lemma implies that $m \in \mathbb{C}[x][T]$. Then $2p \in \mathbb{C}[x]$ gives $p \in \mathbb{C}[x]$. Since $p^2 + q^2(x^3 - 1) \in \mathbb{C}[x]$, we have $q^2(x^3 - 1) \in \mathbb{C}[x]$. From $x^3 - 1$ square-free in $\mathbb{C}[x]$, we conclude $q \in \mathbb{C}[x]$ and $\alpha \in R$. Therefore, R is the integral closure of $\mathbb{C}[x]$ in $\mathbb{C}(x)[y]/(y^2 - (x^3 - 1))$, which implies R is a Dedekind domain.

Spring 2018 Problem 10. By one definition, a Dedekind domain is a commutative Noetherian integral domain R, integrally closed in its fraction field, such that R is not a field and every nonzero prime ideal in R is maximal. Let R be a Dedekind domain, and let S be a multiplicatively closed subset of R. Show that the localization $S^{-1}R$ is either the zero ring, a field, or a Dedekind domain.

If $0 \in S$, then $S^{-1}R$ is the zero ring. If $S = R\backslash\{0\}$, then $S^{-1}R$ is a field. Assume $0 \notin S$ and $S \neq S\backslash\{0\}$. It is clear that $S^{-1}R$ is a commutative integral domain since R is an integral domain. There is a bijective correspondence between the ideals of $\mathfrak{p} \subset R$ that intersect trivially with S and the ideals of $S^{-1}\mathfrak{p} \subset S^{-1}R$. Let

$$S^{-1}I_1 \subset S^{-1}I_2 \subset \dots$$

be an increasing chain of ideals in $S^{-1}R$. Then $I_1 \subset I_2 \subset \dots$ is an increasing chain of ideals in R for

$$I_j := \left\{ r \in R : \frac{r}{1} \in S^{-1}I_j \right\},$$

the ideal of numerators in $S^{-1}I_j$. Since R is Noetherian, the chain terminates so $I_k = I_{k+i}$ for all $i \in \mathbb{N}$. As a result $S^{-1}I_k = S^{-1}I_{k+i}$ for all $i \in \mathbb{N}$ and the chain in $S^{-1}R$ terminates. We conclude that $S^{-1}R$ is Noetherian.

We have a correspondence between prime ideals $\mathfrak{p} \subset R$ that do not intersect S and prime ideals $S^{-1}\mathfrak{p} \subset S^{-1}R$. Take a chain of prime ideals

$$0 \subset S^{-1}\mathfrak{p}_1 \subset S^{-1}\mathfrak{p}_2 \subset \dots$$

which corresponds to a chain of prime ideals $0 \subset \mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \dots$ of R. Each non-zero prime ideal of R is maximal so $\mathfrak{p}_i = \mathfrak{p}_1$ for all $i \in \mathbb{N}$. Thus $S^{-1}\mathfrak{p}_i = S^{-1}\mathfrak{p}_1$ for all $i \in \mathbb{N}$. We conclude that each non-zero prime ideal of $S^{-1}R$ is maximal.

We will show that $S^{-1}R$ is integrally closed in its fraction field. Let K be the fraction field of R and $S^{-1}R$ is a subring of K. Let $\frac{r}{s} \in K$ be integral over $S^{-1}R$. If $\frac{r}{s} \in R$, then $\frac{r}{s} \in S^{-1}R$ so assume $\frac{r}{s} \notin R$. There is a monic polynomial $f = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in (S^{-1}R)[x]$ such that $f(\frac{r}{s}) = 0$. Each $a_i = \frac{r_i}{s_i}$ for $r_i \in R$ and $s_i \in S$. Define $t := \prod_{i=1}^{n-1} s_i \in S$ so

$$\begin{aligned} 0 &= \left(\frac{r}{s}\right)^n + \frac{r_{n-1}}{s_{n-1}}\left(\frac{r}{s}\right)^{n-1} + \dots + \frac{r_0}{s_0} \\ &= t^n\left(\frac{r}{s}\right)^n + t^n\frac{r_{n-1}}{s_{n-1}}\left(\frac{r}{s}\right)^{n-1} + \dots + t^n\frac{r_0}{s_0} \\ &= \left(\frac{tr}{s}\right)^n + \frac{tr_{n-1}}{s_{n-1}}\left(\frac{tr}{s}\right)^{n-1} + \dots + \frac{t^n r_0}{s_0}. \end{aligned}$$

Note that $\frac{t^i r_{n-i}}{s_{n-i}} \in R$ by the choice of $t \in S$. Thus $\frac{tr}{s}$ is a root of a monic polynomial in $R[x]$. Since R is integrally closed, $\frac{tr}{s} \in R$. Then $\frac{r}{s} = \frac{r'}{t} \in S^{-1}R$ for some $r' \in R$. We conclude that $S^{-1}R$ is integrally closed in K. As a result, $S^{-1}R$ is a Dedekind domain.

Fall 2020 Problem 7(a). Let R be a Dedekind domain with quotient field K and I a non-zero ideal in R. Show that every ideal in R/I is a principal ideal.

Since R is a Dedekind domain, there is a unique factorization of I into prime ideals given by $I = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_m^{k_m}$. Then the Chinese Remainder Theorem implies

$$R/I \simeq \oplus_{i=1}^m R/\mathfrak{p}_i^{k_i} \simeq \oplus_{i=1}^m R_{\mathfrak{p}_i}/\mathfrak{p}_i^{k_i}R_{\mathfrak{p}_i}.$$

Each prime ideal is maximal in R so $R_{\mathfrak{p}_i}$ is a DVR and, thus, a PID. The quotient of a PID by an ideal will remain a principal ideal ring via the ideal correspondence. Thus R/I is isomorphic to the direct sum of principal ideal rings, which implies R/I is a principal ideal ring.

Spring 2016 Problem 3. Let A be an integral domain with field of fractions F. For an A-ideal $\mathfrak{a}$, prove that $\mathfrak{a}$ is an A-projective ideal finitely generated over A if there exists an A-submodule $\mathfrak{b}$ of F such that $\mathfrak{ab} = A$, where $\mathfrak{ab}$ is an A-submodule of F generated by ab for all $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$.

We will first show that $\mathfrak{a}$ is a finitely generated ideal of A. Since $\mathfrak{ab} = A$, there is a finite sum $\sum_{i=1}^n a_i b_i = 1$ for $a_i \in \mathfrak{a}$ and $b_i \in \mathfrak{b}$. Let $a \in A$, then $a = a(\sum_{i=1}^n a_i b_i) = \sum_{i=1}^n a_i(ab_i)$. Since $\mathfrak{ab} = A$, we have $ab_i \in A$ for all $1 \leqslant i \leqslant n$. Thus $\{a_i\}_{i=1}^n$ is a generating set of A as an A-module.

Now we will show that $\mathfrak{a}$ is a projective ideal of A. Since $\mathfrak{a}$ is finitely generated by $\{a_i\}_{i=1}^n$, there is a short exact sequence

$$0 \longrightarrow \ker(f) \longrightarrow A^n \xrightarrow{f} \mathfrak{a} \longrightarrow 0$$

with $f(e_i) = a_i$ for $\{e_i\}_{i=1}^n$ the standard generating set of A^n. Define the A-module homomorphism $h : \mathfrak{a} \to A^n$ by $h(a) = \sum_{i=1}^n (ab_i e_i)$. Then $f(h(a)) = f(\sum_{i=1}^n (ab_i e_i)) = \sum_{i=1}^n ab_i f(e_i) = \sum_{i=1}^n ab_i a_i = a$. We conclude that h is a splitting and $A^n \simeq \mathfrak{a} \oplus \ker(f)$. Since $\mathfrak{a}$ is a direct summand of a free A-module, $\mathfrak{a}$ is a projective A-module.

Math 210B Discussion Week 6

Matthew Gherman

February 10, 2022

Spring 2016 Problem 10.

(a) Determine the Galois group of the polynomial $X^4 - 2$ over $\mathbb{Q}$, as a subgroup of a permutation group. Also, give generators and relations for this group.

See Fall 2014 Problem 3 Case 4.

(b) Determine the Galois group of the polynomial $X^3 - 3X - 1$ over $\mathbb{Q}$. (Hint: for polynomials of the form $X^3 + aX + b$, the quantity $\Delta = -4a^3 - 27b^2$, known as the discriminant, plays a key theoretical role.) Explain your answer.

Let K be the splitting field of an irreducible polynomial in $F[x]$ with roots $\{\alpha_1, \dots, \alpha_n\}$. Define

$$\delta := \prod_{i<j} (\alpha_i - \alpha_j),$$

and the discriminant $\Delta := \delta^2$. For $\sigma \in \mathrm{Gal}(f)$, $\sigma(\delta) = \mathrm{sign}(\sigma)\delta$ so $\sigma(\Delta) = \Delta$ for all $\sigma \in \mathrm{Gal}(f)$. Thus $\Delta \in F$, and each $\sigma \in \mathrm{Gal}(f)$ such that $\sigma(\delta) = \delta$ must be an even permutation of the roots of f. If $\delta \in F$, then $\mathrm{Gal}(f)$ must be a subgroup of A_n.

For a degree 3 polynomial, there will be at least one real root. The other roots could both be real or could be a conjugate pair of complex roots. Let the roots of f be $\{x, a + bi, a - bi\}$ for $a, b, x \in \mathbb{R}$, then

$$\delta = (x - (a + bi))(x - (a - bi))(a + bi - (a - bi)) = 2bi(x^2 - 2x + (a^2 + b^2)).$$

Note $\Delta = \delta^2 < 0$ for $b \neq 0$. In this problem, $\Delta = -4a^3 - 27b^2 = -4(-3)^3 - 27(-1)^2 = 81 > 0$ so the roots of f are real. Since $\Delta = 9^2$, we have $\delta \in \mathbb{Q}$. By above, $\mathrm{Gal}(f)$ embeds in A_3, and $|\mathrm{Gal}(f)| \leqslant |A_3| = 3$. By the rational root test, f is irreducible over $\mathbb{Q}$. Then $[F[\alpha] : F] = 3 = |\mathrm{Gal}(f)| = |A_3|$ for some $\alpha \in \mathbb{R}$ a root of f. We conclude $\mathrm{Gal}(f) \simeq A_3$.

Proposition. A polynomial $p \in F[x]$ is separable if and only if it is relatively prime to its formal derivative.

Fall 2017 Problem 7.

(a) Show that there is at most one extension $F(\alpha)$ of a field F such that $\alpha^4 \in F$, $\alpha^2 \notin F$, and $F(\alpha) = F(\alpha^2)$.

We have that α is a root of $f := x^4 - \alpha^4 \in F[x]$ and α^2 is a root of the irreducible polynomial $x^2 - \alpha^4$. Thus $[F[\alpha^2] : F] = 2$.

Assume first that $\mathrm{char}(F) = 2$. Then $x^4 - \alpha^4 = x^4 + \alpha^4 = (x + \alpha)^4$. Since $[F[\alpha] : F] = [F[\alpha^2] : F] = 2$, the minimal polynomial of α must be $(x + \alpha)^2$, which implies $\alpha^2 \in F$, a contradiction.

Assume $\mathrm{char}(F) \neq 2$. Then $f' = 4x^3 \neq 0$, which is relatively prime to f. Then f is separable with roots $\{\pm\alpha, \pm\alpha\xi\}$ for $\xi^2 = -1$. We have two cases for the minimal polynomial of α, denoted $m_\alpha \in F[x]$. If $m_\alpha = (x - \alpha)(x + \alpha)$, then $\alpha^2 \in F$, a contradiction. If $m_\alpha = (x \pm \alpha)(x \pm \alpha\xi)$, then $\alpha^2\xi \in F$. Note $\xi \in F$ would imply $\alpha^2 \in F$ so $\xi \notin F$. But $\alpha^2(\alpha^2\xi) = \alpha^4\xi \in F[\alpha^2] = F[\alpha]$ so $\xi \in F[\alpha]$. We have the tower of fields $F[\alpha]/F[\xi]/F$ with $[F[\alpha] : F] = 2$. Since $\xi \notin F$, we conclude $F[\alpha] = F[\xi]$. Therefore, there is at most one field extension like $F[\alpha]$ since it would equal $F[\xi]$.

(b) Find the isomorphism class of the Galois group of the splitting field of $x^4 - a$ for $a \in \mathbb{Q}$ with $a \notin \pm\mathbb{Q}^2$.

By Fall 2014 Problem 3 Case 4, we have $G \simeq D_4$ for $a > 0$ and, by Fall 2014 Problem 3 Case 5, we have $G \simeq D_4$ for $a < 0$.

Proposition (Eisenstein's Criterion)**.** Let $f \in \mathbb{Z}[x]$ with $f = a_n x^n + \cdots + a_0$. If there exists a prime $p \in \mathbb{Z}$ for which p divides a_i for $0 \leqslant i < n$, p does not divide a_n, and p^2 does not divide a_0, then f is irreducible in $\mathbb{Q}[x]$.

Fall 2016 Problem 7. Let $f \in \mathbb{Q}[X]$ and $\xi \in \mathbb{C}$ a root of unity. Show that $f(\xi) \neq 2^{1/4}$.

We will assume that $f(\xi) = 2^{1/4}$ for some $f \in \mathbb{Q}[X]$ and draw a contradiction. We know that $\mathbb{Q}[\xi]/\mathbb{Q}$ is a Galois extension with $\mathrm{Gal}(\mathbb{Q}[\xi]/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ for ξ a primitive nth root of unity. In particular, $\mathrm{Gal}(\mathbb{Q}[\xi]/\mathbb{Q})$ is abelian so $\mathbb{Q}[\xi]/\mathbb{Q}$ is an abelian Galois extension. By assumption $f(\xi) = 2^{1/4}$ so $2^{1/4} \in \mathbb{Q}[\xi]$ and $\mathbb{Q}[2^{1/4}]/\mathbb{Q}$ is a subextension of $\mathbb{Q}[\xi]/\mathbb{Q}$. By the Galois correspondence, $\mathbb{Q}[2^{1/4}] = (\mathbb{Q}[\xi])^H$ for some subgroup $H \subset \mathrm{Gal}(\mathbb{Q}[\xi]/\mathbb{Q})$ and $\mathbb{Q}[2^{1/4}]/\mathbb{Q}$ should be a normal extension since any subgroup of an abelian group is normal. The minimal polynomial of $2^{1/4}$ over $\mathbb{Q}$ is $x^4 - 2$ which is irreducible by Eisenstein's Criterion. But $x^4 - 2$ does not split in $\mathbb{Q}[2^{1/4}]$ so $\mathbb{Q}[2^{1/4}]/\mathbb{Q}$ is not a Galois extension, contradicting our assumption. We conclude that $f(\xi) \neq 2^{1/4}$ for all $f \in \mathbb{Q}[X]$.

Math 210B Discussion Week 7

Matthew Gherman

February 17, 2022

Theorem (Primitive Element Theorem)**.** There are two common formulations of the result. Result (b) implies (a) via the Galois correspondence.

(a) Every separable field extension of finite degree has the form $F(\beta)/F$ for some β. The element β is known as a *primitive element.*

(b) A finite field extension is separable if and only if there exist finitely many intermediate field extensions.

Fall 2018 Problem 3. Let K/F be a finite extension of fields. Suppose that there exist finitely many intermediate fields $K/E/F$. Show that $K = F(x)$ for some $x \in K$.

If F is a finite field, then K is also a finite field of the same characteristic. We know $K^\times$ is cyclic so $K = F(x)$ for some $x \in K$.

Assume F is not finite. Let $\alpha, \beta \in K$. By assumption, there are only a finite number of distinct fields $F(\alpha + c\beta)$ for all $c \in F$. Since F is infinite, there are $c_1, c_2 \in F$ with $c_1 \neq c_2$ such that $E := F(\alpha + c_1\beta) = F(\alpha + c_2\beta)$. Thus $(c_1 - c_2)\beta \in E$ and $\beta \in E$. Further, $\alpha \in E$ and the field $F(\alpha, \beta)$ can be generated by one element. By an inductive argument, for $E = F(\alpha_1, \ldots, \alpha_n)$ there are corresponding $c_1, \ldots, c_n$ such that $E = F(\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n)$. Since K/F is a finite field extension, $K = F(\alpha_1, \ldots, \alpha_n)$ so $K = F(x)$ for some $x \in K$.

This proof is based on that of the Primitive Element Theorem found in Lang Section 5.4.

Spring 2015 Problem 6. Let $K \subset L$ be subfields of $\mathbb{C}$ and let p be a prime. Assume K contains a non-trivial p-th root of unity. Show that L/K is a degree p Galois extension if and only if there is an element $a \in K$ that does not admit a p-th root, such that $L = K(\sqrt[p]{a})$.

($\Rightarrow$) Assume that L/K is a degree p Galois extension. Let $G := \mathrm{Gal}(L/K)$. Then G is cyclic, generated by some $\sigma \in G$. Let ξ be a primitive p-th root of unity. Since some primitive p-th root of unity is contained in K, we have all primitive p-th roots of unity in K. Thus $\xi \in K$ and $\sigma(\xi) = \xi$. Since L/K is separable, the Primitive Element Theorem implies $L = K[\beta]$ for some β in the algebraic closure of K. Define $\alpha := \sum_{i=0}^{p-1} \sigma^i(\beta)\xi^{p-i}$. Then

$$\sigma(\alpha) = \sigma\left(\sum_{i=0}^{p-1} \sigma^i(\beta)\xi^{p-i}\right) = \sum_{i=0}^{p-1} \sigma^{i+1}(\beta)\sigma(\xi)^{p-i} = \sum_{i=0}^{p-i} \sigma^{i+1}(\beta)\xi^{p-i} = \sum_{i=1}^{p} \sigma^i(\beta)\xi^{p-i+1} = \alpha\xi$$
$$\sigma(\alpha^p) = \sigma(\alpha)^p = (\alpha\xi)^p = \alpha^p\xi^p = \alpha^p$$

shows that $\alpha \notin K$. Additionally G is cyclic so α^p is fixed by G and $\alpha^p \in K$. Define $a := \alpha^p \in K$. Then the splitting field $M := K[\alpha]$ of $x^p - a$ is a subfield of L that strictly contains K. Then $[M : K] \neq 1$ divides $[L : K] = p$ so $[M : K] = p$. We conclude that $L = M = K[\sqrt[p]{a}]$.

($\Leftarrow$) Assume there is an element $a \in K$ that does not admit a p-th root and $L = K(\sqrt[p]{a})$. Then L is the splitting field of $x^p - a$ over K. The roots of $x^p - a$ are $\{\sqrt[p]{a}\xi^i\}$ for ξ a primitive p-th root of unity and $0 \leqslant i \leqslant p-1$. Since $\mathrm{char}(K) = 0$, K is a perfect field. Then L/K is separable and, thus, Galois. Note $\sqrt[p]{a} \notin K$ so there is some $\sigma \in \mathrm{Gal}(L/K)$ that does not fix $\sqrt[p]{a}$. The image of $\sqrt[p]{a}$ is a root which gives $\sigma(\sqrt[p]{a}) = \sqrt[p]{a}\xi^i$ for some $1 \leqslant i \leqslant p-1$. We have $\sigma^p(\sqrt[p]{a}) = \sqrt[p]{a}$ and $\sigma^j(\sqrt[p]{a}) \neq \sqrt[p]{a}$ for all $1 \leqslant j \leqslant p-1$ since p is prime. The order of σ must be at least p. However, L/F Galois implies $p \leqslant |\mathrm{Gal}(L/F)| = [L : F] = [K(\sqrt[p]{a}) : K] \leqslant p$. Thus $[L : K] = p$.

Spring 2016 Problem 7. Show that for every positive integer n, there exists a cyclic extension of $\mathbb{Q}$ of degree n which is contained in $\mathbb{R}$.

By Dirichlet's Theorem, there is some odd prime integer p such that $p \equiv 1 \pmod{2n}$. Let ξ be a primitive pth root of unity. We know that $\mathbb{Q}[\xi]/\mathbb{Q}$ is a Galois extension with $[\mathbb{Q}[\xi] : \mathbb{Q}] = \varphi(p) = p - 1$ for $\varphi : \mathbb{Z} \to \mathbb{Z}$ Euler's totient function. The Galois group $G := \mathrm{Gal}(\mathbb{Q}[\xi]/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ is cyclic. Complex conjugation $\tau : \mathbb{Q}[\xi] \to \mathbb{Q}[\xi]$ is an order two $\mathbb{Q}$-automorphism of $\mathbb{Q}[\xi]$. Let H be the order two subgroup of G generated by τ and $K := \mathbb{Q}[\xi]^H$. We have $K \subset \mathbb{R}$ since K is fixed by complex conjugation. (For a more explicit description, $K = \mathbb{Q}[\xi + \xi^{-1}]$.) Then Galois correspondence implies $\mathbb{Q}[\xi]/K$ is Galois with $[\mathbb{Q}[\xi] : K] = 2$. As a result, $[K : \mathbb{Q}] = \frac{p-1}{2} = kn$ for some positive integer k. Since $\mathbb{Q}[\xi]/\mathbb{Q}$ is cyclic, H is a normal subgroup of G so $K/\mathbb{Q}$ is Galois with $\mathrm{Gal}(K/\mathbb{Q}) \simeq G/H$. The group G/H is cyclic so $K/\mathbb{Q}$ is a cyclic extension of $\mathbb{Q}$ of degree kn with $K \subset \mathbb{R}$. The fixed field of the unique subgroup of order k in $\mathrm{Gal}(K/\mathbb{Q})$ is the desired cyclic degree n extension.

Fall 2016 Problem 5. Let $f \in F[X]$ be an irreducible separable polynomial of prime degree over a field F and let K/F be a splitting field of f. Prove that there is an element in the Galois group of K/F permuting cyclically all roots of f in K.

Note that K/F is a Galois extension since f is separable and K is the splitting field of f. Let $\alpha \in K$ be a root of f. Then $F[\alpha]/F$ is a field extension with $[F[\alpha] : F] = p$ since f is irreducible. Then $K/F[\alpha]/F$ is a tower of field extensions so $[F[\alpha] : F] = p$ divides $[K : F]$. Now $|\mathrm{Gal}(K/F)| = [K : F]$ since K/F is a finite Galois extension of F. Thus $p||\mathrm{Gal}(K/F)|$ and Cauchy's Theorem implies there is some element $\sigma \in \mathrm{Gal}(K/F)$ of order p. We know σ permutes the roots of f, of which there are p, so σ must permute the roots cyclically. Alternatively, embed the Galois group into the symmetric group S_p. The order p elements are p-cycles.

Spring 2016 Problem 6. Let K be a field of characteristic $p > 0$. For an element $a \in K$, show that the polynomial $P(X) = X^p - X + a$ is irreducible over K if and only if it has no root in K. Show also that, if P is irreducible, then any root of it generates a cyclic extension of K of degree p.

($\Rightarrow$) We will prove the contrapositive. Assume P has a root $\alpha \in K$. We can immediately conclude that P is not irreducible in K since $P = (X - \alpha)g$ for some $g \in K[X]$.

($\Leftarrow$) We will prove the contrapositive. Assume P is reducible so $P = \prod_{i=1}^{k} g_i$ for irreducible $g_i \in K[X]$ with $\deg(g_i) < p$. Let $\alpha \in \overline{K}$ be a root of $g := g_1$. Then α is a root of P and $\alpha^p - \alpha + a = 0$. Since K is a field of characteristic p, we have $\mathbb{F}_p \subset K$ for $\mathbb{F}_p$ the field of p elements. Let $k \in \mathbb{F}_p$. Then

$$(\alpha + k)^p - (\alpha + k) + a = \alpha^p + k^p - \alpha - k + a = \alpha^p + k - \alpha - k + a = \alpha^p - \alpha + a = 0.$$

We conclude that the set of roots of P is $\{\alpha + k : k \in \mathbb{F}_p\} \subset K[\alpha]$, which implies P is separable over K. Further, $K[\alpha]$ is the splitting field of P so $K[\alpha]/K$ is a Galois extension. Let $G := \mathrm{Gal}(K[\alpha]/K)$ and take $\sigma \in G$. Then $\sigma(\alpha) = \alpha + k$ for $k \in \mathbb{F}_p$. We see that $\sigma^\ell(\alpha) = \alpha + k\ell$. Then $k\ell = 0$ in $\mathbb{F}_p$ implies $k = 0$ in $\mathbb{F}_p$ or $p|\ell = 0$ in $\mathbb{Z}$. In the latter case, the order of σ is at least p. Since $\sigma^p(\alpha) = \alpha$, we have that the order of σ is p. Then $|G| \geqslant p$, contradicting our assumption that $\deg(g) < p$. We conclude $\sigma(\alpha) = \alpha$ and $g = X - \alpha$, which implies P has a root in K.

Assume P is irreducible. Let $\alpha \in \overline{K}$ be a root of P. By above, the roots of the separable polynomial P are $\{\alpha + k : k \in \mathbb{F}_p\}$ so P splits in $K[\alpha]$. Then $K[\alpha]/K$ is Galois with $[K[\alpha] : K] = p$. The Galois group $\mathrm{Gal}(K[\alpha]/K)$ is order p and, thus, cyclic. We conclude that any root of P generates a cyclic extension of K of degree p.

The polynomial in question is an example of an Artin-Schreier polynomial.

Proposition. Let L and M be field extensions of K. If L is a Galois extension of K, then the following are equivalent:

(a) L and M are linearly disjoint over K

(b) $L \cap M = K$

(c) The restriction map $\mathrm{Gal}(LM/M) \to \mathrm{Gal}(L/K)$ is an isomorphism.

Spring 2018 Problem 2. Let $\zeta^9 = 1$ and $\zeta^3 \neq 1$ with $\zeta \in \mathbb{C}$.

(a) Show that $\sqrt[3]{3} \notin \mathbb{Q}(\zeta)$.

For the sake of contradiction, assume that $\sqrt[3]{3} \in \mathbb{Q}(\zeta)$. Note that ζ is a primitive ninth root of unity. Then $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a Galois extension with $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq (\mathbb{Z}/9\mathbb{Z})^\times$. In particular, $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is abelian. The

polynomial $f = x^3 - 3$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion with roots $\{\sqrt[3]{3}\zeta^{3i}\}_{i=0}^{2}$ for $\sqrt[3]{3} \in \mathbb{R}$. Thus $\mathbb{Q}(\sqrt[3]{3}) \subset \mathbb{R}$ is not the splitting field of f, the minimal polynomial of $\sqrt[3]{3}$. Since $\mathbb{Q}(\zeta)/\mathbb{Q}$ is abelian, $\mathbb{Q}(\sqrt[3]{3})/\mathbb{Q}$ is a normal extension, a contradiction. We conclude that $\sqrt[3]{3} \notin \mathbb{Q}(\zeta)$.

(b) If $\alpha^3 = 3$, show that α is not a cube in $\mathbb{Q}(\zeta, \alpha)$.

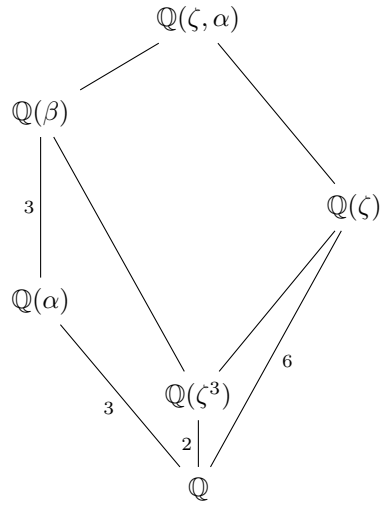
Assume that $\beta^3 = \alpha$ and $\beta \in \mathbb{Q}(\zeta, \alpha)$ for the sake of contradiction. Then $\mathbb{Q}(\zeta, \alpha)$ is the splitting field of $m_\beta = x^9 - 3$ over $\mathbb{Q}$. By Eisenstein's Criterion, m_β is irreducible in $\mathbb{Q}[x]$ so $[\mathbb{Q}(\beta) : \mathbb{Q}] = 9$. Since $\mathbb{Q}$ is perfect, $\mathbb{Q}(\zeta, \alpha)/\mathbb{Q}$ is a Galois extension. We build the tower of fields below. Since $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\zeta)$ is a subfield of a degree 3 extension $\mathbb{Q}(\alpha)/\mathbb{Q}$, either $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\zeta) = \mathbb{Q}(\alpha)$ or $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\zeta) = \mathbb{Q}$. By (a), $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\zeta) = \mathbb{Q}$. Since $\mathbb{Q}(\zeta)/\mathbb{Q}$ Galois, the above Proposition implies $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\zeta)$ are linearly disjoint. Thus the degree of their compositum over $\mathbb{Q}$ is

$$[\mathbb{Q}(\zeta, \alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}][\mathbb{Q}(\zeta) : \mathbb{Q}] = 18.$$

Further, $\mathbb{Q}(\alpha, \zeta)/\mathbb{Q}(\alpha)$ is Galois and the restriction map from $\mathrm{Gal}(\mathbb{Q}(\alpha, \zeta)/\mathbb{Q}(\alpha))$ to $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is an isomorphism. As before, $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is abelian so $\mathbb{Q}(\beta)/\mathbb{Q}(\alpha)$ must be a Galois extension. The polynomial $g = x^3 - \alpha$ has no roots in $\mathbb{Q}(\alpha)$ and, as a degree 3 polynomial, is irreducible over $\mathbb{Q}(\alpha)$. With g the minimal polynomial of β over $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)/\mathbb{Q}(\alpha)$ Galois, g must split in $\mathbb{Q}(\beta)$. Thus the roots $\{\beta\zeta^{3i}\}_{i=0}^{2}$ of g are elements of $\mathbb{Q}(\beta)$. Proceeding,

$$\zeta^3 = \beta^2(\beta\zeta^3) \in \mathbb{Q}(\beta)$$

so $\mathbb{Q}(\zeta^3)$ is a subfield of $\mathbb{Q}(\beta)$. However, $[\mathbb{Q}(\beta) : \mathbb{Q}] = 9$ and $[\mathbb{Q}(\zeta^3) : \mathbb{Q}] = \varphi(3) = 2$ for φ Euler's totient function, a contradiction. Therefore, α does not have a third root in $\mathbb{Q}(\zeta, \alpha)$.



Math 210B Discussion Week 8

Matthew Gherman

February 24, 2022

Theorem (Isomorphism extension)**.** Let $L/K/F$ be a tower of algebraic field extensions. For every automorphism $\sigma : K \to K$, there is an automorphism $\tilde{\sigma} : L \to L$ such that $\tilde{\sigma}|_K = \sigma$.

Spring 2017 Problem 10. Let K/F be a (finite) Galois field extension with $G = \mathrm{Gal}(K/F)$ and let $H \subset G$ be a subgroup. Determine in terms of H and G the group $\mathrm{Gal}(K^H/F)$ of all field automorphisms of K^H over F.

Take an element $\sigma \in G$. We want to show that $\sigma|_{K^H} \in \mathrm{Aut}(K^H/F)$ if and only if $\sigma \in N_G(H)$. ($\Rightarrow$) Assume $\sigma|_{K^H} \in \mathrm{Aut}(K^H/F)$ so $\sigma(K^H) \subset K^H$. Let $h \in H$ and $x \in K^H$. Then

$$(\sigma h \sigma^{-1})(x) = \sigma(h(\sigma^{-1}(x))) = \sigma(\sigma^{-1}(x)) = x$$

since $\sigma^{-1}(x) \in K^H$. We note $\sigma h \sigma^{-1}$ fixes all $x \in K^H$ so $\sigma h \sigma^{-1} \in H$. Thus $\sigma \in N_G(H)$. ($\Leftarrow$) We will prove the contrapositive. Assume $\sigma|_{K^H} \notin \mathrm{Aut}(K^H/F)$. Then there is some $y \in K^H$ for which $\sigma(y) = z \notin K^H$. Thus there is some $h \in H$ such that $h(z) \neq z$ so $\sigma^{-1}(h(\sigma(y))) = \sigma^{-1}(h(z)) \neq y$. As a result, $\sigma(h(\sigma^{-1}(x))) \notin H$ and $\sigma \notin N_G(H)$.

The above result allows us to define the restriction homomorphism $r : N_G(H) \to \mathrm{Aut}(K^H/F)$ by $r(\sigma) = \sigma|_{K^H}$. By the Isomorphism Extension Theorem, r is surjective. It is clear that $H \subset \ker(r)$ since $h \in H$ fixes all elements of K^H. Take $\sigma \in \ker(r)$ so σ fixes each $x \in K^H$. Then the subgroup $I \subset G$ generated by σ satisfies $K^I \supset K^H$. This implies $I \subset H$ and $\sigma \in H$. We conclude that $\ker(f) = H$ and $\mathrm{Aut}(K^H/F) \simeq N_G(H)/H$ by the First Isomorphism Theorem.

Fall 2017 Problem 8. Let F be a field, and let $f, g \in F[x]\backslash\{0\}$ be relatively prime and not both constant. Show that $F(x)$ has finite degree $d = \max(\deg(f), \deg(g))$ over its subfield $F\left(\frac{f}{g}\right)$. (Hint: If the degree were less than d, show that there exists a nonzero polynomial with coefficients in $F[x]$ of degree less than d having $\frac{f}{g}$ as a root.)

Note that $\frac{f}{g}$ is a root of the irreducible polynomial $p = gy - f$ for $p \in (F[x])[y]$. Since f and g are relatively prime, p is primitive. The polynomial $q = \frac{f}{g}g(T) - f(T) \in \left(F\left(\frac{f}{g}\right)\right)[T]$ is degree d and has x as a root. Thus $\left[F(x) : F\left(\frac{f}{g}\right)\right] \leqslant d$ and $F(x)$ is a finite extension of $F\left(\frac{f}{g}\right)$. Let $m = a_k T^k + a_{k-1}T^{k-1} + \cdots + a_0$ be the minimal polynomial of x over $F\left(\frac{f}{g}\right)$. By clearing denominators, we may assume that each $a_i \in F\left[\frac{f}{g}\right]$. Then $m = b_n\left(\frac{f}{g}\right)^n + b_{n-1}\left(\frac{f}{g}\right)^{n-1} + \cdots + b_0$ for $b_i \in F[T]$. Replace the variable T with x in each b_i to obtain $M = b_n y^n + b_{n-1}y^{n-1} \cdots + b_0$ in $(F[x])[y]$ with $\frac{f}{g}$ as a root. Thus p divides M in $(F[x])[y]$. Since p is primitve, g divides b_n and f divides b_0. We have $\deg(b_n) \geqslant \deg(g)$ and $\deg(b_0) \geqslant \deg(f)$ so $\deg(m) \geqslant d$. Therefore, $\left[F(x) : F\left(\frac{f}{g}\right)\right] = d$.

Fall 2015 Problem 4. Let K be a field and let L be the field $K(X)$ of rational functions over K.

(a) Show that there are two unique K-automorphisms f and g of the field $L = K(X)$ such that $f(X) = X^{-1}$ and $g(X) = 1 - X$. Let G be the subgroup of the group of K-automorphisms of L generated by f and g. Show that $|G| > 3$.

We define $f : L \to L$ as $f(k) = k$ for $k \in K$ and $f(X) = X^{-1}$. Then extend f to a K-homomorphism. Similarly, $g : L \to L$ is defined as $g(k) = k$ for $k \in K$ and $g(X) = 1 - X$. Then we extend g to a K-homomorphism. We will now show that f and g are automorphisms of L. Since L is a field, f and g are injective. Take $\frac{p(X)}{q(X)} \in L$

for $p(X), q(X) \in K[X]$. Then $f\left(\frac{p(X^{-1})}{q(X^{-1})}\right) = \frac{f(p(X^{-1}))}{f(q(X^{-1}))} = \frac{p(X)}{q(X)}$. Thus f is a K-automorphism. Similarly, $g\left(\frac{p(1-X)}{q(1-X)}\right) = \frac{p(X)}{q(X)}$ so g is a K-automorphism.

Note that $f \neq g$ via the image of X. Then G contains at least $\{e, f, g\}$ where e is the identity K-automorphism.

$$gf(X) = g(X^{-1}) = \frac{1}{1-X}$$
$$fg(X) = f(1-X) = 1 - X^{-1} = \frac{X-1}{X}$$

If $\frac{1}{1-X} = \frac{X-1}{X}$, then $\frac{X+(1-X)^2}{X(1-X)} = 0$ and X would be algebraic over K, a contradiction. Thus $gf \neq fg$ as K-automorphisms. A similar argument shows that both gf and fg are distinct from e, f, and g. Thus G contains at least $\{e, f, g, fg, gf\}$ and $|G| > 3$.

It will be important later to show that $|G| \geqslant 6$.

$$fgf(X) = f\left(\frac{1}{1-X}\right) = \frac{1}{1-X^{-1}} = \frac{X}{X-1}$$

A similar argument to above shows that fgf is distinct from e, f, g, fg, and gf. Thus $|G| \geqslant 6$.

(b) Let $E = L^G$. Show that $P = \frac{(X^2-X+1)^3}{X^2(X-1)^2} \in E$.

We want to show that P is fixed under f and g action.

$$f(P) = \frac{f((X^2-X+1)^3)}{f(X^2(X-1)^2)} = \frac{(X^{-2}-X^{-1}+1)^3}{X^{-2}(X^{-1}-1)^2} = \frac{(\frac{1-X+X^2}{X^2})^3}{\frac{(1-X)^2}{X^2X^2}} = \frac{(1-X+X^2)^3}{X^2(1-X)^2} = P$$
$$g(P) = \frac{g((X^2-X+1)^3)}{g(X^2(X-1)^2)} = \frac{((1-X)^2-(1-X)+1)^3}{(1-X)^2(-X)^2} = \frac{(X^2-X+1)^3}{X^2(X-1)^2} = P$$

Thus $P \in L^G$.

(c) Show that $L/K(P)$ is a finite extension of degree 6.

We construct a polynomial with coefficients in $K(P)$ for which X is a root. Define

$$p(T) := (T^2-T+1)^3 - P(T^2(T-1)^2)$$

for $p(T) \in K(P)[T]$ so $p(X) = 0$. Since p is degree 6, $[L : K(P)] \leqslant 6$. Note that $P \in L^G$ by (b) so $K(P) \subset L^G \subset L$. By the final argument of (a), we have $6 \leqslant [L : L^G] \leqslant [L : K(P)] \leqslant 6$. Therefore, $L/K(P)$ is a finite extension of degree 6.

(d) Deduce that $E = K(P)$ and that G is isomorphic to the symmetric group S_3.

The chain of inequalities in (c) implies $[L : L^G] = 6$. By Galois correspondence, L/L^G is a Galois extension with Galois group $\mathrm{Gal}(L/L^G) \simeq G$. The finite Galois extension satisfies $|G| = [L : L^G] = 6$. By (a), it is clear that G is not abelian. The only non-abelian group of order 6 is S_3.

Fall 2018 Problem 4. Let K be a subfield of the real numbers and f an irreducible degree 4 polynomial over K. Suppose that f has exactly two real roots. Show that the Galois group of f is either S_4 or of order 8.

Note that $\mathrm{char}(K) = 0$ so each finite field extension is separable. Let $r, s \in \mathbb{R}$ be the two distinct real roots of f. Let $\alpha \in \mathbb{C}$ be a complex root of f so $\overline{\alpha}$ is the final root of f. Since f is irreducible, $[K[r] : K] = 4$. Case 1: Assume $s \in K[r]$. Then $f = (x-r)(x-s)h$ for $h \in (F[r])[x]$ and $\deg(h) = 2$. Note that $K[r] \subset \mathbb{R}$ but $\alpha \notin \mathbb{R}$. Thus the quadratic h is irreducible over $K[r]$. We conclude $[K[r, \alpha] : K] = [K[r, \alpha] : K[r]][K[r] : K] = 8$ where $K[r, \alpha]$ is the splitting field of f over K. Then $K[r, \alpha]/K$ is Galois and $|\mathrm{Gal}(f)| = 8$.

Case 2: Assume $s \notin K[r]$. Then $f = (x-r)g$ with $g \in (K[r])[x]$ and $\deg(g) = 3$. Since $K[r] \subset \mathbb{R}$ and $s \notin K[r]$, the cubic g is irreducible over $K[r]$. Then $[K[r, s] : K] = 12$ and $f = (x-r)(x-s)h$ for $h \in (K[r, s])[x]$ with $\deg(h) = 2$. Since $K[r, s] \subset \mathbb{R}$, the quadratic h will be irreducible over $K[r, s]$. We have $K[r, s, \alpha]$ is the splitting field of f over K so $K[r, s, \alpha]/K$ is Galois. Additionally, $[K[r, s, \alpha] : K] = |\mathrm{Gal}(K[r, s, \alpha]/K)| = 24$. The Galois group defines a group action on the set of four roots of f. Therefore, we have an injective group homomorphism $\phi : \mathrm{Gal}(K[r, s, \alpha]/K) \to S_4$. By an order argument, ϕ is surjective and $\mathrm{Gal}(K[r, s, \alpha]/K) \simeq S_4$.

Spring 2019 Problem 5. Let Φ_n denote the nth cyclotomic polynomial in $\mathbb{Z}[X]$ and let a be a positive integer and p a (positive) prime not dividing n. Prove that if $p|\Phi_n(a)$ in $\mathbb{Z}$, then $p \equiv 1 \bmod n$.

We have $\Phi_n(a)$ divides $a^n - 1$ so p divides $a^n - 1$. With $\gcd(a, a^n - 1) = 1$, we conclude that p does not divide a. In particular, the equivalence class of a is a unit in $(\mathbb{Z}/p\mathbb{Z})^\times$. Since $a^n \equiv 1 \pmod{p}$, we know that the order of a in $(\mathbb{Z}/p\mathbb{Z})^\times$ divides n. If the order of a is n, then n divides $|(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$ as desired.

Assume now that the order of a is strictly less than n. Then p divides $a^k - 1$, and there is some divisor d of k for which p divides $\Phi_d(a)$. Since $\Phi_d(a)\Phi_n(a)$ divides $x^n - 1$, a is a double root of $x^n - 1$. However, the polynomial $x^n - 1$ has formal derivative nx^{n-1}. Since p does not divide n, we conclude that $x^n - 1$ is separable over $\mathbb{F}_p$, a contradiction.

Math 210B Discussion Week 9

Matthew Gherman

March 3, 2022

Definition 1. A left R-module M is *simple* if $M \neq 0$ and M has no non-trivial submodules. M is simple if and only if $M \simeq R/I$ as R-modules for some maximal left ideal I.

Lemma (Schur)**.** Let $f : M \to N$ be an R-module homomorphism of simple R-modules. Then $f = 0$ or f is an isomorphism. As a corollary, if M is a simple R-module, then $\mathrm{End}_R(M)$ is a division ring.

Definition 2. A left R-module M is *semisimple* if there is a family of simple submodules M_i such that

$$M = \oplus_i M_i.$$

A semisimple ring R is semisimple as a left R-module. Equivalently, R will be semisimple as a right R-module.

Remark 1. A simple ring is not necessarily semisimple. Simple rings are those without two-sided ideals while semisimplicity is a module concept.

Theorem. Let R be a ring. The following are equivalent:

(a) R is semisimple;

(b) every left R-module is semisimple;

(c) every left R-module is projective;

(d) every left R-module is injective;

(e) every short exact sequence of left R-modules is split.

Theorem (Artin-Wedderburn)**.** A ring R is semisimple if and only if

$$R \simeq M_1(D_1) \times \cdots \times M_k(D_k)$$

for some division rings $D_1, \ldots, D_k$.

Definition 3. The *Jacobson radical* $J(R)$ of a ring is the two-sided ideal that is the intersection of all left maximal ideals of R. An element $x \in R$ is in $J(R)$ if and only if $1 - axb$ is in $R^\times$ for all $a, b \in R$. Equivalently, the Jacobson radical is the set of elements $r \in R$ such that $rM = 0$ for M a simple left R-module.

Theorem. A ring R is semisimple if and only if R is Artinian and $J(R) = 0$.

Theorem. A ring is simple and Artinian if and only if $R = M_n(D)$ for some division ring D.

Fall 2014 Problem 5. Let R be a commutative algebra over $\mathbb{Q}$ of finite dimension n. Let $\rho : R \to M_n(\mathbb{Q})$ be the regular representation, and define $\mathrm{Tr} : R \to \mathbb{Q}$ by the matrix trace of ρ. If the pairing $(x, y) = \mathrm{Tr}(xy)$ is non-degenerate on R, prove that R is semi-simple.

We will show that a non-degenerate trace implies that R has no non-trivial nilpotent elements. Let $r \in R$ be nilpotent with $r^k = 0$. Then $\rho(r)$ is a matrix such that $\rho(r^k) = \rho(r)^k = 0$. Then the minimal polynomial of $\rho(r)$ has the form X^m for some m. We conclude that $\mathrm{Tr}(r) = 0$ since $\mathrm{Tr}(r)$ appears as a non-leading coefficient in the minimal polynomial. In particular, rx is nilpotent for all $x \in R$ since R is commutative. Thus $\mathrm{Tr}(rx) = 0$ for all $x \in R$. If (x, y) is non-degenerate, then R has no non-trivial nilpotent elements. In other words, the nilradical of R is trivial.

Every ideal of R is closed under multiplication by R, which means each ideal is a $\mathbb{Q}$-subspace of a finite-dimensional vector space. Thus R is Artinian by a dimension argument for a descending chain of ideals. In an Artinian commutative ring, each prime is maximal so the Jacobson radical and nilradical are equal. Since the nilradical is trivial, the Jacobson radical of A is trivial. We now prove that an Artinian ring with trivial Jacobson radical is semi-simple. A Artinian implies there are finitely many maximal ideal $\{\mathfrak{m}_i\}$ for $1 \leqslant i \leqslant \ell$. Thus $\cap_{i=1}^{\ell} \mathfrak{m}_i = 0$. By the Chinese Remainder Theorem,

$$A \simeq A/\cap_{i=1}^{\ell} \mathfrak{m}_i \simeq \oplus_{i=1}^{\ell} A/\mathfrak{m}_i.$$

Each $A/\mathfrak{m}_i$ is a simple R-module so R is a semi-simple R-module. This shows R is a semi-simple ring.

Fall 2017 Problem 3. Let k be a field and A a finite-dimensional k-algebra. Denote by $J(A)$ the Jacobson radical of A. Let $t : A \to k$ be a morphism of k-vector spaces such that $t(ab) = t(ba)$ for all $a, b \in A$. Assume $\ker(t)$ contains no non-zero left ideal. Let M be the set of elements a in A such that $t(xa) = 0$ for all $x \in J(A)$. Show that M is the largest semi-simple left A-submodule of A.

We want to show that M is the sum of all of the simple modules of A. Let N be a simple left A-module. Then $J(A)N = 0$ by the definition of the Jacobson radical as the annihilator of all simple left A-modules. Since $t(xn) = 0$ for $n \in N$ and all $x \in J(A)$, we have $N \subset M$. Thus M contains the sum of all the simple left A-submodules of A.

Take a descending chain of left ideals of A. Each left ideal is a finite-dimensional k-vector space. Thus the chain must terminate, and A is left Artinian as a left A-module. The same argument works for right ideals so A is Artinian as a ring. Consequently, $A/J(A)$ is an Artinian ring. Since $J(A)$ is a two-sided ideal of A, we have $J(A)M$ is a left ideal contained in $\ker(t)$. We assume $\ker(t)$ contains no non-zero left ideal so $J(A)M = 0$. Thus M has the structure of a left $A/J(A)$-module. Now $A/J(A)$ is Artinian and has trivial Jacobson radical so $A/J(A)$ is a semisimple ring. We conclude that M is a semisimple left $A/J(A)$-module. In other words, M is the direct sum of simple left $A/J(A)$-modules. These simple $A/J(A)$-modules are simple as A-modules so M is a semisimple left A-module. Since M contains the sum of all simple left A-modules, M is the largest semisimple left A-submodule of A.

Fall 2018 Problem 12. Let F be a finite field and $K \subset \overline{F}$ the subfield of an algebraic closure generated by all roots of unity. Find all simple finite dimensional K-algebras.

Let L/F be an algebraic extension. Then for each $\alpha \in L$, we have a finite extension $F[\alpha]/F$. Then $F[\alpha]$ is the finite field of order q for q some power of a prime. Since $(F[\alpha])^{\times}$ is cyclic of order $q-1$, $K[\alpha]$ is a subfield of K for each $\alpha \in L$ so L is a subfield of K. We conclude that K is the algebraic closure of F.

By Artin-Wedderburn, a simple finite dimensional K-algebra A is a matrix algebras with coefficients in a division ring D over K. However, if $\dim_K(D)$ is finite, we must have $D \subset K$ by K algebraically closed. Thus $A \simeq M_n(K)$ for some integer $n \geqslant 1$.

Spring 2019 Problem 7. Let F be a field and let R be the ring of 3×3 matrices over F with (3,1) and (3,2) entry equal to 0. Thus,

$$R = \begin{pmatrix} F & F & F \\ F & F & F \\ 0 & 0 & F \end{pmatrix}.$$

(a) Determine the Jacobson radical J of R.

Left multiplication by elements of R can perform the row operations: multiplication of a row by a constant, switching rows 1 and 2, and adding a multiple of any row to rows 1 or 2. The elementary matrices except $i = 1, 2$, $j = 3$ do not satisfy $(I - rE_{ij}) \in R^{\times}$ for all $r \in R$. The elementary matrices E_{13} and E_{23} do satisfy $(I - rE_{ij}) \in R^{\times}$ for all $r \in R$ and, thus, generate the Jacobson radical J.

(b) Is J a minimal left (respectively right) minimal ideal?

J is a minimal left ideal since the possible row operations can produce any matrix in J from a non-zero entry in the 13 or 23 position. J is similarly a minimal right ideal by looking instead at column operations.

Fall 2019 Problem 4. Find all isomorphism classes of simple (i.e., irreducible) left modules over the ring $M_n(\mathbb{Z})$ of n by n matrices with $\mathbb{Z}$-entries with $n \geqslant 1$.

Every simple module is $M_n(\mathbb{Z})/I$ for a left maximal ideal I of $M_n(\mathbb{Z})$. Left ideals in $M_n(\mathbb{Z})$ are closed under row operations. The Euclidean algorithm in $\mathbb{Z}$ allows us to reduce each column to elements that are multiples of the greatest common divisor. The maximal ideals of $\mathbb{Z}$ are (p) for $p \in \mathbb{Z}$ prime. Thus the left maximal ideals of $M_n(\mathbb{Z})$ should be matrices with any integers in the entries of two columns and the third column entries are multiples of p for a prime $p \in \mathbb{Z}$.

Fall 2020 Problem 3. A ring R (commutative or non-commutative) is called a domain if $ab = 0$ in R implies $a = 0$ or $b = 0$. Suppose that R is a domain such that $M_n(R)$, the ring of $n \times n$ matrices over R, is a semisimple ring. Prove that R is a division ring.

Prove that $M_n(R)$ is right Artinian implies R is right Artinian. (In fact, it is true that $M_n(R)$ is right Artinian if and only if R is right Artinian.) Then R is an Artinian domain and, thus, a division ring by looking at the multiplication by r on the left module map.

Take a descending chain of left ideals I_k in R. Then the corresponding descending chain of left ideals in $M_n(R)$ terminates in finitely many steps. Then the scalar matrix for $r \in I_{m+1}$ can be written as an $M_n(R)$-linear combination of elements of I_m. By looking at the diagonal entries of the linear combination, the element $r \in I_{m+1}$ can be written as an R-linear combination of elements of I_m.

Math 210B Discussion Week 10

Matthew Gherman

March 10, 2022

Definition 1. Let F be a field. An *F-algebra* A is a ring that has the structure of an F-vector space. A *central* F-algebra A is one for which $Z(A) = F$. A *simple* F-algebra A is one that does not have non-trivial two-sided ideals. By Artin Wedderburn, a simple F-algebra is isomorphic to $M_n(D)$ for D a division F-algebra.

Proposition. Let A and B be two simple F-algebras. If A is central, then $A \otimes_F B$ is simple F-algebra. As a result, if A and B are central simple F-algebras, then $A \otimes_F B$ is a central simple F-algebra.

Theorem (Noether-Skolem)**.** Let A be a finite-dimensional central simple algebra over F and let $S, T \subset A$ be simple subalgebras. Let $f : S \to T$ be an F-algebra isomorphism. Then there exists $a \in A^\times$ such that $f(s) = asa^{-1}$ for all $s \in S$.

Definition 2. The *centralizer* of a subalgebra $S \subset A$ is

$$C_A(S) = \{a \in A : as = sa \text{ for all } s \in S\}.$$

Theorem (Double centralizer)**.** Let A be a central simple algebra over F and let $S \subset A$ be a simple subalgebra.

(a) $C_A(S)$ is simple with $Z(C_A(S)) = S \cap C_A(S) = Z(S)$,

(b) $(\dim(S))(\dim(C_A(S))) = \dim(A)$,

(c) $C_A(C_A(S)) = S$.

Corollary. Let S be a central simple subalgebra of a central simple algebra A. Then $A = S \otimes_F C_A(S)$.

Proposition. If A is a central simple algebra over F, then $\dim_F A = n^2$ for some n.

Fall 2014 Problem 4. Let D be a 9-dimensional central division algebra over $\mathbb{Q}$ and $K \subset D$ be a field extension of $\mathbb{Q}$ of degree greater than 1. Show that $K \otimes_{\mathbb{Q}} K$ is not a field and deduce that $D \otimes_{\mathbb{Q}} K$ is no longer a division algebra.

Note K is a finite extension of $\mathbb{Q}$ and $\mathbb{Q}$ is perfect. By the Primitive Element Theorem, $K \simeq \mathbb{Q}[x]/(f)$ for some irreducible polynomial $f \in \mathbb{Q}[x]$. Since f is no longer irreducible in K, (f) is neither a maximal nor a prime ideal of $K[x]$. We conclude $K \otimes_{\mathbb{Q}} K \simeq K[x]/(f)$ is not a field and, further, not a domain. Alternatively, we can factor $f = (x-\alpha)(x-\beta)$ for $\alpha, \beta \in K$, and $K \otimes_{\mathbb{Q}} K \simeq K[x]/(f) \simeq K[x]/(x-\alpha) \times K[x]/(x-\beta)$ by the Chinese Remainder Theorem. (Note that the extension is separable so α and β are distinct.) Therefore, $K \otimes_{\mathbb{Q}} K$ is not even a domain.

Now $K \otimes_{\mathbb{Q}} K$ is a commutative subring of $D \otimes_{\mathbb{Q}} K$ that is not a domain. We conclude that $D \otimes_{\mathbb{Q}} K$ cannot be a division algebra.

Spring 2018 Problem 4. Let p be a prime number, and let D be a central simple division algebra of dimension p^2 over a field k. Pick $\alpha \in D$ not in the center and write K for the subfield of D generated by α. Prove that $D \otimes_k K \simeq M_p(K)$ (the $p \times p$ matrix algebra with entries in K).

Note that $Z(D \otimes_k K) = Z(D) \otimes_k Z(K) = k \otimes_k K = K$. The tensor product of a central simple algebra and a simple algebra is simple. Therefore, $D \otimes_k K$ is a central simple K-algebra. By Artin-Wedderburn, $D \otimes_k K$ is the product of matrix algebras over division rings. However, $\dim_K(D \otimes_k K) = \dim_k(D) = p^2$ so either $D \otimes_k K$ is a division algebra or $D \otimes_k K \simeq M_p(K)$. Now $K \otimes_k K$ is a subring of $D \otimes_k K$. We will show next that $K \otimes_k K$ has zero divisors so $D \otimes_k K$ is not a division ring.

Let $m_\alpha \in k[x]$ be the minimal polynomial of α over k. Then $K \otimes_k K = k[x]/(m_\alpha) \otimes_k K = K[x]/(m_\alpha)$. Since K contains a root of m_α, $m_\alpha = \prod_{i=1}^m g_i$ for some irreducible polynomials $g_i \in K[x]$. Therefore, $K[x]/(m_\alpha) = K[x]/(\prod_{i=1}^m g_i) \simeq \prod_{i=1}^m K[x]/(g_i)$ by the Chinese Remainder Theorem. It is clear that $\prod_{i=1}^m K[x]/(g_i)$ has zero divisors for $m \geqslant 2$.

Spring 2020 Problem 5. If $K \neq \mathbb{Q}$ appears as a subfield (sharing the identity) of some central simple algebra over $\mathbb{Q}$ of $\mathbb{Q}$-dimension 9, determine (isomorphism classes of) the groups appearing as the Galois group of the Galois closure of K over $\mathbb{Q}$.

A central simple algebra A is not a field since $Z(A) = \mathbb{Q}$. Further $K \neq \mathbb{Q}$ so $\dim_{\mathbb{Q}}(K) = 3$. The field $\mathbb{Q}$ is perfect so K is a separable field extension of $\mathbb{Q}$. We can write $K = \mathbb{Q}(\alpha)$ by Primitive Element Theorem with m_α of degree 3. Let L be the normal closure of K over $\mathbb{Q}$. We can embed $\mathrm{Gal}(L/\mathbb{Q})$ in S_3 which implies $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$ or S_3.

The action on K via left multiplication by α is a $\mathbb{Q}$-linear ring homomorphism. Since K is a field, the kernel of the map is trivial. Thus the map is an isomorphism between K and a subfield of $M_3(\mathbb{Q})$. We have shown that any degree 3 field extension K of $\mathbb{Q}$ is a subfield of $M_3(\mathbb{Q})$. The field extension $K = \mathbb{Q}(\xi_7 + \xi_7^{-1})$ is cyclic Galois of degree 3. The polynomial $x^3 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion. Let $K = \mathbb{Q}[x]/(x^3 - 2)$ so $\mathrm{Gal}(L/\mathbb{Q}) \simeq S_3$. Thus $\mathbb{Z}/3\mathbb{Z}$ and S_3 are the possibilities for the Galois group of the normal closure of K over $\mathbb{Q}$.

Spring 2018 Problem 8. Let F be a field that contains the real numbers $\mathbb{R}$ as a subfield. Show that the tensor product $F \otimes_{\mathbb{R}} \mathbb{C}$ is either a field or isomorphic to the product of two copies of F, $F \times F$.

We note that $\mathbb{C} \simeq \mathbb{R}[x]/(x^2+1)$ so $F \otimes_{\mathbb{R}} \mathbb{C} \simeq F \otimes_{\mathbb{R}} \mathbb{R}[x]/(x^2+1) \simeq F[x]/(x^2+1)$. If x^2+1 is irreducible in $F[x]$, then $F[x]/(x^2+1)$ is a field. If x^2+1 has a root in F, then $F[x]/(x^2+1) \simeq F[x]/(x-\alpha) \times F[x]/(x-\beta) \simeq F \times F$ by the Chinese Remainder Theorem. Therefore, $F \otimes_{\mathbb{R}} \mathbb{C}$ is either a field or isomorphic to $F \times F$.

Spring 2020 Problem 4. Compute the dimension of the tensor products of two algebras $\mathbb{Q}[\sqrt{2}] \otimes_{\mathbb{Z}} \mathbb{Q}[\sqrt{2}]$ over $\mathbb{Q}$ and $\mathbb{Q}[\sqrt{2}] \otimes_{\mathbb{Z}} \mathbb{R}$ over $\mathbb{R}$. Is $\mathbb{R} \otimes_{\mathbb{Z}} \mathbb{R}$ finite dimensional over $\mathbb{R}$?

By the Chinese Remainder Theorem,

$$\begin{aligned}
\mathbb{Q}[\sqrt{2}] \otimes_{\mathbb{Z}} \mathbb{Q}[\sqrt{2}] &\simeq (\mathbb{Q}[\sqrt{2}])[x]/(x^2-2) \\
&\simeq (\mathbb{Q}[\sqrt{2}])[x]/(x-\sqrt{2}) \times (\mathbb{Q}[\sqrt{2}])[x]/(x+\sqrt{2}) \\
&\simeq \mathbb{Q}[\sqrt{2}] \times \mathbb{Q}[\sqrt{2}] \\
\mathbb{Q}[\sqrt{2}] \otimes_{\mathbb{Z}} \mathbb{R} &\simeq \mathbb{R}[x]/(x^2-2) \\
&\simeq \mathbb{R}[x]/(x-\sqrt{2}) \times \mathbb{R}[x]/(x+\sqrt{2}) \\
&\simeq \mathbb{R} \times \mathbb{R}.
\end{aligned}$$

Let $\{p_i\}$ be the prime integers in increasing order. We want to show that the field extension $\mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_{k+1}}]$ over $\mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_k}]$ is degree 2. Then $\mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_k}, \ldots]$ is an infinite degree field extension over $\mathbb{Q}$ that is a subalgebra of $\mathbb{R}$. Then $\mathbb{R} \otimes_{\mathbb{Z}} \mathbb{R}$ will be infinite dimensional over $\mathbb{R}$ by applying the above argument to $\mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_k}, \ldots] \otimes_{\mathbb{Z}} \mathbb{R}$.