SPRING 2024: MATH 791 HOMEWORK

The page numbers in each assignment below refer to those in the course textbooks. AAC refers to the text *Algebra: Abstract and Concrete* and AFYGS refers to the text *Algebra for First Year Graduate Students*.

Homework 1. 1. Let G be a group. Prove the following statements:

(i) The identity element in G is unique.
(ii) Each element g has a unique inverse.

2. Write out a group table for S_3, where $S_3 = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ are defined as in class.

3. Let G be a group. Show that G is abelian if and only if $(ab)^2 = a^2b^2$, for all $a, b \in G$.

4. A k-cycle is a permutation $\sigma \in S_n$ of the following type: There exist $i_1, \dots, i_k \in X = \{1, 2, \dots, n\}$, such that $\sigma(i_1) = i_2, \sigma(i_2) = i_3, \dots, \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1$ and $\sigma(j) = j$, for $j \in X \backslash \{i_1, \dots, i_k\}$. Prove that if σ is a k-cycle, then $\sigma^k = e$ and $\sigma^j \neq e$, for all $1 \leq j \leq k-1$. (We are assuming $k > 1$.)

Homework 2. Throughout this homework set, G denotes a group. For any subsets $H, K \subseteq G$, we define HK to be the set $\{hk \mid h \in H, k \in K\}$.

1. Let X be a set and $\sim$ an equivalence relation on X. For $x \in X$, let $[x]$ denote the equivalence class of x. Prove that for any $x, y \in X$, either $[x] = [y]$ or $[x] \cap [y] = \emptyset$. Conclude that the distinct equivalence classes partition X. What can you say if X is finite and for all $x \in X$, $|[x]| = r$?

2. Let $H \subseteq G$ be a subgroup. Prove that the following conditions are equivalent:

(a) H is a **normal** subgroup of G, i.e., $gH = Hg$, for all $g \in G$.
(b) $gHg^{-1} = H$, for all $g \in G$.
(c) $gHg^{-1} \subseteq H$, for all $g \in G$.
(d) $ghg^{-1} \in H$, for all $g \in G$ and $h \in H$.

3. Prove that if H and K are subgroups of G, then HK is a subgroup if and only if $HK = KH$. Conclude that if H is a normal subgroup of G, then HK is a subgroup of G.

4. Fix $n \in \mathbb{Z}$, and set $n\mathbb{Z} := \{rn \mid r \in \mathbb{Z}\}$, i.e., the set of all multiples of n. Prove that:

(a) $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ (under addition).
(b) $0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}$ are the distinct cosets of $n\mathbb{Z}$ in $\mathbb{Z}$.

5. Let $X \subseteq G$ be a subset. Prove that $\langle X \rangle$ is the intersection of all subgroups of G containing X.

Homework 3. 1. Suppose G is a group and H a subgroup. Let X denote the set of distinct left cosets of H in G and Y denote the set of distinct right cosets of H in G. Prove that there is a a 1-1, onto function from X to Y. Here, we do not assume the sets X and Y are finite.

2. Let $K \subseteq H$ be subgroups of G. Prove that $[G : K]$ is finite if and only if $[G : H]$ and $[H : K]$ are finite, in which case, $[G : K] = [G : H] \cdot [H : K]$.

3. Let $G := S_3 = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$, $H := \langle\sigma\rangle$, and $K := \langle\tau\rangle$, with our usual notation. Show that, as subsets of G: $(\tau H) \cdot (\tau H) = H$ and $(\sigma K) \cdot (\sigma K) \neq \sigma^2 K$. Be sure to write final answers in terms of our established notation for S_3.

Homework 4. 1. Let $\phi : G_1 \to G_2$ be a group homomorphism. Show that ϕ is 1-1 if and only if the kernel of ϕ is $\{e_1\}$.

2. Let G be a group. The *center of* G, denoted $Z(G)$, is the set $Z(G) := \{z \in G \mid zg = gz, \text{ for all } g \in G\}$. For example, $K := \{-1, 1\}$ is the center of Q_8. Prove:

(i) $Z(G)$ is a normal subgroup of G.
(ii) If $G/Z(G)$ is cyclic, then G is an abelian group.

(iii) Give an example to show that if $K \subseteq G$ is normal and G/K is cyclic, then G need not be abelian.

3. Let N be a normal subgroup of the group G. Show that if $aN = cN$ and $bN = dN$, for $a, b, c, d \in G$, then $abN = cdN$. This shows that if we define a binary operation * on the set of left cosets by $(aN) * (bN) = abN$, then this operation is well-defined.

4. Let $G = \langle a \rangle$ be a cyclic group. Suppose $H \subseteq G$ is a subgroup. Prove that H is a cyclic group. Hint: consider a^r, where r is the least positive integer such that $a^r \in H$.

5. Let G be a group and $e \neq a \in G$. We say that a has *finite order* if $a^n = e$, for some $n \geq 2$. The *order of* a is the least positive integer r such that $a^r = e$, and we write $o(a) = r$. Prove the following statements:

(i) If a has finite order, then there exists a least positive integer r such that $a^r = e$.
(ii) If $o(a) = r$, then r divides any n satisfying $a^n = e$.
(iii) If $o(a) = r$, then $\langle a \rangle = \{e, a, a^2, \dots, a^{r-1}\}$. In particular, $o(a) = |\langle a \rangle|$.

Homework 5. 1. Let $\phi : G_1 \to G_2$ be a surjective group homomorphism. Prove that if $G_1 = \langle X \rangle$, for X a subset of G_1, then $G_2 = \langle \phi(X) \rangle$.

2. Find all group homomorphisms from $\mathbb{Z}_3$ to itself.

3. An *automorphism* of the group G is a 1-1, onto group homomorphisms from G to itself. Prove that the set $\mathrm{Aut}(G)$ of automorphisms of G forms a group under composition.

4. Fix $g \in G$. Prove that $\phi : G \to G$ defined by $\phi(x) = g^{-1}xg$, for all $x \in G$ is an automorphism of G. Such a map is called an *inner automorphism* of G.

5. Describe the automorphism groups of $\mathbb{Z}_8$ and $\mathbb{Z}_{12}$.

Homework 6. 1. Let H, K be subgroups of the group G such that K is normal in G. Prove that $(HK)/K$ is isomorphic to $H/(H \cap K)$.

2. Show that every element in S_4 can be written as a finite product of elements from the set $\{\sigma, \tau\}$ where $\sigma = (1, 2)$ and $\tau = (1, 2, 3, 4)$.

3. List all subgroups of S_4 having four elements.

4. Suppose $\tau \in S_n$ is a k-cycle and $\gamma \in S_n$ is an s-cycle. Prove that if τ and γ are disjoint, then the order of $\gamma\tau$ is the least common multiple of k and s.

Homework 7. Throughout this assignment S_n denotes the symmetric group acting on $X_n = \{1, 2, \dots, n\}$.

1. Recall that if G is any group and $g \in G$, then multiplication by g gives a 1-1, onto function from G to itself. That is, multiplication by g permutes the elements of G. Now, let $G := \{g_1, g_2, \dots, g_n\}$ be a group of order n. Define $\phi : G \to S_n$ as follows. For $g \in G$, $\phi(g) = \sigma_g$, where $\sigma_g(i) = j$ if and only if $gg_i = g_j$. In other words, σ_g permutes the set X according to the multiplication map $G \xrightarrow{\cdot g} G$. Prove *Cayley's Theorem* by showing that ϕ is an injective group homomorphism. In other words, any finite group is isomorphic to a subgroup of S_n, for some $n \geq 1$.

2. Write out the elements of S_4 having order four in terms of their cycle decomposition. What is the largest order of an element of S_4? What is the largest order of an element in S_5?

3. Let p be a prime. Show that an element in S_n has order p if and only if it can be written as a product of disjoint p-cycles. Give an example to show that this is false if p is not a prime.

4. Elements x and y in a group G are said to be *conjugate*, if there exists $g \in G$ such that $gxg^{-1} = y$. Let $\tau = (i_1, \dots, i_k)$ be a k-cycle in S_n ($k \leq n$).

(i) For $\gamma \in S_n$, show that $\gamma\tau\gamma^{-1} = (\gamma(i_1), \dots, \gamma(i_k))$. In other words, the conjugate of a k-cycle is a k-cycle.
(ii) Let $\sigma \in S_n$ be any k-cycle. Show that σ is a conjugate of τ.

Conclude that the set of all k-cycles equals the set of all conjugates of τ.

Homework 8. 1. Show that $N := \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ is a normal subgroup of A_4. Hint: Use Problem 4 from Homework 7.

2. Suppose $n \geq 3$ and $\sigma \in S_n$. Show there exists $\tau \in S_n$ such that $\sigma\tau \neq \tau\sigma$, i.e., the center of S_n is trivial.

3. Prove the statements below to establish the following fact: For $n \geq 5$, A_n is the only non-trivial normal subgroup of S_n.

(i) Let G be a group and A, B normal subgroups of G. Show that $A \cap B$ is a normal subgroup. Conclude that if A is a simple group, then $A \cap B = \{e\}$.

(ii) Suppose G is a group and $A \subseteq G$ is a normal subgroup of index two. Let $B \subseteq G$ be a normal subgroup. Show that if A is a simple group, then B must have order two. (Hint: For $b_1, b_2 \in B$, consider the cosets b_1A and b_2A.)

(iii) Let G be a group and $B = \{e, b\}$ a normal subgroup of order two. Then $b \in Z(G)$, the center of G.

(iv) Suppose G is a group, and $A \subseteq G$ is a normal subgroup of index two. Show that if A is a simple group and $Z(G) = \{e\}$, then A is the only proper normal subgroup of G.

Conclude that A_n is the only proper normal subgroup of S_n, for $n \geq 5$.

Homework 9. 1. Let Y be a set with n elements and S_Y denote the group of one-to-one onto functions from Y to itself, with composition of functions for the binary operation. Show that S_Y is isomorphic to S_n, where, S_n, as defined in class, is the set of one-to-one onto functions from $X = \{1, 2, \ldots, n\}$ to itself. Thus, when working with S_n are are free to think of S_n as the group of permutations of any particular set with n elements.

2. In class, we showed that if the group G acts on the set X, with $|X| = n$, then there is a group homomorphism $\phi : G \to S_n$. Prove the converse by showing that if $\phi : G \to S_n$ is a group homomorphism, then G acts on any set $X := \{x_1, \ldots, x_n\}$ by showing that the product $g \cdot x_i := x_{\phi(g)(i)}$ gives an action of G on X. Thus, to give an action of a group G on a set with n elements is equivalent to giving a group homomorphism from G to S_n.

3. Let G be a group and suppose $\phi : G \to \mathrm{Gl}_n(\mathbb{R})$ is a group homomorphism. Let X denote $\mathbb{R}^n$, written as column vectors. Show that G acts on X via ϕ. A group homomorphism from G to $\mathrm{Gl}_n(\mathbb{R})$ is called a *group representation.*.

4. Let G act on the set X. For $x, y \in X$, define $x \sim y$ if and only if $y = gx$, for some $g \in G$. Show that $\sim$ is an equivalence relation on X. For $x \in X$, the equivalence class of x is called the *orbit of x*. Thus, the distinct orbits of G acting on X partition X.

Homework 10. 1. Recalling that if G acts on a set X with n elements, there exists a group homomorphism $\phi : G \to S_n$, find an *explicit* group homomorphism from $\mathbb{Z}_2 \times \mathbb{Z}_2 \to S_4$.

2. Let Q_8 act on itself via left multiplication. Use this action to find an explicit group homomorphism from Q_8 to S_8. Now find two elements in S_8 that generate a subgroup isomorphic to Q_8.

3. A group G acts *transitively* on the set X if there is just one orbit under the action. Suppose H is a subgroup of G, X is the set of left cosets of H and G acts via left translation on X. Show that: (a) The action is transitive and (b) $G_H = H$.

4. Find all conjugacy classes in Q_8 and A_4.

5. If G is a group and $[G : Z(G)] = n$, show that $|c(g)| \leq n$, for all $g \in G$.

Homework 11. 1. Let G be a group of order p^2, p a prime. Prove that G is isomorphic to $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.

2. Prove that a group G of order thirty having a subgroup H of index five is not a simple group. (Hint: Let G act on the left cosets of H).

3. Prove that the center of S_n is $\{id\}$, for $n \geq 3$.

4. Let G be a finite group and $x_1, \ldots, x_n \in G$ representatives of the distinct conjugacy classes of G. Show that G is abelian if $x_i x_j = x_j x_i$, for all $1 \leq i \neq j \leq n$.

5. Show that $\langle (1,2), (1,2,\ldots,n) \rangle = S_n$.

Homework 12. Let S be any ring and R denote the ring of 2×2 matrices over S. Prove that $I \subseteq R$ is a two-sided ideal if and only if there exists a two-sided ideal $J \subseteq S$ such that $I = \mathrm{M}_2(J)$.

2. Let R be a ring and $X \subseteq R$ be a subset. Define $\langle X \rangle$, the *two-sided ideal generated by* X to be the intersection of all two-sided ideals of R containing X. First, show that $\langle X \rangle$ is a two-sided ideal of R containing X and then show $\langle X \rangle$ is the set of all finite expressions of the form $r_1 x_1 s_1 + \cdots + r_n x_n s_n$, with each $r_i, s_j \in R$ and $x_i \in X$.

3. Let R and S be rings. Let $R \times S$ denote $\{(r, s) \mid r \in R \text{ and } s \in S\}$.

(i) Show that $R \times S$ is a ring under coordinate-wise addition and multiplication.
(ii) Show that $K \subseteq R \times S$ is a two-sided ideal if and only if $K = I \times J$, for I a two-sided ideal in R and J a two-sided ideal in S.

4. Let R be a commutative ring. An element $e \in R$ is called an *idempotent* if $e^2 = e$. We say that e is a *non-trivial idempotent* if $e \neq 0, 1$.

(i) Suppose that $e \in R$ is a non-trivial idempotent. Show that $1 - e$ is also a non-trivial idempotent and $e \cdot (1 - e) = 0$.
(ii) Show that Re is both an ideal and a ring. Similarly for $R(1 - e)$.
(iii) Show that $Re \cap R(1 - e) = 0$.
(iv) Show that R is isomorphic to $Re \times R(1 - e)$ as rings.

Homework 13. 1. Let R be a ring and $I \subseteq R$ a two-sided ideal. Give complete proofs showing that there is a one-to-one correspondence between the right (respectively, left, respectively two-sided) ideals of R containing I and right (respectively, left, respectively two-sided) ideals of R/I. Conclude that every right (respectively, left, respectively two-sided) ideal of R/I is of the form J/I for some right (respectively, left, respectively two-sided) ideal of R containing I.

2. Suppose $J \subseteq I$ are two-sided ideals in the ring R. Prove that $(R/J)/(I/J)$ and R/I are isomorphic as rings.

3. Suppose I, J are two-sided ideals in the ring R. Show that $I \cap J$ and $I + J := \{i + j \mid i \in I \text{ and } j \in J\}$ are two-sided ideals, and that there is an injective ring homomorphism $\phi : R/(I \cap J) \to R/I \times R/J$. Suppose R is commutative. Can you think of a sufficient condition on I and J that guarantees that ϕ is surjective? (Hint: If you know it, consider a ring version of the Chinese Remainder Theorem.)

4. Let R be a ring and I, J, K be two-sided ideals. Define $IJ := \langle X \rangle$, where $X := \{ij \mid i \in I \text{ and } j \in J\}$.

(i) Show that IJ is a two-sided ideal.
(ii) Show that $I \cdot (J + K) = IJ + IK$.
(iii) Show that if, in addition, R is commutative, $I + J = R$ implies $I \cap J = IJ$.

Homework 14. 1. Let F be a field. Give a complete proof of the fact that every monic polynomial with coefficients in F can be factored uniquely as a product of monic, irreducible polynomials with coefficients in F. Hint: Just follow the steps used to prove the Fundamental Theorem of Arithmetic.

2. Prove that repeated applications of the division algorithm can be used to find the GCD of $a, b \in \mathbb{Z}$, and that backwards substitution with the system of equations generated by this process gives $m, n \in \mathbb{Z}$ such that $\mathrm{GCD}(a, b) = ma + nb$. This process is called the *Euclidean algorithm*.

3. Use the Euclidean algorithm to find GCD(120, 54) and write the GCD as an integer combination of 120 and 54 as in Bezout's Principle.

Homework 15. In this assignment, you will verify that the ring $R = \mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ does not have the unique factorization property. The *norm* from R is $\mathbb{Z}$ is defined as follows: For $x = a + b\sqrt{-5}$, $N(x) := a^2 + 5b^2$.

1. Show that $N(xy) = N(x)N(y)$, for all $x, y \in R$.

2. Use the norm to describe the units in R.

3. Show that $3, 2 + \sqrt{-5}, 2 + \sqrt{-5}$ are irreducible elements in R.

4. Use the equation $3 \cdot 3 = (2+\sqrt{-5}) \cdot (2-\sqrt{-5})$ to show that $3, 2+\sqrt{-5}, 2-\sqrt{-5}$ are not prime in R. Conclude that R does not have the unique factorization property.

5. Show that the ideal of R generated by 3 and $2+\sqrt{-5}$ is not a principal ideal, i.e., there does not exist $f \in R$ such that $\langle 3, 2+\sqrt{-5}\rangle = \langle f\rangle$.

Homework 16. Throughout this assignment, R is an integral domain. The first three problems show that we can construct a field containing R in the exact manner that the rational numbers are constructed from the integers. Recall, that formally speaking, the rational numbers are the set of equivalence classes of ordered pairs (a, b) of integers (with $b \neq 0$) such that (a, b) is equivalent to (c, d) if and only if $ad = bc$. Of course, we denote the equivalence class of an ordered pair (a, b) as a/b.

1. Let Q denote the set of ordered pairs (a, b) with $a, b \in R$ and $b \neq 0$. For $(a, b), (c, d) \in Q$, define $(a, b) \sim (c, d)$ if and only if $ad = bd$ in R. Show that $\sim$ is an equivalence relation.

2. Let K denote the set of equivalence classes under the equivalence relation in 1. Temporarily using $[(a, b)]$ to denote the equivalence class of (a, b), define addition and multiplication of elements in K as follows:

$$[(a, b)] + [(c, d)] := [(ad + bc, bd)] \quad \text{and} \quad [(a, b)] \cdot [(c, d)] = [(ac, bd)].$$

Show that addition and multiplication in K are well defined.

3. Show that K is a field under the operations above and that the set of elements in K of the form $[(a, 1)]$ is a subring of K isomorphic to R. The field K is called the *quotient field* of R or *fraction field* of R.

Remark. Henceforth we will write the elements of K as a/b, rather and $[(a, b)]$ and an element $a \in R$ either as a or $a/1$ and regard R as a subring of K. Note then that $a/b + c/d = (ad + bc)/bd$ and $a/b \cdot c/d = ac/bd$, as expected.

4. Let L be a field containing R. Show that L contains K (or at least an isomorphic copy of K). Thus, in this sense, K is the smallest field containing R.

5. Let A be an $m \times n$ matrix with entries in R satisfying $m < n$. Set $\mathbf{x} := \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$, and $\mathbf{0} := \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$. Use standard facts from linear algebra to show that the homogeneous system of equations $A \cdot \mathbf{x} = \mathbf{0}$ has infinitely many solutions over R (assuming R is infinite).

Homework 17. Let R be an integral domain. In what follows, $a, b, c, d, e, f \in R$ will be non-zero, non-unit elements. Given $a, b \in R$, $d \in R$ is said to be a *greatest common divisor*, or GCD, of a and b if the following conditions hold:

(i) $d \mid a$ and $d \mid b$
(ii) Whenever $e \mid a$ and $e \mid b$, then $e \mid d$.

Use this definition to prove the following problems.

1. Show that if GCDs exist, they are unique up to a unit multiple.

2. Suppose d_1 is a GCD of ab and ac, and d_2 is a GCD of b and c. Prove that, d_1 is a unit multiple of ad_2. Use this to show that if d is a GCD of a and b, then 1 is a GCD of $\frac{a}{d}$ and $\frac{b}{d}$.

3. Show that if 1 is a GCD of a and b and 1 is also a GCD of a and c, then 1 is a GCD of a and bc.

4. Show that if R is a PID, and $a, b \in R$, then d is a GCD of a and b if and only if $\langle a, b\rangle = \langle d\rangle$. In particular, every two non-zero, non-units have a GCD, and if d is a GCD of a and b, then $d = ra + sb$, for some $r, s \in R$.

5. Let $R = \mathbb{Q}[x, y]$ be the polynomial ring in two variables over $\mathbb{Q}$. Show that 1 is a GCD of x and y, but there is no equation of the form $1 = f \cdot x + g \cdot y$, for $f, g \in R$.

Homework 18. The problems in this homework set deal with a special kind of PID. Let R be a principal ideal domain with the property that, given any two prime elements, π_1 and π_2, $\langle \pi_1\rangle = \langle \pi_2\rangle$, i.e., up to unit multiple, there is just one prime element, say $\pi \in R$. Such a ring is is called a *discrete valuation ring*, denoted DVR, and $\pi \in R$ is called a *uniformizing parameter*.

1. Fix a prime $p \in \mathbb{Z}$. Let R denote the set of rational numbers whose denominator is not divisible by p. First show that R is a subring of $\mathbb{Q}$, and then show that R is a DVR with uniformizing parameter p.

2. Let R be a DVR with uniformizing parameter $\pi \in R$. Show that $\bigcap_{n\geq 1}\langle \pi^n \rangle = 0$.

3. Let R be a DVR with uniformizing parameter $\pi \in R$. Show that every element in R can be written uniquely as $u\pi^n$, for some $n \geq 0$ and $u \in R$ a unit. Conclude that if K denotes the quotient field of R, then every element in K can be written uniquely in the form $u\pi^n$, for some $n \in \mathbb{Z}$ and $u \in R$, a unit.

4. Let R be a DVR with uniformizing parameter $\pi \in R$, and quotient field K. Define $v : K \to \mathbb{Z} \cup \{\infty\}$ by $v(0) = \infty$ and for $\alpha \neq 0$, $v(\alpha) = n$, where $\alpha \in K$ and $\alpha = u\pi^n$, as in 3. Show that for all $\alpha, \beta \in K$:

(i) $v(\alpha + \beta) \geq \min\{v(\alpha), v(\beta)\}$
(ii) $v(\alpha\beta) = v(\alpha) + v(\beta)$.

Observe that $R = \{\alpha \in K \mid v(\alpha) \geq 0\}$.

5. Let K be a field. Suppose $v : K \to \mathbb{Z} \cup \{\infty\}$ is a function such that for all $\alpha, \beta \in K$:

(i) $v(\alpha) = \infty$ if and only if $\alpha = 0$
(ii) $v(\alpha + \beta) \geq \min\{v(\alpha), v(\beta)\}$
(iii) $v(\alpha\beta) = v(\alpha) + v(\beta)$.

Such a function is called a *discrete valuation* on K. We assume that v takes values other than 0 and ∞. Set $R := \{\alpha \in K \mid v(\alpha) \geq 0\}$. Prove that R is DVR by following the steps below.

(i) Show that $u \in R$ is a unit if and only if $v(u) = 0$. Hint: First show $v(1) = 0$.
(ii) Show there exist elements $r \in R$, with $v(r) > 0$.
(iii) Prove that if $r \in R$, and $v(r) > 0$, then as an element of K, $v(\frac{1}{r}) = -v(r)$.
(iv) Suppose $c := \min\{v(r) \mid r \in R \text{ and } v(r) > 0\}$. Show that the image of v is $c\mathbb{Z}$.
(v) Show that if $\pi \in R$ and $v(\pi) = c$, then R is a DVR with uniformizing parameter π.

Homework 19. Throughout this assignment R denotes a commutative ring.

1. Let $I \subseteq R$ be an ideal, and $R[x]$ denote the polynomial ring in x over R. Let $I[x]$ denote the set of polynomials in R with coefficients in I and let $\langle I \rangle$ denote the ideal of $R[x]$ generated by the set I. Show that $I[x] = \langle I \rangle$.

2. Maintaining the notation from 1, show that the rings $R[x]/I[x]$ and $(R/I)[x]$ are isomorphic.

3. Let $R[[x]]$ denote the formal power series ring over R, i.e., the set of expressions of the form $\Sigma_{i=0}^{\infty} a_i x^i$, with $a_i \in R$. Note this is purely an algebraic expression and does not involve any notion of convergence. We add and multiply elements of $R[[x]]$ in the expected way: If $f = \Sigma_{i=0}^{\infty} a_i x^i$ and $g = \Sigma_{i=0}^{\infty} b_i x^i$, then: $f + g = \Sigma_{i=0}^{\infty}(a_i + b_i)x^i$ and $fg = \Sigma_{k=0}^{\infty} c_k x^k$, where $c_k = \Sigma_{i+j=k} a_i b_j$. For $I \subseteq R$ let $I[[x]]$ denote the elements in $R[[x]]$, all of whose coefficients belong to I.

(i) Verify that $R[[x]]$ is a ring and $I[[x]]$ is an ideal of $R[[x]]$ and $R[[x]]/I[[x]] \cong (R/I)[[x]]$.
(ii) Show that if I is finitely generated, then $\langle I \rangle = I[[x]]$ as ideals of $R[[x]]$.
(iii) Can you give an example where $I[[x]] \neq \langle I \rangle$?

Here is Eisenstein's Criterion, which is an important test for irreducibility of polynomials over a UFD.

Eisenstein's Criterion. Let R be a UFD with quotient field K. Suppose $f(x) = a_n x^n + \cdots + a_0 \in R[x]$ is a primitive polynomial. Let $p \in R$ be a prime element and suppose: (i) $p \mid a_i$, for all $0 \leq i < n$, (ii) $p \nmid a_n$, and (iii) $p^2 \nmid a_0$. Then $f(x)$ is irreducible over K (equivalently, over R). For example, $x^6 + 10x^2 + 5x + 15$ is irreducible over $\mathbb{Q}$, by using Eisenstein's criterion and $p = 5$.

4. Let $p \in \mathbb{Z}$ be prime and $f_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 \in \mathbb{Z}[x]$. Use Eisenstein's criterion, together with the following fact to show that $f_p(x)$ is irreducible over $\mathbb{Q}[x]$: $f_p(x)$ is irreducible over $\mathbb{Q}$ if and only if $f_p(x + 1)$ is irreducible over $\mathbb{Q}$.

5. Use Eisenstein's criterion and the fact that $\mathbb{Q}[x]$ is a UFD to show that $x^2 + y^2 - 9$ is irreducible in $\mathbb{Q}[x, y]$.

Homework 20. Throughout this assignment, R is a commutative ring.

1. An ideal $P \neq R$ is said to be a *prime ideal* if for $a, b \in R$, whenever $ab \in P$, then $a \in P$ or $b \in P$. Prove that P is a prime ideal if and only if R/P is an integral domain.

2. An ideal $M \neq R$ is a *maximal ideal* if whenever $J \subseteq R$ is an ideal satisfying $M \subseteq J \subseteq R$, then $J = M$ or $J = R$. In other words, M is maximal among the proper ideals of R. It follows from Zorn's Lemma, that if $I \subsetneq R$ is an ideal, then there exists a maximal ideal $M \subseteq R$ with $I \subseteq M$. In particular, every commutative ring has at least one maximal ideal. Prove that M is a maximal ideal if and only if R/M is a field. Conclude that every maximal ideal is a prime ideal, and give an example of a prime ideal that is not a maximal ideal.

3. Let R be a commutative ring. Ideals $I, J \subseteq R$ are said to be *comaximal* if $I + J = R$. Prove that I and J are comaximal if and only if there is no maximal ideal M containing both I and J.

4. Suppose I, J are comaximal ideals in the commutative ring R. Show that $I \cap J = IJ$.

5. For I and J as in 4, prove that that the natural map $\phi : R \to (R/I) \times (R/J)$ given by $\phi(r) = (r + I, r + J)$ is a surjective ring homomorphism whose kernel equals $I \cap J$. Conclude that $R/IJ \cong (R/I) \times (R/J)$. When $R = \mathbb{Z}$, this isomorphism is one version of the *Chinese remainder theorem.*

Homework 21. Suppose $F \subseteq K$ are fields. We will write $[K : F]$ to denote the dimension of K as a vector space over F.

1. Prove that $1, \sqrt[3]{2}, \sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2})$ are linearly independent over $\mathbb{Q}$. Thus, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

2. Find the multiplicative inverse of $1 + 2\sqrt[3]{2}$ in $\mathbb{Q}(\sqrt[3]{2})$.

3. Can you write down the multiplicative inverse of $1 + \sqrt[3]{2} + \sqrt[3]{4}$ in $\mathbb{Q}(\sqrt[3]{2})$ without doing any calculations?

4. Let $F := \mathbb{Q}(\sqrt{2})$. Define $K := F(\sqrt{3})$ to be the set $\{a + b\sqrt{3} \mid a, b \in F\}$. Show that $[K : F] = 2$. Can you guess $[K : \mathbb{Q}]$? If so, give a proof validating your guess.

5. Let $p(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$.
   (i) Show that $p(x)$ is irreducible over $\mathbb{Z}_2$.
   (ii) Show that the commutative ring $\mathbb{Z}_2[x]/\langle p(x) \rangle$ has just four elements.
   (iii) Prove that the ring $\mathbb{Z}_2[x]/\langle p(x) \rangle$ is a field.

Homework 22. 1. Let $F \subseteq K$ be fields and $U := \{u_1, \ldots, u_r\}$ a subset of K. Define $F(U)$ to be the intersection of all subfields of K containing F and U. We also denote this intersection as $F(u_1, \ldots, u_r)$.
   (i) Show that $F(U)$ is the smallest subfield of K containing F and U.
   (ii) Show that

$$F(U) = \{a(u_1, \ldots, u_r)b(u_1, \ldots, u_r)^{-1} \mid a(x_1, \ldots, x_r), b(x_1, \ldots, x_r) \in F[x_1, \ldots, x_r] \text{ with } b(u_1, \ldots, u_r) \neq 0\}.$$

2. Suppose $U = \{u\}$ in problem 1 and u is algebraic over F. Reconcile the description of $F(u)$ in problem 1 with the description of $F(u)$ from the lecture of March 27.

3. Maintaining the notation from problem 1.
   (i) Suppose $r = 2$. Show that $F(u_1, u_2) = F(u_1)(u_2)$.
   (ii) Let $X_1 \cup \cdots \cup X_s$ (with $s \leq t$) be a partition of U. Prove that $F(U) = F(X_1)(X_2) \cdots (X_s)$.

3. Maintaining the notation from problem 1, we say that $u_1, \ldots, u_r \in K$ are *algebraically independent* over F of $p(u_1, \ldots, u_r) \neq 0$, for all polynomials $p(x_1, \ldots, x_r) \in F[x_1, \ldots, x_r]$. Show that if $u_1, \ldots, u_r$ are algebraically independent over F, then $F(u_1, \ldots, u_n)$ is isomorphic to the quotient field of $F[x_1, \ldots, x_r]$, i.e., the rational function field in r variables over F.

Homework 23. 1. Show that $p(x) = x^3 + x^2 + 2x + 1$ is irreducible over $\mathbb{Z}_3$.

2. For $p(x)$ as in the previous problem, from class we know that there is a field K containing $\mathbb{Z}_3$ and $\alpha \in K$ such that $p(\alpha) = 0$.
   (i) How many elements are in the field $\mathbb{Z}_3(\alpha)$?
   (ii) In the field $\mathbb{Z}_3(\alpha)$ calculate $A \cdot B$ and A^{-1}, for $A := 1 + 2\alpha + \alpha^2$ and $B := 2 + \alpha + 2\alpha^2$.

3. Given an example of a field with 125 elements.

4. Fix a prime p. Assume that for all $n \geq 1$, there exists an irreducible polynomial in $\mathbb{Z}_p[x]$ having degree n. Show that for all primes p and $n \geq 1$, there exists a field with p^n elements.

5. Let $\alpha \in K \supseteq \mathbb{Z}_2$ be a root of $x^2 + x + 1$. Show that $\mathbb{Z}_2(\alpha)$ is splitting field of $x^2 + x + 1$ over $\mathbb{Z}_2$.

Homework 24. 1. Write out addition and multiplication tables for the field $\mathbb{Z}_2(\alpha)$ in problem 5 of the previous assignment.

2. Now let $p(x)$ and α be as in problems 1 and 2 from Homework 23. Determine whether or not $\mathbb{Z}_3(\alpha)$ is the splitting field for $p(x)$ over $\mathbb{Z}_3$.

3. Let α be a root of the irreducible polynomial $x^2 + x + 2 \in \mathbb{Z}_3[x]$. Show that $\mathbb{Z}_3(\alpha)$ is its splitting field over $\mathbb{Z}_3$ and $\mathbb{Z}_3(\alpha)$ is a field with nine elements.

4. Let $p, q \in \mathbb{Z}$ be distinct prime numbers. Show that $[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}] = 4$.

5. Let $n \geq 2$ and set $\epsilon := e^{\frac{2\pi i}{n}}$.
   (i) Show that $\mathbb{Q}(\epsilon)$ is the splitting field for $x^n - 1$ over $\mathbb{Q}$.
   (ii) If $n = p$ is prime, find $[\mathbb{Q}(\epsilon) : \mathbb{Q}]$. Hint: First make an educated guess for the minimal polynomial of ϵ over $\mathbb{Q}$, then show that the function $\phi : \mathbb{Q}[x] \to \mathbb{Q}[x]$ given by $\phi(f(x)) = f(x+1)$ is an automorphism, and then apply Eisenstein's criterion.

Homework 25. 1. Consider $\alpha := 1 + \sqrt{2} + \sqrt{3} + \sqrt{6} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Find a polynomial $p(x) \in \mathbb{Q}[x]$ such that $p(\alpha) = 0$. Determine if the polynomial you found is the minimal polynomial for α over $\mathbb{Q}$.

2. Prove that for any field L containing $\mathbb{Z}_p$ and $a, b \in L$, then $(a + b)^p = a^p + b^p$.

3. Let x, y be indeterminates over the field $\mathbb{Z}_2$. Set $F := \mathbb{Z}_2(x^2, y^2)$ and $K := \mathbb{Z}_2(x, y)$. Set $E := \mathbb{Z}(x, y^2)$. Prove that $[E : F] = 2$ and $[K : E] = 2$. Conclude that $[K : F] = 4$.

4. In the notation of problem 3, prove that $\alpha^2 \in F$, for all $\alpha \in K$.

5. Use the previous two problems to show that for $F \subseteq K$ as in problem 3, there does **not** exist $\alpha \in K$ such that $K = F(\alpha)$. Conclude that there are infinitely many intermediate fields $F \subsetneq E \subsetneq K$.

Homework 26. 1. Construct a field K with 16 elements, and identify explicitly a subfield with 4 elements. Hint: Start by finding an irreducible polynomial of degree four over $\mathbb{Z}_2$.

2. For K as in problem 1, is there a subfield of K with 8 elements?

3. Let K be a field with p^m elements, with p prime and $m \geq 1$. Let $\sigma : K \to K$ be given by $\sigma(\alpha) = \alpha^p$, for all $\alpha \in K$. Show that σ is an automorphism of K fixing $\mathbb{Z}_p$. We call σ the *Frobenius automorphism* of K.

4. For K and σ as in problem 3, what is $\sigma^j(\alpha)$, for $j \geq 1$ and $\alpha \in K$? What is σ^m?

5. Let K and σ be as in problem 3. Suppose $n \mid m$. Show that $F := \{\alpha \in K \mid \sigma^n(\alpha) = \alpha\}$ is the unique subfield of K containing p^n elements.

Homework 27. Let $F \subseteq K$ be an extension of fields, and write $\mathrm{Gal}(K/F)$ for the set of automorphisms of K fixing F, i.e., if $\sigma \in \mathrm{Gal}(K/F)$, then σ is an automorphism of K and $\sigma(\lambda) = \lambda$, for all $\lambda \in F$.

1. Show that $\mathrm{Gal}(K/F)$ is a group.

2. Show that if $f(x) \in F[x]$, $\alpha \in K$ satisfies $f(\alpha) = 0$, then $f(\sigma(\alpha)) = 0$, for all $\sigma \in \mathrm{Gal}(K/F)$.

3. Show that if $K = F(\alpha)$, for $\alpha \in K$ a primitive element, then $\mathrm{Gal}(K/F)$ is finite. In particular, if $F \subseteq K$ is a finite extension, with $\mathbb{Q} \subseteq F$, then $\mathrm{Gal}(K/F)$ is a finite group.

Homework 28. Prove the following statements about finite fields. You may use the following fact: Let F be a field and $f(x) \in F[x]$ a non-constant polynomial. If $f(x)$ and $f'(x)$ are relatively prime, then $f(x)$ has distinct roots in its splitting field.
   (i) If F is a finite field, then $|F| = p^n$, for some prime p and and integer $n \geq 1$. Moreover F contains a subfield isomorphic to $\mathbb{Z}_p$.

(ii) Given a prime p and an integer $n \geq 1$, there exists a field F with p^n elements, namely the splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$. Prove this by showing that F turns out to be the set of distinct roots of $x^{p^n} - x$.

(iii) If F is a field with p^n elements, then F is a splitting field for $x^{p^n} - x$ over $\mathbb{Z}_p$. Conclude that any two fields with p^n elements are isomorphic (since any two splitting fields for the same polynomial over the same base field are isomorphic, a fact we have not yet established in class).

(iv) Suppose $F \subseteq K$ are finite fields with $|F| = p^n$ and $|K| = p^m$. Then $n \mid m$. Conversely, if K is a field with p^m elements and $n \mid m$, then there exists a subfield $F \subseteq K$ with $|F| = p^n$.

(v) If K is a finite field with $|K| = p^m$, then there is a *unique* subfield F of K with $|F| = p^n$, for all n dividing m.

Homework 29. 1. For $K := \mathbb{Q}(\sqrt{2}, \sqrt{3})$, use the Crucial Proposition from the lecture of April 12 to calculate $\mathrm{Gal}(K/\mathbb{Q})$. Use your answer to find all of the roots to $p(x) = x^4 - 10x^2 + 1$. Hint: From class, you already know one of the roots of $p(x)$.

2. Let $\gamma \in \mathbb{C}$ be a primitive 8^{th} root of unity (e.g., $e^{\frac{2\pi i}{8}}$) and set $K := \mathbb{Q}(\gamma)$. Find (with proof) the minimal polynomial of α

3. Let $\gamma \in \mathbb{C}$ be a primitive 8^{th} root of unity (e.g., $e^{\frac{2\pi i}{8}}$) and set $K := \mathbb{Q}(\gamma)$. Find $\mathrm{Gal}(K/\mathbb{Q})$.

4. Write out a group table for the Galois group you found in problem 3.

5. For K as in problem 2, set $\alpha := \gamma + \gamma^2$. Find the minimal polynomial $p(x)$ for α over $\mathbb{Q}$ and all of the roots of $p(x)$.

Homework 30. 1. Let F be a field and $f(x) \in F[x]$ be a non-constant polynomial. Prove that $f(x)$ and $f'(x)$ have no common factor in $F[x]$ if and only if $f(x)$ has distinct roots in its algebraic closure $\overline{F}$

2. Let $\epsilon \in \mathbb{C}$ be a primitive nth root of unity, e.g., $\epsilon = e^{\frac{2\pi i}{n}}$. The minimal polynomial for ϵ over $\mathbb{Q}$ is called the nth *cyclotomic polynomial* and is denoted $\Phi_n(x)$. It is a standard fact that $\Phi_n(x)$ has integer coefficients and degree $\phi(n)$, the Euler totient function.

(i) Show that $\mathbb{Q}(\epsilon)$ is a splitting field for $x^n - 1$ over $\mathbb{Q}$.

(ii) By definition, $\gamma \in \mathbb{C}$ is a primitive nth root of unity if and only if $\gamma^n = 1$ and $\gamma^r \neq 1$ for $r < n$. Prove that: ϵ^i is a primitive nth root of unity if and only if i and n are relatively prime if and only if $\langle \epsilon^i \rangle = \langle \epsilon \rangle$ and that this accounts for all primitive nth roots of unity.

(iii) Prove that the distinct roots of $\Phi_n(x)$ are the primitive roots of unity.

(iv) Prove that $\mathrm{Gal}(\mathbb{Q}(\epsilon)/\mathbb{Q}) \cong (\mathbb{Z}_n)^*$, the multiplicative group of units in the ring $\mathbb{Z}_n$.

(v) Show that $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

(vi) Use (v) and induction to prove that $\Phi_n(x) \in \mathbb{Z}[x]$, for all $n \geq 1$.

Homework 31. 1. Let $F \subseteq K$ be an arbitrary (i.e., not necessarily finite) algebraic extension. Show that any field homomorphism $\sigma : F \to \overline{F}$ extends to a field homomorphism $\hat{\sigma} : K \to \overline{F}$. Note that a field homomorphism is automatically one-to-one. Hint: Use Zorn's Lemma together with the Crucial Proposition from April 12.

2. Use the previous problem to show that any two algebraic closures of the field F are isomorphic.

Homework 32. 1. Let ϵ be a primitive 5th root of unity. Find all of the subgroups of the Galois group of the extension $\mathbb{Q} \subseteq \mathbb{Q}(\epsilon)$ and the corresponding fixed fields.

2. Let $K := \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Show that $[K : \mathbb{Q}] = 8$ and $\mathrm{Gal}(K/\mathbb{Q}) = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Then use the Galois correspondence theorem to find all intermediate fields between $\mathbb{Q}$and K. Hints: (i) It may be more convenient to write the Galois group multiplicatively, rather than additively. (ii) If A, B are abelian groups, there may be more subgroups than just subgroups of the form $H \times K$, where H is a subgroup of A and K is a subgroup of B.