MATH 415

Modern Algebra I

Lecture 25:
Review for the final exam.

Topics for the final exam

Group theory:

- Binary operations
- Groups
- Subgroups, cyclic groups
- Groups of permutations
- Cosets, Lagrange's theorem
- Direct product of groups
- Classification of abelian groups
- Homomorphisms of groups
- Factor groups
- Group actions

Fraleigh: Sections 0–17

Topics for the final exam

Theory of rings and fields:

- Rings and fields
- Integral domains
- Modular arithmetic
- Rings of polynomials
- Factorization of polynomials

- Ideals
- Factor rings
- Homomorphisms of rings
- Prime and maximal ideals
- Euclidean algorithm

Fraleigh: Sections 18–23, 26–27.

Sample problems

Problem 1. For any positive integer n let $n\mathbb{Z}$ denote the set of all integers divisible by n.

(i) Does the set $3\mathbb{Z} \cup 4\mathbb{Z} \cup 7\mathbb{Z}$ form a semigroup under addition? Does it form a group?

(ii) Does the set $3\mathbb{Z} \cup 4\mathbb{Z} \cup 7\mathbb{Z}$ form a semigroup under multiplication? Does it form a group?

Problem 2. Consider a relation $\sim$ on a group G defined as follows. For any $g, h \in G$ we let $g \sim h$ if and only if g is conjugate to h, which means that $g = xhx^{-1}$ for some $x \in G$ (where x may depend on g and h). Show that $\sim$ is an equivalence relation on G.

Problem 3. Find all subgroups of the group G_{15} (multiplicative group of invertible congruence classes modulo 15.)

Sample problems

Problem 4. Let $\pi = (1\,2)(2\,3)(3\,4)(4\,5)(5\,6)$ and $\sigma = (1\,2\,3)(2\,3\,4)(3\,4\,5)(4\,5\,6)$. Find the order and the sign of the following permutations: π, σ, $\pi\sigma$, and $\sigma\pi$.

Problem 5. Let G be a group. Suppose H is a subgroup of G of finite index $(G : H)$ and K is a subgroup of H of finite index $(H : K)$. Prove that K is a subgroup of finite index in G and, moreover, $(G : K) = (G : H)(H : K)$.

Problem 6. Let G be the group of all symmetries of a regular tetrahedron T. The group G naturally acts on the set of vertices of T, the set of edges of T, and the set of faces of T.

(i) Show that each of the three actions is transitive.

(ii) Show that the stabilizer of any vertex is isomorphic to the symmetric group S_3.

(iii) Show that the stabilizer of any edge is isomorphic to the Klein 4-group $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(iv) Show that the stabilizer of any face is isomorphic to S_3.

Sample problems

Problem 7. Let S be a nonempty set and $\mathcal{P}(S)$ be the set of all subsets of S. **(i)** Prove that $\mathcal{P}(S)$ with the operations of symmetric difference $\triangle$ (as addition) and intersection $\cap$ (as multiplication) is a commutative ring with unity.

(ii) Prove that the ring $\mathcal{P}(S)$ is isomorphic to the ring of functions $\mathcal{F}(S, \mathbb{Z}_2)$.

Problem 8. Solve a system of congruences (find all solutions):

$$\begin{cases} x \equiv 2 \bmod 5, \\ x \equiv 3 \bmod 6, \\ x \equiv 6 \bmod 7. \end{cases}$$

Problem 9. Find all integer solutions of a system

$$\begin{cases} 2x + 5y - z = 1, \\ x - 2y + 3z = 2. \end{cases}$$

Sample problems

Problem 10. Factor a polynomial $p(x) = x^4 - 2x^3 - x^2 - 2x + 1$ into irreducible factors over the fields $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_5$ and $\mathbb{Z}_7$.

Problem 11. Let

$$M = \left\{ \begin{pmatrix} x & 0 \\ y & z \end{pmatrix} \;\middle|\; x, y, z \in \mathbb{R} \right\}, \quad J = \left\{ \begin{pmatrix} 0 & 0 \\ y & 0 \end{pmatrix} \;\middle|\; y \in \mathbb{R} \right\}.$$

(i) Show that M is a subring of the matrix ring $\mathcal{M}_{2,2}(\mathbb{R})$.
(ii) Show that J is a two-sided ideal in M.
(iii) Show that the factor ring M/J is isomorphic to $\mathbb{R} \times \mathbb{R}$.

Problem 12. The polynomial $f(x) = x^6 + 3x^5 - 5x^3 + 3x - 1$ has how many distinct complex roots?

Problem 1. For any positive integer n let $n\mathbb{Z}$ denote the set of all integers divisible by n.

(i) Does the set $3\mathbb{Z} \cup 4\mathbb{Z} \cup 7\mathbb{Z}$ form a semigroup under addition? Does it form a group?

(ii) Does the set $3\mathbb{Z} \cup 4\mathbb{Z} \cup 7\mathbb{Z}$ form a semigroup under multiplication? Does it form a group?

The set $S = 3\mathbb{Z} \cup 4\mathbb{Z} \cup 7\mathbb{Z}$ consists of all integers divisible by at least one of the numbers 3, 4 and 7. This set is not closed under addition. For example, the numbers 4 and 7 belong to S while their sum $4 + 7 = 11$ does not. Therefore S is neither a semigroup nor a group with respect to addition.

Each of the sets $3\mathbb{Z}$, $4\mathbb{Z}$ and $7\mathbb{Z}$ is closed under multiplication by any integer. Hence their union S is also closed under multiplication by any integer. In particular, S is a semigroup with respect to multiplication. It is not a group since it does not contain 1 (and 1 is the only number that can be the multiplicative identity element unless $S = \{0\}$).

Problem 2. Consider a relation $\sim$ on a group G defined as follows. For any $g, h \in G$ we let $g \sim h$ if and only if g is conjugate to h, which means that $g = xhx^{-1}$ for some $x \in G$ (where x may depend on g and h). Show that $\sim$ is an equivalence relation on G.

We have to show that the relation $\sim$ is reflexive, symmetric and transitive.

Reflexivity. $g \sim g$ since $g = ege^{-1}$, where e is the identity element.

Symmetry. Assume $g \sim h$, that is, $g = xhx^{-1}$ for some $x \in G$. Then $h = x^{-1}gx = x^{-1}g(x^{-1})^{-1} = x_1 g x_1^{-1}$, where $x_1 = x^{-1}$. Hence $h \sim g$.

Transitivity. Assume $g \sim h$ and $h \sim k$, that is, $g = x_1 h x_1^{-1}$ and $h = x_2 k x_2^{-1}$ for some $x_1, x_2 \in G$. Then $g = x_1(x_2 k x_2^{-1})x_1^{-1} = (x_1 x_2)k(x_2^{-1}x_1^{-1}) = (x_1 x_2)k(x_1 x_2)^{-1}$ $= xkx^{-1}$, where $x = x_1 x_2$. Hence $g \sim k$.

Problem 3. Find all subgroups of the group G_{15} (multiplicative group of invertible congruence classes modulo 15.)

A congruence class $[a]_{15}$ belongs to G_{15} if and only if $\gcd(a, 15) = 1$. Hence the group G_{15} consists of the following 8 elements: $[1]$, $[2]$, $[4]$, $[7]$, $[8]$, $[11]$, $[13]$, $[14]$ or, equivalently, $[1]$, $[2]$, $[4]$, $[7]$, $[-7]$, $[-4]$, $[-2]$, $[-1]$.

First we find all cyclic subgroups of G_{15}. These are $\{[1]\}$, $\{[1], [4]\}$, $\{[1], [-4]\}$, $\{[1], [-1]\}$, $\{[1], [2], [4], [8]\}$, and $\{[1], [4], [7], [13]\} = \{[1], [-2], [4], [-8]\}$.

Note that any subgroup of G_{15} is a union of (one or more) cyclic subgroups. By Lagrange's Theorem, a subgroup of G_{15} can be of order 1, 2, 4 or 8. It follows that the only possible non-cyclic subgroups of G_{15} might be G_{15} itself and $\{[1], [4], [-4], [-1]\}$. We can check that both are indeed subgroups.

Problem 4. Let $\pi = (1\,2)(2\,3)(3\,4)(4\,5)(5\,6)$ and $\sigma = (1\,2\,3)(2\,3\,4)(3\,4\,5)(4\,5\,6)$. Find the order and the sign of the following permutations: π, σ, $\pi\sigma$, and $\sigma\pi$.

Any transposition is an odd permutation, its sign is -1. Any cycle of length 3 is an even permutation, its sign is $+1$. Since the sign is a multiplicative function, we obtain that $\operatorname{sgn}(\pi) = (-1)^5 = -1$ and $\operatorname{sgn}(\sigma) = 1^4 = 1$. Then $\operatorname{sgn}(\pi\sigma) = \operatorname{sgn}(\sigma\pi) = \operatorname{sgn}(\pi)\operatorname{sgn}(\sigma) = -1$.

To find the order of a permutation, we need to decompose it into a product of disjoint cycles. First we decompose π and σ: $\pi = (1\,2\,3\,4\,5\,6)$, $\sigma = (1\,2)(5\,6)$. Then we use these decompositions to decompose $\pi\sigma$ and $\sigma\pi$: $\pi\sigma = (1\,3\,4\,5)$ and $\sigma\pi = (2\,3\,4\,6)$. The order of a product of disjoint cycles equals the least common multiple of their lengths. Therefore $o(\pi) = 6$, $o(\sigma) = 2$, and $o(\pi\sigma) = o(\sigma\pi) = 4$.

Problem 5. Let G be a group. Suppose H is a subgroup of G of finite index $(G : H)$ and K is a subgroup of H of finite index $(H : K)$. Prove that K is a subgroup of finite index in G and, moreover, $(G : K) = (G : H)(H : K)$.

First assume G is a finite group. Then any subgroup is of finite order and of finite index. By Lagrange's Theorem, $|G| = (G : H)\,|H|$ and $|H| = (H : K)\,|K|$ so that $|G| = (G : H)(H : K)\,|K|$. Also by Lagrange's Theorem, $|G| = (G : K)\,|K|$. It follows that $(G : K) = (G : H)(H : K)$.

In the general case, we need a different argument.

Problem 5. Let G be a group. Suppose H is a subgroup of G of finite index $(G : H)$ and K is a subgroup of H of finite index $(H : K)$. Prove that K is a subgroup of finite index in G and, moreover, $(G : K) = (G : H)(H : K)$.

Let $n = (G : H)$ and suppose $g_1, g_2, \ldots, g_n$ is a complete list of representatives of the left cosets of H in G. Further, let $k = (H : K)$ and suppose $h_1, h_2, \ldots, h_k$ is a complete list of representatives of the left cosets of K in H. Then G is a disjoint union of cosets $g_1H, g_2H, \ldots, g_nH$ while H is a disjoint union of cosets $h_1K, h_2K, \ldots, h_kK$. It follows that each g_iH is a disjoint union of sets $g_ih_1K, g_ih_2K, \ldots, g_ih_kK$, which are cosets of K in G. Therefore G is a disjoint union of all sets of the form g_ih_jK, $1 \leq i \leq n$, $1 \leq j \leq k$. Hence these are all cosets of the subgroup K in G. Thus the number $(G : K)$ of the cosets equals $nk = (G : H)(H : K)$.

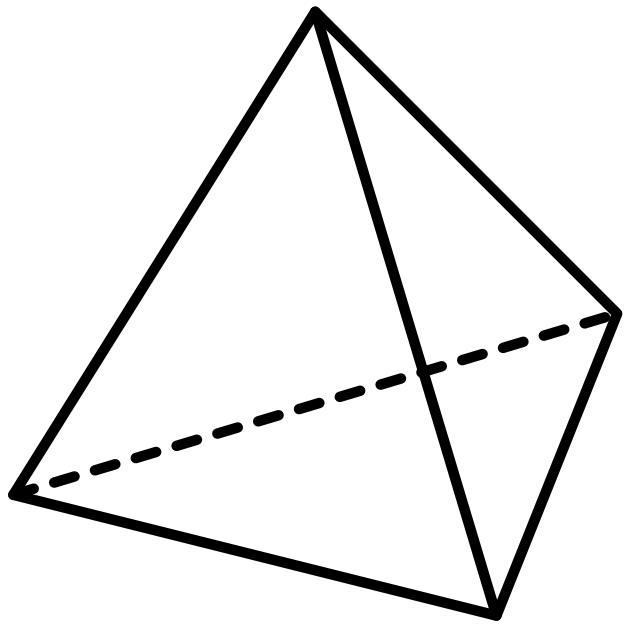
Problem 6. Let G be the group of all symmetries of a regular tetrahedron T. The group G naturally acts on the set of vertices of T, the set of edges of T, and the set of faces of T.

(i) Show that each of the three actions is transitive.

(ii) Show that the stabilizer of any vertex is isomorphic to the symmetric group S_3.

(iii) Show that the stabilizer of any edge is isomorphic to the Klein 4-group $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(iv) Show that the stabilizer of any face is isomorphic to S_3.



Problem 7. Let S be a nonempty set and $\mathcal{P}(S)$ be the set of all subsets of S. **(i)** Prove that $\mathcal{P}(S)$ with the operations of symmetric difference $\triangle$ (as addition) and intersection $\cap$ (as multiplication) is a commutative ring with unity.

(ii) Prove that the ring $\mathcal{P}(S)$ is isomorphic to the ring of functions $\mathcal{F}(S, \mathbb{Z}_2)$.

For any subset $E \subset S$ let $\chi_E : S \to \{0, 1\}$ be the characteristic function of E,

$$\chi_E(x) = \begin{cases} 1 & \text{if} \quad x \in E, \\ 0 & \text{if} \quad x \notin E. \end{cases}$$

Let E_1 and E_2 be any subsets of S. Note that $\chi_{E_1 \cap E_2}(x) = 1$ if and only if $\chi_{E_1}(x) = \chi_{E_2}(x) = 1$. Hence $\chi_{E_1 \cap E_2} = \chi_{E_1} \chi_{E_2}$. Since $E_1 \triangle E_2 = (E_1 \cup E_2) \setminus (E_1 \cap E_2)$, it follows that

$$\chi_{E_1 \triangle E_2} = \chi_{E_1} + \chi_{E_2} - 2\chi_{E_1 \cap E_2} \equiv \chi_{E_1} + \chi_{E_2} (\mathrm{mod}\, 2).$$

Let us consider the characteristic functions χ_E as taking their values in the ring $\mathbb{Z}_2$ rather than $\mathbb{R}$. This yields a map $F : \mathcal{P}(S) \to \mathcal{F}(S, \mathbb{Z}_2)$ given by $F(E) = \chi_E$ for all $E \subset S$.

By the above F is a homomorphism of the binary structure $\big(\mathcal{P}(S), \cap\big)$ to $\big(\mathcal{F}(S, \mathbb{Z}_2), \cdot\big)$ and, simultaneously, a homomorphism of $\big(\mathcal{P}(S), \triangle\big)$ to $\big(\mathcal{F}(S, \mathbb{Z}_2), +\big)$. The map F is clearly injective. It is also surjective since any function $g : S \to \mathbb{Z}_2$ can be represented as χ_E, where $E = \{x \in S \mid g(x) = 1\}$. Hence the homomorphism F is actually an isomorphism.

Since $\mathcal{F}(S, \mathbb{Z}_2)$ is a commutative ring with unity, the binary structure $\big(\mathcal{F}(S, \mathbb{Z}_2), +\big)$ is an abelian group while the binary structure $\big(\mathcal{F}(S, \mathbb{Z}_2), \cdot\big)$ is a commutative monoid. In view of the isomorphism F, the set $\mathcal{P}(S)$ is an abelian group relative to the operation $\triangle$ and a commutative monoid relative to the operation $\cap$. Moreover, $\cap$ distributes over $\triangle$, which follows (through F) from the distributive law in $\mathcal{F}(S, \mathbb{Z}_2)$. Thus $\big(\mathcal{P}(S), \triangle, \cap\big)$ is a commutative ring with unity and F is an isomorphism of rings.

Problem 8. Solve a system of congruences: $\begin{cases} x \equiv 2 \bmod 5, \\ x \equiv 3 \bmod 6, \\ x \equiv 6 \bmod 7. \end{cases}$

The moduli 5, 6 and 7 are pairwise coprime. By the generalized Chinese Remainder Theorem, all solutions of the system form a single congruence class modulo $5 \cdot 6 \cdot 7 = 210$. It remains to find a particular solution. One way to do this is to represent 1 as an integral linear combination of $6 \cdot 7 = 42$, $5 \cdot 7 = 35$ and $5 \cdot 6 = 30$ (note that 1 is the greatest common divisor of these numbers). Suppose $1 = 42n_1 + 35n_2 + 30n_3$ for some integers n_1, n_2, n_3. Then the numbers $x_1 = 42n_1$, $x_2 = 35n_2$ and $x_3 = 30n_3$ satisfy the following systems of congruences:

$$\begin{cases} x_1 \equiv 1 \bmod 5 \\ x_1 \equiv 0 \bmod 6 \\ x_1 \equiv 0 \bmod 7 \end{cases} \qquad \begin{cases} x_2 \equiv 0 \bmod 5 \\ x_2 \equiv 1 \bmod 6 \\ x_2 \equiv 0 \bmod 7 \end{cases} \qquad \begin{cases} x_3 \equiv 0 \bmod 5 \\ x_3 \equiv 0 \bmod 6 \\ x_3 \equiv 1 \bmod 7 \end{cases}$$

It follows that $x_0 = 2x_1 + 3x_2 + 6x_3$ is a solution of the given system.

Let us apply the generalized Euclidean algorithm (in matrix form) to 42, 35 and 30. We begin with the augmented matrix of a system

$$\begin{cases} y_1 = 42, \\ y_2 = 35, \\ y_3 = 30. \end{cases}$$

At each step, we choose two numbers in the rightmost column, divide the larger of them by the smaller, and replace the dividend with the remainder. This can be done by applying an elementary row operation to the matrix.

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & 42 \\ 0 & 1 & 0 & 35 \\ 0 & 0 & 1 & 30 \end{array}\right) \to \left(\begin{array}{ccc|c} 1 & 0 & -1 & 12 \\ 0 & 1 & 0 & 35 \\ 0 & 0 & 1 & 30 \end{array}\right)$$

$$\to \left(\begin{array}{ccc|c} 1 & 0 & -1 & 12 \\ -2 & 1 & 2 & 11 \\ 0 & 0 & 1 & 30 \end{array}\right) \to \left(\begin{array}{ccc|c} 3 & -1 & -3 & 1 \\ -2 & 1 & 2 & 11 \\ 0 & 0 & 1 & 30 \end{array}\right)$$

The first row of the last matrix corresponds to a linear equation $3y_1 - y_2 - 3y_3 = 1$. By construction, $(y_1, y_2, y_3) = (42, 35, 30)$ is a solution of that equation. In other words,

$$1 = 42 \cdot 3 + 35 \cdot (-1) + 30 \cdot (-3).$$

Let x_1, x_2, x_3 be the terms in this expansion of 1: $x_1 = 42 \cdot 3 = 126$, $x_2 = 35 \cdot (-1) = -35$ and $x_3 = 30 \cdot (-3) = -90$. By the above, one solution of the given system of congruences is

$$\begin{aligned} x_0 &= 2x_1 + 3x_2 + 6x_3 \\ &= 2 \cdot 126 + 3(-35) + 6(-90) = -393. \end{aligned}$$

Another solution is $-393 + 2 \cdot 210 = 27$. The general solution is $x = 27 + 210n$, $n \in \mathbb{Z}$.

Problem 8. Solve a system of congruences: $\begin{cases} x \equiv 2 \bmod 5, \\ x \equiv 3 \bmod 6, \\ x \equiv 6 \bmod 7. \end{cases}$

Alternative solution. The general solution of the first congruence is $x = 2 + 5k$, $k \in \mathbb{Z}$. Substituting this into the second congruence, we obtain a linear congruence in k:

$$2 + 5k \equiv 3 \bmod 6 \iff 5k \equiv 1 \bmod 6$$

The multiplicative inverse of 5 modulo 6 is -1 since $5 \cdot (-1) = -5 \equiv 1 \bmod 6$. Hence the general solution of the linear congruence is $k = -1 + 6m$, where $m \in \mathbb{Z}$. Then $x = 2 + 5k = 2 + 5(-1 + 6m) = -3 + 30m$. Substituting this into the third congruence of the system, we obtain

$$-3 + 30m \equiv 6 \bmod 7 \iff 30m \equiv 9 \bmod 7$$
$$\iff 2m \equiv 2 \bmod 7 \iff m \equiv 1 \bmod 7$$

Hence $m = 1 + 7n$, where $n \in \mathbb{Z}$. Then $x = -3 + 30m$ $= -3 + 30(1 + 7n) = 27 + 210n$ is the general solution of the system.

Problem 9. Find all integer solutions of a system

$$\begin{cases} 2x + 5y - z = 1, \\ x - 2y + 3z = 2. \end{cases}$$

First we solve the second equation for x and substitute it into the first equation:

$$\begin{cases} 2(2y - 3z + 2) + 5y - z = 1, \\ x = 2y - 3z + 2 \end{cases} \iff \begin{cases} 9y - 7z = -3, \\ x = 2y - 3z + 2. \end{cases}$$

For any integer solution of the equation $9y - 7z = -3$, the number y is a solution of the linear congruence $9y \equiv -3 \bmod 7$. Solving the congruence, we obtain

$$9y \equiv -3 \bmod 7 \iff 2y \equiv 4 \bmod 7 \iff y \equiv 2 \bmod 7.$$

Hence $y = 2 + 7k$, where $k \in \mathbb{Z}$. Now we find z and x by back substitution: $z = (9y + 3)/7 = (9(2 + 7k) + 3)/7$ $= 3 + 9k$ and $x = 2y - 3z + 2 = 2(2 + 7k) - 3(3 + 9k) + 2$ $= -3 - 13k$. Note that z and x are integers for all $k \in \mathbb{Z}$.

Problem 10. Factor a polynomial $p(x) = x^4 - 2x^3 - x^2 - 2x + 1$ into irreducible factors over the fields $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_5$ and $\mathbb{Z}_7$.

First consider p as a function on $\mathbb{C}$. For any $x \neq 0$ we have

$$\frac{p(x)}{x^2} = x^2 - 2x - 1 - \frac{2}{x} + \frac{1}{x^2} = \left(x^2 + \frac{1}{x^2}\right) - 2\left(x + \frac{1}{x}\right) - 1.$$

Let $y = x + \dfrac{1}{x}$. Then $x^2 + \dfrac{1}{x^2} = y^2 - 2$. Consequently,

$$p(x)/x^2 = (y^2 - 2) - 2y - 1 = y^2 - 2y - 3 = (y - 3)(y + 1).$$

Then

$$\begin{aligned} p(x) &= x^2(y - 3)(y + 1) = x^2(x + x^{-1} - 3)(x + x^{-1} + 1) \\ &= (x^2 - 3x + 1)(x^2 + x + 1). \end{aligned}$$

We have obtained the above factorization of p as an equality of functions on $\mathbb{C} \setminus \{0\}$. Now we can check (by direct multiplication) that, in fact, it holds as an equality of polynomials over any field.

Problem 10. Factor a polynomial $p(x) = x^4-2x^3-x^2-2x+1$ into irreducible factors over the fields $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_5$ and $\mathbb{Z}_7$.

We already know that $p(x) = (x^2 - 3x + 1)(x^2 + x + 1)$ over any field. Depending on the field, any of the two quadratic factors either is irreducible (if it has no roots) or else splits as a product of two linear factors.

Over the field $\mathbb{C}$, the polynomial $x^2 - 3x + 1$ has roots $\alpha_{1,2} = \frac{1}{2}(3 \pm \sqrt{5})$ and the polynomial $x^2 + x + 1$ has roots $\beta_{1,2} = \frac{1}{2}(-1 \pm i\sqrt{3})$. Hence the factorization into irreducible factors over $\mathbb{C}$ is $p(x) = (x - \alpha_1)(x - \alpha_2)(x - \beta_1)(x - \beta_2)$. Note that the numbers β_1 and β_2 are not real while α_1 and α_2 are real but not rational. Since $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, it follows that over $\mathbb{R}$, the factorization is $p(x) = (x-\alpha_1)(x-\alpha_2)(x^2+x+1)$, and over $\mathbb{Q}$, it is $p(x) = (x^2 - 3x + 1)(x^2 + x + 1)$.

In the case of a finite field, we find roots by trying all elements of the field. We obtain that $p(x) = (x+1)^2(x^2 + x + 1)$ over the field $\mathbb{Z}_5$ and $p(x) = (x^2 - 3x + 1)(x - 2)(x + 3)$ over $\mathbb{Z}_7$.

Problem 11. Let

$$M = \left\{ \begin{pmatrix} x & 0 \\ y & z \end{pmatrix} \,\middle|\, x, y, z \in \mathbb{R} \right\}, \quad J = \left\{ \begin{pmatrix} 0 & 0 \\ y & 0 \end{pmatrix} \,\middle|\, y \in \mathbb{R} \right\}.$$

(i) Show that M is a subring of the matrix ring $\mathcal{M}_{2,2}(\mathbb{R})$.

For any $x, y, z, x', y', z' \in \mathbb{R}$ we obtain

$$\begin{pmatrix} x & 0 \\ y & z \end{pmatrix} + \begin{pmatrix} x' & 0 \\ y' & z' \end{pmatrix} = \begin{pmatrix} x + x' & 0 \\ y + y' & z + z' \end{pmatrix},$$

$$\begin{pmatrix} x & 0 \\ y & z \end{pmatrix} - \begin{pmatrix} x' & 0 \\ y' & z' \end{pmatrix} = \begin{pmatrix} x - x' & 0 \\ y - y' & z - z' \end{pmatrix},$$

$$\begin{pmatrix} x & 0 \\ y & z \end{pmatrix} \begin{pmatrix} x' & 0 \\ y' & z' \end{pmatrix} = \begin{pmatrix} xx' & 0 \\ yx' + zy' & zz' \end{pmatrix}.$$

It follows that the set M is closed under addition, subtraction and multiplication. Clearly, M is nonempty. Therefore M is a subring of the matrix ring $\mathcal{M}_{2,2}(\mathbb{R})$.

Problem 11. Let

$$M = \left\{ \begin{pmatrix} x & 0 \\ y & z \end{pmatrix} \;\middle|\; x, y, z \in \mathbb{R} \right\}, \quad J = \left\{ \begin{pmatrix} 0 & 0 \\ y & 0 \end{pmatrix} \;\middle|\; y \in \mathbb{R} \right\}.$$

(ii) Show that J is a two-sided ideal in M.
(iii) Show that the factor ring M/J is isomorphic to $\mathbb{R} \times \mathbb{R}$.

Consider a map $\phi : M \to \mathbb{R} \times \mathbb{R}$ given for any $x, y, z \in \mathbb{R}$ by

$$\phi \begin{pmatrix} x & 0 \\ y & z \end{pmatrix} = (x, z).$$

It follows from the solution of part **(i)** that the map ϕ is a homomorphism of rings. Observe that the kernel $\mathrm{Ker}(\phi) = \phi^{-1}(0, 0)$ coincides with the set J. Therefore J is a two-sided ideal in M (since the kernel of any homomorphism is a two-sided ideal). By the Fundamental Theorem on Homomorphisms, the factor ring M/J is isomorphic to $\phi(M) = \mathbb{R} \times \mathbb{R}$.

Problem 12. The polynomial $f(x) = x^6 + 3x^5 - 5x^3 + 3x - 1$ has how many distinct complex roots?

Let $p \in \mathbb{C}[x]$ be a nonzero polynomial. We say that $\alpha \in \mathbb{C}$ is a root of p of multiplicity $k \geq 1$ if the polynomial is divisible by $(x-\alpha)^k$ but not divisible by $(x-\alpha)^{k+1}$. Equivalently, $p(x) = (x-\alpha)^k q(x)$ for some polynomial q such that $q(\alpha) \neq 0$. If this is the case then

$$\begin{aligned} p'(x) &= \left((x-\alpha)^k\right)' q(x) + (x-\alpha)^k q'(x) \\ &= k(x-\alpha)^{k-1} q(x) + (x-\alpha)^k q'(x) = (x-\alpha)^{k-1} r(x), \end{aligned}$$

where $r(x) = kq(x) + (x-\alpha)q'(x)$. Note that $r(x)$ is a polynomial and $r(\alpha) = kq(\alpha) \neq 0$. Hence α is a root of p' of multiplicity $k-1$ if $k > 1$ and not a root of p' if $k = 1$.

Problem 12. The polynomial $f(x) = x^6 + 3x^5 - 5x^3 + 3x - 1$ has how many distinct complex roots?

By the Fundamental Theorem of Algebra, any polynomial $p \in \mathbb{C}[x]$ of degree $n \geq 1$ can be represented as

$$p(x) = c(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n),$$

where $c, \alpha_1, \dots, \alpha_n \in \mathbb{C}$ and $c \neq 0$. The numbers $\alpha_1, \alpha_2, \dots, \alpha_n$ are roots of p, they need not be distinct. We have

$$p(x) = c(x - \beta_1)^{k_1}(x - \beta_2)^{k_2} \dots (x - \beta_m)^{k_m},$$

where $\beta_1, \dots, \beta_m$ are distinct roots of p and $k_1, \dots, k_m$ are their multiplicities. It follows from the above that

$$\gcd(p(x), p'(x)) = (x - \beta_1)^{k_1 - 1}(x - \beta_2)^{k_2 - 1} \dots (x - \beta_m)^{k_m - 1}.$$

As a consequence, the number of distinct roots of the polynomial p equals $\deg(p) - \deg(\gcd(p, p'))$.

Problem 12. The polynomial $f(x) = x^6 + 3x^5 - 5x^3 + 3x - 1$ has how many distinct complex roots?

Let's use the Euclidean algorithm to find the greatest common divisor of the polynomials $f(x) = x^6 + 3x^5 - 5x^3 + 3x - 1$ and $f'(x) = 6x^5 + 15x^4 - 15x^2 + 3$. First we divide f by f':

$$x^6+3x^5-5x^3+3x-1 = (6x^5+15x^4-15x^2+3)\left(\tfrac{1}{6}x+\tfrac{1}{12}\right) + r(x),$$

where $r(x) = -\frac{5}{4}x^4 - \frac{5}{2}x^3 + \frac{5}{4}x^2 + \frac{5}{2}x - \frac{5}{4}$. It is convenient to replace the remainder $r(x)$ by its scalar multiple $\tilde{r}(x) = -\frac{4}{5}r(x) = x^4 + 2x^3 - x^2 - 2x + 1$. Next we divide f' by $\tilde{r}$:

$$6x^5 + 15x^4 - 15x^2 + 3 = (x^4 + 2x^3 - x^2 - 2x + 1)(6x + 3).$$

Since f' is divisible by $\tilde{r}$, it follows that $\gcd(f, f') = \gcd(f', r) = \gcd(f', \tilde{r}) = \tilde{r}$. Thus the number of distinct complex roots of the polynomial f equals $\deg(f) - \deg(\gcd(f, f')) = 6 - 4 = 2$.

Problem 12. The polynomial $f(x) = x^6 + 3x^5 - 5x^3 + 3x - 1$ has how many distinct complex roots?

As a follow-up to the solution, we can find the roots of the polynomial f. It follows from the solution that the polynomial $g = f / \gcd(f, f')$ has the same roots as f but, unlike f, all roots of g are simple (i.e., of multiplicity 1). Dividing f by $\tilde{r}(x) = x^4 + 2x^3 - x^2 - 2x + 1$, we obtain

$$x^6+3x^5-5x^3+3x-1 = (x^4+2x^3-x^2-2x+1)(x^2+x-1).$$

The polynomial $g(x) = x^2 + x - 1$ has two real roots $\beta_{1,2} = \frac{1}{2}(-1 \pm \sqrt{5})$. Therefore $f(x) = (x - \beta_1)^{k_1}(x - \beta_2)^{k_2}$, where k_1 and k_2 are positive integers, $k_1 + k_2 = 6$. Note that $\beta_1\beta_2 = -1$ (the constant term of g) and $\beta_1^{k_1}\beta_2^{k_2} = -1$ (the constant term of f). Then $\beta_1^{k_1-k_2} = (-1)^{k_2+1}$, a rational number. This suggests $k_1 - k_2 = 0$ (so that $k_1 = k_2 = 3$). We can check by direct multiplication that, indeed,

$$x^6+3x^5-5x^3+3x-1 = (x^2+x-1)^3 = (x-\beta_1)^3(x-\beta_2)^3.$$