Spring 2016

1. (a) Prove that every subgroup of a cyclic group is cyclic.

Proof. Let G be a cyclic group. First, suppose that G is of infinite order. Then sending the generator of G to $1 \in \mathbb{Z}$ gives an isomorphism $G \cong \mathbb{Z}$. We claim that every subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$, which is clearly cyclic. Let H be a subgroup of G and let n be the smallest positive integer in H. Then $n\mathbb{Z} \subseteq H$. Suppose the containment is strict and let m be the smallest positive integer in $H \setminus n\mathbb{Z}$. We then have that $1 \leq \gcd(m, n) < n$ and by Bezout's identity we have that $\gcd(m, n) = um + vn$ for some $u, v \in \mathbb{Z}$ is in H. But this contradicts the minimality of n, so we conclude that $H = n\mathbb{Z}$.

Suppose now that $G = \langle g \rangle$ is finite of order n so that $G \cong \mathbb{Z}/n\mathbb{Z}$. By the fourth isomorphism theorem (or lattice/correspondence theorem) there is a one-to-one correspondence between subgroups of $\mathbb{Z}/n\mathbb{Z}$ and subgroups of $\mathbb{Z}$ containing $n\mathbb{Z}$. We have already shown that all subgroups of $\mathbb{Z}$ are cyclic, and since the homomorphic image of a cyclic group is cyclic ($\varphi(g^k) = \varphi(g)^k$), we have that all subgroups of $\mathbb{Z}/n\mathbb{Z}$ are cyclic. □

(b) Is the automorphism group of a cyclic group necessarily cyclic?

Solution. This need not be the case. Let $G \cong \mathbb{Z}/N\mathbb{Z}$. As G is cyclic, any automorphism of G is determined by where it sends a generator and it must map a generator to a generator. The generators of $\mathbb{Z}/N\mathbb{Z}$ exactly correspond to the elements of $(\mathbb{Z}/N\mathbb{Z})^\times$ and we have that $\mathrm{Aut}(\mathbb{Z}/N\mathbb{Z}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$. If N is a product of distinct primes $p, q > 2$ then the Chinese remainder theorem says that

$$(\mathbb{Z}/N\mathbb{Z})^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/(q-1)\mathbb{Z},$$

which is not cyclic □

2. Let $G = \mathbb{Z}/25\mathbb{Z}$ be the cyclic group of order 25.

(a) Can G be given the structure of a $\mathbb{Z}[i]$-module?

Solution. Yes it can. Observe that in $\mathbb{Z}/25\mathbb{Z}$, $-1 = 24 = 6 \cdot 4 = 9^2 \cdot 2^2$, so $18^2 = -1$. Define the action of $a + bi \in \mathbb{Z}[i]$ on $m \in \mathbb{Z}/25\mathbb{Z}$ by

$$(a + bi) \cdot m = (a + 18b)m.$$

This action gives G the structure of a $\mathbb{Z}[i]$-module since

$$\begin{aligned}
[(a+bi)+(c+di)]\cdot m &= [(a+c)+(b+d)i]\cdot m \\
&= [(a+c)+18(b+d)]m \\
&= (a+bi)\cdot m + (c+di)\cdot m. \\
(a+bi)\cdot(m+n) &= (a+18b)(m+n) \\
&= (a+bi)\cdot m + (a+bi)\cdot n. \\
[(a+bi)(c+di)]\cdot m &= [(ac-bd)+(ad+bc)i]m \\
&= [(ac-bd)+18(ad+bc)]m \\
&= (a+bi)\cdot[(c+di)\cdot m].
\end{aligned}$$

□

(b) Can G be given the structure of a $\mathbb{Z}/5\mathbb{Z}$ module?

Solution. No it cannot. If it could then we would have

$$\begin{aligned}
0 &= 0\cdot 1 \\
&= 5\cdot 1 \\
&= (1+1+1+1+1)\cdot 1 \\
&= 1\cdot 1+1\cdot 1+1\cdot 1+1\cdot 1+1\cdot 1 \\
&= 5 \\
&\neq 0.
\end{aligned}$$

□

3. Prove that there is no simple group of order 520.

Proof. Write $520 = 2^3\cdot 5\cdot 13$. By Sylow's theorems, the number of Sylow-5 subgroups, n_5 is 1 mod 5 and divides $2^3\cdot 13 = 104$. The only positive integers satisfying these constraints are 1 and 26. The same reasoning shows that n_{13} must be 1 or 40. If either of n_5 or n_{13} is 1, then since Sylow-p subgroups are conjugate to one another, then that subgroup would be normal. Suppose then that $n_5 = 26$ and $n_{13} = 40$. Then there are $26\cdot 4 = 104$ elements of order 5 and $40\cdot 12 = 480$ elements of order 13. But $104 + 480 = 584 > 520$, so this cannot be the case. We conclude that there must be a unique Sylow-5 or Sylow-13 subgroup which is normal. □

4. Let G be a finite group acting transitively on a set X with $|X| > 1$.

   (a) State the orbit-stabilizer theorem.

   Solution. If a group G acts on a set X then for any $x \in X$, the size of the orbit of x under G is the index of the stabilizer of x under G, $|\mathcal{O}(x)| = [G : \mathrm{Stab}(x)]$. □

   (b) Show that there is some element of G fixing no element of X.

   Proof. Since the action of G on X is transitive there is a single orbit. Burnside's lemma (which immediately follows from the orbit-stabilizer theorem) then states that

$$1 = \frac{1}{|G|} \sum_{g \in G} |\{x \in X : g \cdot x = x\}|.$$

   If $g \in G$ has fixed points then it contributes at least $1/|G|$ to the above sum. If *every* element has a fixed point then we must have that every term in the sum is $1/|G|$. But the identity element fixes every element in X and $|X| > 1$, so we must have that one term in this sum is zero, i.e. at least one element of G is fixed point free. □

5. Let K be a field and let $\overline{K}$ be an algebraic closure of K. Assume $\alpha, \beta \in \overline{K}$ have degree 2 and 3 over K, respectively.

   (a) Can $\alpha\beta$ have degree 5 over K?

   Solution. No it cannot. We have that $K(\alpha\beta)$ is contained in the composite extension $K(\alpha)K(\beta)$. Furthermore, since the degrees of $K(\alpha)$ and $K(\beta)$ over K are relatively prime, we have that the composite extension has degree 6 over K. Since $K(\alpha\beta)$ is a subfield of the composite extension, its degree over K must divide 6. Since 5 doesn't divide 6 we have that $K(\alpha\beta)$ cannot have degree 5 over K. □

   (b) Can $\alpha\beta$ have degree 6 over K?

   Solution. Yes it can. Consider $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt[3]{2})$. $x^2 - 2$ and $x^3 - 2$ are irreducible over $\mathbb{Q}$ by Eisenstein so these extensions are of degree 2 and 3, respectively. We claim that the product $2^{1/2} \cdot 2^{1/3} = 2^{5/6}$ has degree 6 over $\mathbb{Q}$.

   We start by showing that $\mathbb{Q}(2^{5/6}) = \mathbb{Q}(2^{1/6})$. Clearly $\mathbb{Q}(2^{5/6}) \subseteq \mathbb{Q}(2^{1/6})$. On the other hand, $\frac{1}{2^4}(2^{5/6})^5 = 2^{1/6}$, so $\mathbb{Q}(2^{1/6}) \subseteq \mathbb{Q}(2^{5/6})$. Finally, $2^{1/6}$ is a root of the polynomial $x^6 - 2$, which is irreducible over $\mathbb{Q}$ by Eisenstein, so we have that $2^{1/6}$, and therefore $2^{5/6}$, has degree 6 over $\mathbb{Q}$. □

6. Let $L/\mathbb{Q}$ denote a Galois extension with Galois group isomorphic to A_4.

   (a) Does there exist a quadratic extension $K/\mathbb{Q}$ contained in L?

Solution. By the fundamental theorem of Galois theory, a quadratic extension $K/\mathbb{Q}$ corresponds to a subgroup of $\mathrm{Gal}(L/\mathbb{Q}) \cong A_4$ of index 2 (order 6). We claim that there is no such subgroup, and therefore no such quadratic sub-extension.

Any group of order 6 is isomorphic to either $\mathbb{Z}/6\mathbb{Z}$ or S_3. A_4 consists of double 2-cycles, e.g. (1 2)(3 4), and 3-cycles, e.g. (1 2 3), none of which have order 6, so that leaves S_3. S_3 has three elements of order 2, and since the three double 2-cycles in A_4 are exactly its elements of order 2, they must all lie in any subgroup isomorphic to S_3. However, the elements of order 2 don't commute with one another in S_3 while they do in A_4, so we cannot have a subgroup of A_4 isomorphic to S_3. □

(b) Does there exist a degree 4 polynomial in $\mathbb{Q}[x]$ with splitting field equal to L?

Solution. □

7. Let $A : V \to V$ be a linear transformation of a vector space V over the field $\mathbb{Q}$ which satisfies the relation $(A^3 + 3I)(A^3 - 2I) = 0$. Show that the dimension $\dim_{\mathbb{Q}}(V)$ is divisible by 3.

Proof. Since A satisfies the polynomial $(x^3+3)(x^3-2)$, the minimal polynomial of A over $\mathbb{Q}$ must divide $(x^3 + 3)(x^3 - 2)$. Since $x^3 + 3$ and $x^3 - 2$ are both irreducible over $\mathbb{Q}$ by Eisenstein, the minimal polynomial must be either $x^3 + 3$, $x^3 - 2$ or $(x^3 + 3)(x^3 - 2)$. Furthermore, the minimal polynomial divides the characteristic polynomial whose degree is the dimension of V over $\mathbb{Q}$. Since the minimal polynomial and characteristic polynomial have the same roots in an algebraic closure, we must have that the characteristic polynomial is of the form $(x^3+3)^a(x^3-2)^b$ for some nonnegative integers a, b at least one of which is positive. Since the degree of such a polynomial is divisible by 3, we must have that the dimension of V over $\mathbb{Q}$ is divisible by 3. □

8. True/False.

(a) If K_1, K_2 are fields and $\varphi : K_1 \to K_2$ is a ring homomorphism such that $\varphi(1) = 1$, then φ is injective.

Solution. True. The kernel of φ is an ideal in K_1. Since K_1 is a field its only ideals are (0) and all of K_1. Since $\varphi(1) = 1$, we have that the kernel of φ is not all of K_1, so it must be trivial, forcing φ to be injective. □

(b) The unit group of $\mathbb{C}$ is isomorphic to the additive group of $\mathbb{C}$.

Solution. Assuming "the unit group of $\mathbb{C}$" means the nonzero complex numbers, $\mathbb{C}^\times$, then this is false. $\mathbb{C}^\times$ contains an element of order 2, -1, whereas the additive group $(\mathbb{C}, +)$ contains no elements of order 2. □

(c) Let n be a positive integer. Then $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} = 0$.

Solution. True. For any simple tensor $a \otimes \frac{p}{q}$ in $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}$ we have

$$\begin{aligned} a \otimes \frac{p}{q} &= a \otimes \frac{np}{nq} \\ &= na \otimes \frac{p}{nq} \\ &= 0 \otimes \frac{p}{nq} \\ &= 0. \end{aligned}$$

□

9. For each of the following either give an example or show that none exists.

(a) An element $\alpha \in \mathbb{Q}(\sqrt{2}, i)$ such that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, i)$.

Solution. As this is a finite extension of $\mathbb{Q}$ and since any such extension is separable as $\mathbb{Q}$ is perfect, the primitive element theorem guarantees the existence of such an α. We claim that $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2} + i)$. The inclusion $\mathbb{Q}(\sqrt{2} + i) \subseteq \mathbb{Q}(\sqrt{2}, i)$ is obvious. Note that $(\sqrt{2} + i)^3 = -\sqrt{2} + 5i$. This gives

$$(\sqrt{2} + i)^3 + (\sqrt{2} + i) = 6i,$$

so $i \in \mathbb{Q}(\sqrt{2} + i)$. Subtracting i from $\sqrt{2} + i$ shows that $\sqrt{2} \in \mathbb{Q}(\sqrt{2} + i)$ as well and we have the reverse inclusion. □

(b) A tower of field extensions $L \supseteq K' \supseteq K$ such that L/K' and K'/K are Galois extensions but L/K is not Galois.

Solution. Consider the extensions $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$. Both of these extensions are Galois since they are quadratic. However, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not Galois because it doesn't contain the non-real roots of $x^4 - 2$. □

10. Let $L_1, \ldots, L_r$ be all pairwise non-isomorphic complex irreducible representations of a group G of order 12. What are the possible values for their dimensions $n_i = \dim_{\mathbb{C}} L_i$? For each of the possible answers of the form $(n_1, \ldots, n_r)$ give an example of G which has such irreducible representations.

Solution. We have that $n_1^2 + \cdots + n_r^2 = 12$ and that r is the number of conjugacy classes in G. Since the one-dimensional trivial representation is always a representation of G, we know that at least one of the n_i is 1. We also know that the number of conjugacy classes divides the order of G by Lagrange's theorem. These constraints give us three possible configurations of the n_i:

$$(1,1,1,1,1,1,1,1,1,1,1,1) \quad (1,1,1,1,2,2) \quad (1,1,1,3).$$

Here are some examples from each class.

$(1, \ldots, 1)$: The irreducible representations of an abelian group are all one-dimensional, so a group like $\mathbb{Z}/12\mathbb{Z}$ would fall into this category.

$(1, 1, 1, 1, 2, 2)$: We can safely place the dihedral group D_{12} in this category because it has six conjugacy classes and this is the only configuration of the n_i consistent with this.

$(1, 1, 1, 3)$: The alternating group A_4 is in this category because it has four conjugacy classes.

□

Fall 2015

1. (a) Define **prime ideal**.

   Solution. An ideal $P \neq R$ of the commutative ring R is prime if $ab \in R$ implies that $a \in R$ or $b \in R$. Equivalently, P is prime if and only if R/P is an integral domain. □

   (b) Define **maximal ideal**.

   Solution. An ideal $I \neq R$ of the ring R is maximal if I is not properly contained in another ideal (that isn't all of R). If R is commutative, then I is maximal if and only if R/I is a field. □

   (c) Give an example of a ring R and ideal P_1, P_2, and P_3 of R such that for the properties "prime ideal" and "maximal ideal" of R,

   i. P_1 satisfies both properties,

   ii. P_2 satisfies neither property

   iii. P_3 satisfies one property but not the other.

   Solution. Let $R = \mathbb{Q}[x, y]$. The ideal $P_1 = (x, y)$ is maximal since $R/P_1 = \mathbb{Q}$, which is a field. Since all fields are integral domains, we have that P_1 is prime as well.

   The ideal $P_2 = (x^2)$ is not prime since $x \cdot x$ is in P_2 but x is not. Since maximal ideals are always prime, this shows that P_2 isn't maximal either.

   The ideal $P_3 = (x)$ is prime but not maximal since $R/P_3 = \mathbb{Q}[y]$, which is an integral domain but not a field. □

2. Show that if a group G has only finitely many subgroups then G is a finite group.

Proof. Suppose G is an infinite group. If G has an element g of infinite order then $\langle g \rangle \cong \mathbb{Z}$, which has infinitely many subgroups. Suppose then that every element of G has finite order. Since $G = \cup_{g \in G} \langle g \rangle$ and every $\langle g \rangle$ is a finite set, the only way to cover the infinite set G by finite sets $\langle g \rangle$ is to have infinitely many distinct $\langle g \rangle$. Thus, an infinite group must have infinitely many subgroups, so a group with finitely many subgroups must be finite. □

3. Let A be an $n \times n$ matrix with entires in $\mathbb{R}$ such that $A^2 = -I$.

   (a) Prove that n is even.

   Proof. Since A satisfies the polynomial $x^2 + 1$, its minimal polynomial over $\mathbb{R}$ must divide $x^2 + 1$. This polynomial is irreducible over $\mathbb{R}$ and since the minimal polynomial divides the characteristic polynomial and both polynomials have the same roots in $\mathbb{C}$, the characteristic polynomial must be $(x^2 + 1)^d$ for some $d \geq 1$. The degree of the characteristic polynomial, $2d$, is n, so n is even. □

   (b) Prove that A is diagonalizable over $\mathbb{C}$ and describe the corresponding diagonal matrices.

   Proof. The minimal polynomial of A, x^2+1 splits completely into distinct linear factors over $\mathbb{C}$, $(x+i)(x-i)$, so A is diagonalizable over $\mathbb{C}$. The Jordan blocks of A are all of size 1, so A is similar to a diagonal matrix with an equal number of i's and $-i$'s along the diagonal. □

4. Let G be a group of order 70. Prove that G has a normal subgroup of order 35.

   Proof. Any subgroup of G with order 35 will be normal as it will have index 2. It then suffices to simply show that G has a subgroup of order 35.

   $70 = 2 \cdot 5 \cdot 7$. By Sylow's theorem, the number of Sylow-7 subgroups, n_7 is 1 mod 7 and divides $2 \cdot 5 = 10$. The only possibility is $n_7 = 1$. Similarly we have that $n_5 = 1$ as well. Since the Sylow-p subgroups are conjugate to one another, the fact that we have unique Sylow-5 and Sylow-7 subgroups shows that these subgroups, H and K, are normal in G. Consequently, the product subgroup HK is a subgroup of G with order

   $$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

   Since H and K are cyclic with relatively prime orders they must intersect trivially, so $|HK| = 35$. □

5. Construct a Galois extension F of $\mathbb{Q}$ satisfying $\mathrm{Gal}(F/\mathbb{Q}) \cong D_8$.

Solution. Consider the splitting field of $p(x) = x^4 - 2$ over $\mathbb{Q}$. p has roots $i^k 2^{1/4}$ for $k = 0, 1, 2, 3$, so $F = \mathbb{Q}(2^{1/4}, i)$. $\mathbb{Q}(2^{1/4})$ is a real degree 4 subextension. $[\mathbb{Q}(2^{1/4}, i) : \mathbb{Q}(2^{1/4})] = 2$, so we have that $[\mathbb{Q}(2^{1/4}, i) : \mathbb{Q}] = 8$. Since $\mathrm{Gal}(F/\mathbb{Q})$ is the Galois group of a degree-4 polynomial, it must be a subgroup of S_4. Any order 8 subgroup of S_4 is one of its (all isomorphic) Sylow-2 subgroups. The dihedral group D_8 is an order 8 subgroup of S_4, so we must have that $\mathrm{Gal}(F/\mathbb{Q}) \cong D_8$. □

6. Let F be a field. Prove that every ideal of $F[x]$ is principal.

Proof. Let I be a nonzero proper ideal of $F[x]$ and let a be an element of I of minimal degree. If $\deg a = 0$ then a is a unit, in which case $I = F[x]$. We claim that a divides every element of I, so since (a) is clearly contained in I, we'll have that $I = (a)$. Let b be any element of I. Since F is a field we can perform polynomial division with remainder to obtain unique q and r with $b = aq + r$, where r is either zero or has degree strictly less than that of a. r cannot have degree strictly less than that of a because a was chosen to have minimal degree, so we must have that $r = 0$ and a divides every element of I. □

7. Give an example of a module M over a ring R such that M is not finitely generated as an R-module.

Proof. Any infinitely generated abelian group will do the trick, e.g. $\bigoplus_{\mathbb{N}} \mathbb{Z}$. Abelian groups are $\mathbb{Z}$-modules, so an infinitely generated abelian group is not a finitely generated $\mathbb{Z}$-module.

Suppose $\bigoplus_{\mathbb{N}} \mathbb{Z}$ is finitely generated. Elements of this module are of the form $(a_i)_{i=1}^{\infty}$ where all but finitely many of the a_i are zero. If we could find a finite generating set of this module, there would be some maximal N with a_N nonzero an $a_j = 0$ for all $j > N$ and all generators (a_i). But $\bigoplus_{\mathbb{N}} \mathbb{Z}$ clearly contains elements where $a_j \neq 0$ for $j > N$, so this module cannot be finitely generated. □

8. Suppose H is a normal subgroup of a finite group G.

   (a) Prove or disprove: If H has order 2, then H is a subgroup of the center of G.

   Solution. This is true. Write $H = \{e, h\}$ where $h \neq e$. Since H is normal, ghg^{-1} is in H for all $g \in G$. If $ghg^{-1} = e$ then cancellation forces $h = e$, which isn't true, so we must have $ghg^{-1} = h$, which implies that $gh = hg$ for all g, which puts H in the center of G. □

   (b) Prove or disprove: If H has order 3, then H is a subgroup of the center of G.

   Solution. This is not true. Consider the symmetric group $S_3 = \langle r, s : r^3 = s^2 = e,\ rs = sr^2 \rangle$. The subgroup generated by r has order 3 and is normal since it has index 2 in S_3. However, it is not in the center of S_3 as $rs = sr^2 \neq sr$. □

9. (a) What does it mean for a representation to be irreducible?

Solution. A representation of G is irreducible if it contains no proper subrepresentations, i.e. V is irreducible if there is no proper subspace W of V invariant under G. □

(b) Suppose p is a prime. Let $G = \mathbb{Z}/p\mathbb{Z}$ and let $\rho : G \to \mathrm{GL}_2(\mathbb{F}_p)$ be a representation. Show that ρ is reducible.

Solution. Let V be a subspace of $\mathbb{F}_p^2$ fixed by G. If we let G act on $V \setminus \{0\}$ by ρ, the orbit stabilizer theorem tells us that the size of the orbit $|\mathcal{O}_x|$ divides the order of $\mathbb{Z}/p\mathbb{Z}$, p, for each $x \in V \setminus \{0\}$. The orbits partition $V \setminus 0$, so if we add up the sizes of each orbit we will get the size of $V \setminus \{0\}$, which is $p^n - 1$ for $n = 0$, 1, or 2. Since the size of each orbit is a divisor of p, there must be at least one orbit of size 1, i.e. a vector fixed by the action of G. But then the span of this vector is a subspace of V invariant under G: a proper subrepresentation. □

10. (a) Compute the order of $\mathrm{GL}_4(\mathbb{F}_{3^2})$.

Solution. The first row in an element of $\mathrm{GL}_4(\mathbb{F}_9)$ can be any nonzero vector, of which there are $9^4 - 1$. The second row can be any vector not in the span of the first one, of which there are $9^4 - 9$. Continuing in this fashion, the i-th row can be any vector not in the span of the first $i - 1$ rows, which gives

$$|\mathrm{GL}_4(\mathbb{F}_9)| = (9^4 - 1)(9^4 - 9)(9^4 - 9^2)(9^4 - 9^3).$$

□

(b) Compute the order of $\mathrm{SL}_4(\mathbb{F}_{3^2})$.

Solution. $\mathrm{SL}_4(\mathbb{F}_9)$ is the kernel of the determinant map $\det : \mathrm{GL}_4(\mathbb{F}_9) \to \mathbb{F}_9^\times$. We can construct invertible matrices with any desired nonzero determinant by using diagonal matrices if we like, so this map is surjective. By the first isomorphism theorem we then have

$$\frac{|\mathrm{GL}_4(\mathbb{F}_9)|}{|\mathrm{SL}_4(\mathbb{F}_9)|} = |\mathbb{F}_9^\times|.$$

By part (a) we have

$$|\mathrm{SL}_4(\mathbb{F}_9)| = \frac{1}{8}(9^4 - 1)(9^4 - 9)(9^4 - 9^2)(9^4 - 9^3).$$

□

(c) Show that $\mathbb{Z}[\sqrt{10}]$ is not a UFD.

Solution. Observe that $10 = 2 \cdot 5 = \sqrt{10} \cdot \sqrt{10}$. If we can show that 2, 5, and $\sqrt{10}$ are irreducible in $\mathbb{Z}[\sqrt{10}]$ then we will have exhibited two decompositions of 10 into non-associate irreducible factors.

Define the norm $N(a + b\sqrt{10}) = a^2 - 10b^2$. It's easy to see that $N(\alpha\beta) = N(\alpha)N(\beta)$ and that $N(\alpha) = \pm 1$ if and only if α is a unit. Now $N(2) = 4 = 2^2$. If we can show that there are no elements with norm ± 2 then we will have shown that 2 is irreducible.

Suppose $N(\alpha) = a^2 - 10b^2 = \pm 2$. Reducing mod 4 we have $a^2 + 2b^2 \equiv 2 \pmod 4$. x^2 can only be zero or 1 mod 4, the former if x is even and the latter if x is odd. We conclude that a must be even and b odd. Substitute $a = 2m$ and $b = 2n + 1$ to obtain

$$4m^2 - 10(4n^2 + 4n + 1) = \pm 2$$

$$\iff 4(m^2 - 10n^2 - 10n) - 10 = \pm 2$$

$$\iff m^2 - 10n^2 - 10n = 2 \text{ or } 3.$$

Reducing mod 10 we have $m^2 \equiv 2$ or 3 mod 10, which has no solutions. We conclude that no element of $\mathbb{Z}[\sqrt{10}]$ has norm ± 2, so 2 is irreducible.

Now we'll show that 5 is irreducible. $N(5) = 25 = 5^2$, so let's show that there are no elements with norm ± 5. Reducing $a^2 - 10b^2 = \pm 5$ mod 5 we have that a must be a multiple of 5. Substituting $a = 5m$ and dividing by 5 gives $5m^2 - 2b^2 = \pm 1$. Again, reducing mod 5 we obtain

$$3b^2 \equiv \pm 1 \pmod 5$$

$$\iff b^2 \equiv \pm 3 \pmod 5,$$

which has no solutions. We conclude that no element has norm ± 5, so 5 is irreducible.

Since $N(\sqrt{10}) = -10 = -2 \cdot 5$, we have also shown that $\sqrt{10}$ is irreducible. Thus, the decompositions $10 = 2 \cdot 5 = \sqrt{10} \cdot \sqrt{10}$ are non-associate irreducible decompositions, so $\mathbb{Z}[\sqrt{10}]$ is not a UFD. $\square$