Math 121 Practice Final

(1) Define precisely the following concepts (the emphasis is on the italicized words; for example, for the first question, you do not need to define "module", just "direct sum".) If a concept has multiple uses, you can define any one of them.

- **(a)** The *direct sum* of two modules.
- **(b)** A *bilinear* function;
- **(c)** An *algebraic* extension of fields;
- **(d)** The *Jordan normal form* of a linear transformation;
- **(e)** A *splitting field* for a polynomial f over a field F.

Solution.

- **(a)** A universal property definition: The direct sum of R-modules M_1 and M_2 is an R-module M with R-module homomorphisms $M \to M_1$ and $M \to M_2$ such that for any R-module N with R-module homomorphisms $N \to M_1$ and $N \to M_2$, there exists a unique R-module homomorphism $N \to M$ such that for i in $\{1,2\}$, the compositions $N \to M \to M_i$ and $N \to M_i$ are equal.

  A less intrinsic definition, but needed, for example, to show existence, is that M is the cartesian product $M_1 \times M_2$ with componentwise addition and R-action. This is sometimes called the external direct sum of M_1 and M_2. If each M_i is a submodule of some $\tilde{M}$, then the submodule $M_1 + M_2$ of $\tilde{M}$ is isomorphic to the external direct sum and sometimes called the internal direct sum.
- **(b)** A bilinear function is a mapping from $M \times N$, the cartesian product of R-modules M and N, to an R-module P that is R-linear in each factor.
- **(c)** A field extension K/F is algebraic if every element of K is a root of a nonzero (equivalently monic) element of $F[x]$.
- **(d)** The Jordan normal form of a linear transformation is a block diagonal matrix representing the linear transformation where each of the diagonal blocks is a Jordan block of the form

$$\begin{pmatrix} \lambda & 1 & & & \\ & \lambda & \ddots & & \\ & & \ddots & 1 & \\ & & & \lambda & 1 \\ & & & & \lambda \end{pmatrix}.$$

(e) A splitting field for a polynomial f over a field F is a field extension K of F minimal with respect to the property that f factors into linear factors (splits completely) over K. □

(3) For any R-module M, we shall say an element $s \in R$ is *invertible on* M if the map $M \to M$ given by $x \mapsto sx$ is bijective. Prove that, for any submodule N,

$$s \text{ invertible on } N \text{ and } M/N \implies s \text{ invertible on } M$$

Solution. Assume that s is invertible on N and M/N. Let m in M be such that $sm = 0$. Then $s(m+N) = sm + N = 0 + N$, but s is injective on M/N so $m + N = 0 + N$, that is m is in N. Since s is injective on N, this implies that $m = 0$. Therefore s is injective on M. Let m' be an element of M. Since s is surjective on M/N, there exists an element, say $m'' + N$, of M/N such that $sm'' + N = m' + N$. Then $s(m'') - m'$ is in N. Since s is surjective on N, there exists n in N such that $sn = s(m'') - m'$. Then $m' = s(m'') - sn = s(m'' - n)$ so s is surjective on M. Finally, s is invertible on M. □

(4) Prove that $\mathbf{Q} \otimes_{\mathbf{Z}} A$ is zero for any finite abelian group A. Prove that, for any nonzero $\mathbf{Q}$-module V, $V \otimes_{\mathbf{Q}} V$ is nonzero.

Solution. If A is a finite abelian group, say with cardinality n, then for any q in $\mathbf{Q}$ and any a in A, the simple tensor $q \otimes a$ is zero because

$$q \otimes a = n(q/n) \otimes a = (q/n) \otimes (na) = (q/n) \otimes 0 = 0,$$

but the tensor product $\mathbf{Q} \otimes_{\mathbf{Z}} A$ is generated by simple tensors and hence must be zero.

Let V be a nonzero vector space, say containing a nonzero v. Then there exists ℓ in V^* not killing v. The map $\ell \otimes \ell \colon V \otimes_{\mathbf{Q}} V \to \mathbf{Q} \otimes_{\mathbf{Q}} \mathbf{Q} = \mathbf{Q}$ sends $v \otimes v$ to a $\ell(v)^2$, which is nonzero, so $V \otimes_{\mathbf{Q}} V$ contains the nonzero vector $v \otimes v$ and hence is nonzero. □

(5) Let V be a finite-dimensional vector space over the real numbers, and $J \in \mathrm{Hom}(V, V)$ with the property that $J^2 = -1$. Prove that the rule

$$(a + b\mathrm{i})v = av + bJ(v) \qquad a, b \in \mathbf{R}$$

makes V a module over the complex numbers. Using this, prove that the dimension of V is even.

Solution. For $a_1 + b_1\mathrm{i}$ and $a_2 + b_2\mathrm{i}$ in $\mathbf{C}$ and v in V,

$$\begin{aligned}(a_1 + b_1\mathrm{i} + a_2 + b_2\mathrm{i})v &= (a_1 + a_2 + (b_1 + b_2)\mathrm{i})v \\ &= (a_1 + a_2)v + (b_1 + b_2)J(v) \\ &= a_1v + a_2v + b_1J(v) + v_2J(v) \\ &= a_1v + b_1J(v) + a_2v + b_2J(v) \\ &= (a_1 + b_1\mathrm{i})v + (a_2 + b_2\mathrm{i})v\end{aligned}$$

and

$$\begin{aligned}(a_2 + b_2\mathrm{i})((a_1 + b_1\mathrm{i})v) &= (a_2 + b_2\mathrm{i})(a_1v + b_1J(v)) \\ &= a_2(a_1v + b_1J(v)) + b_2J(a_1v + b_1J(v)) \\ &= a_2(a_1v + b_1J(v)) + b_2(a_1J(v) + b_1J^2(v)) \\ &= (a_2a_1 - b_2b_1) + (a_2b_1 + b_2a_1)J(v) \\ &= ((a_2a_1 - b_2b_1) + (a_2b_1 + b_2a_1)\mathrm{i})v \\ &= ((a_2 + b_2\mathrm{i})(a_1 + b_1\mathrm{i}))v.\end{aligned}$$

For $a + b\mathrm{i}$ in $\mathbf{C}$ and v_1 and v_2 in V,

$$\begin{aligned}(a + b\mathrm{i})(v_1 + v_2) &= a(v_1 + v_2) + bJ(v_1 + v_2) \\ &= av_1 + av_2 + bJ(v_1) + bJ(v_2) \\ &= av_1 + bJ(v_1) + av_2 + bJ(v_2) \\ &= (a + b\mathrm{i})v_1 + (a + b\mathrm{i})v_2.\end{aligned}$$

Also for any v in V, $(1 + 0\mathrm{i})v = v$.

Therefore $(a + b\mathrm{i})v = av + bJ(v)$ defines a $\mathbf{C}$-module structure on V. For all v in V, $(1+0\mathrm{i})v = v+0J(v) = v$, so the restriction of scalars via $\mathbf{R} \hookrightarrow \mathbf{C}$ of the $\mathbf{C}$-module V just defined is the original $\mathbf{R}$-module V.

Assume M is a free R-module on $\{m_i\}$ and R is an S-algebra (An S-algebra R is a ring homomorphism $S \to R$ making R into an S-module by restriction of scalars from the natural R-module structure on R.) that is free on $\{r_i\}$. Any m in M can be written as $m = \sum c_jm_j$ for c_i in R, but for each j we have $c_j = \sum d_{ij}r_i$ for some d_{ij} in S so

$$m = \sum d_{ij}r_im_j.$$

Therefore $\{r_im_j\}$ spans M as an S-module. Now assume d_{ij} are elements of S and $\sum d_{ij}r_im_j = 0$. Then $\sum c_jm_j = 0$ where $c_j = \sum_i d_{ij}r_i$ so $c_j = 0$ for each j. Consequently $d_{ij} = 0$ for all i and j. Thus M is a free S-module on $\{r_im_j\}$. In particular $\operatorname{rank}_S M = \operatorname{rank}_R M \times \operatorname{rank}_S R$.

The **R**-dimension of V must then be even since V is obtained by restriction of scalars from a **C**-vector space and **C** is 2-dimensional as an **R**-vector space. □

(6) Let X, Y be finite-dimensional vector spaces over F, $x, x' \in X$, $y, y' \in Y$. Prove that $x \otimes y = x' \otimes y'$ (equality inside $X \otimes Y$) if and only if there exists a scalar α so $\alpha x = x', y = \alpha y'$ or $x \otimes y = x' \otimes y' = 0$.[1]

Solution. If $x \otimes y = x' \otimes y' = 0$ then in particular $x \otimes y = x' \otimes y'$ and if there exists a scalar α so that $\alpha x = x', y = \alpha y'$, then

$$x \otimes y = x \otimes (\alpha y') = (\alpha x) \otimes y' = x' \otimes y'.$$

We now prove the inverse. Assume that one of $x \otimes y$ or $x' \otimes y'$ is nonzero. If any of x, y, x' or y' is zero, then one of $x \otimes y$ or $x' \otimes y'$ vanishes, but by assumption they don't both vanish so $x \otimes y \neq x' \otimes y'$. Thus we may assume that x, y, x' and y' are nonzero. Assume first that there does not exist a scalar α so that $\alpha x = x'$. Then x and x' are independent so there exists a functional ℓ_1 in X^* so that $\ell_1(x) = 0$ and $\ell_1(x') \neq 0$. Choose a functional ℓ_2 in Y^* so that $\ell_2(y') \neq 0$. Then $\ell_1 \otimes \ell_2 \colon X \otimes Y \to F \otimes F = F$ kills $x \otimes y$, but does not kill $x' \otimes y'$ so the two elements of $X \otimes Y$ are distinct. Similarly, if there does not exist a scalar α so that $y = \alpha y'$, then $x \otimes y$ and $x' \otimes y'$ are distinct elements of $X \otimes Y$. Finally assume that there exist distinct scalars β and γ so that $\beta x = x'$ and $y = \gamma y'$. Necessarily β and γ are nonzero. Then

$$\beta x \otimes y = \gamma x' \otimes y'$$

but $\beta \neq \gamma$ and both of $x \otimes y$ and $x' \otimes y'$ are nonzero, since at least one is nonzero, so $x \otimes y \neq x' \otimes y'$. This completes the proof. □

(7) Let V, W be vector spaces with subspaces $U \subseteq V, S \subseteq W$.

- **(a)** Prove that the set of $T \in \mathrm{Hom}(V, W)$ for which $U \subseteq \mathrm{Ker}(T)$ and $\mathrm{Im}(T) \subseteq S$ is a linear subspace. What is its dimension.
- **(b)** Define T^* and state, with proof, the relation between the dimensions of $\mathrm{Ker}(T)$ and $\mathrm{Ker}(T^*)$.

[1] This question is from the practice midterm, but the statement has been clarified by including the necessary phrase "or $x \otimes y = x' \otimes y' = 0$". The solution provided for the practice midterm is incorrect; it does not provide a proof of the false, as stated, result of the practice midterm because it uses this condition in order to "Choose a functional ℓ_2 in Y^* so that $\ell_2(y') \neq 0$."

Solution.

(a) Precomposition with the projection $V \twoheadrightarrow V/U$ and postcomposition with the inclusion $S \hookrightarrow W$ gives a linear map

$$\mathrm{Hom}(V/U, S) \to \mathrm{Hom}(V, W)$$

that maps injectively onto

$$\{T \in \mathrm{Hom}(V, W) \mid U \subseteq \mathrm{Ker}(T) \text{ and } \mathrm{Im}(T) \subseteq S\},$$

Composing with the projection $V \twoheadrightarrow V/U$ gives an injective linear map

$$\mathrm{Hom}(V/U, Y) \to \mathrm{Hom}(V, Y)$$

onto the subspace of $\mathrm{Hom}(V, Y)$ consisting of the maps $V \to Y$ with kernel containing U. Composing with the inclusion $S \hookrightarrow W$ gives an injective linear map

$$\mathrm{Hom}(X, S) \to \mathrm{Hom}(X, W)$$

onto the subspace of $\mathrm{Hom}(X, W)$ consisting of the maps $X \to W$ with image contained in S.

which must be a subspace, being the image of a linear map.

Alternatively, directly prove the subspace properties using

$$\mathrm{Ker}\, T_1 \cap \mathrm{Ker}\, T_2 \subseteq \mathrm{Ker}(T_1 + T_2) \qquad \text{and} \qquad \mathrm{Ker}\, T \subseteq \mathrm{Ker}\, cT$$

and

$$\mathrm{Im}(T_1 + T_2) \subseteq \mathrm{Im}\, T_1 + \mathrm{Im}\, T_2 \qquad \text{and} \qquad \mathrm{Im}\, cT \subseteq \mathrm{Im}\, T.$$

Then

$$\{T \in \mathrm{Hom}(V, W) \mid U \subseteq \mathrm{Ker}(T) \text{ and } \mathrm{Im}(T) \subseteq S\}$$

is a subspace of $\mathrm{Hom}(V, W)$ of the same dimension

$$\dim(V/U)\dim(S) = (\dim V - \dim U)\dim(S)$$

as $\mathrm{Hom}(V/U, S)$.

(b) Write F for the base field. The dual of T^* is the linear map

$$T^* = \mathrm{Hom}(T, F) \colon W^* = \mathrm{Hom}(W, F) \to V^* = \mathrm{Hom}(V, F)$$

defined as precomposition with T. Note that

$$\mathrm{Ker}(T^*) = \{\ell \in W^* \mid \mathrm{Ker}\, \ell \supseteq \mathrm{Im}(T) = 0\},$$

and by part (a) the latter set is a subspace of $W^* = \mathrm{Hom}(W, F)$ of dimension

$$\dim(W/\mathrm{Im}(T))\dim(F) = \dim W - \dim \mathrm{Im}(T),$$

but we can rewrite this using the rank-nullity theorem as

$$\dim W - \dim V + \dim \operatorname{Ker} T.$$

Finally using $\dim W^* = \dim W$ we have the relation

$$\dim V - \dim \operatorname{Ker} T = \dim W^* - \dim \operatorname{Ker}(T^*).$$

The form of the solution above suggests an alternative solution. The ranks of T and T^* coincide (equivalently the row and column ranks of a matrix are equal). The rank-nullity theorem applied to both T and T^* then gives the result obtained above.

Constructing the linear map used in the proof of part (a) and applying it to part (b) gives $\operatorname{Ker}(T^*) \cong (\operatorname{Coker}(T))^*$, which provides an alternative (although essentially the same as the first) solution and illustrates the duality between Ker and Coker.

□

(8) Compute the Jordan normal form of $\begin{pmatrix} 5 & 1 & 0 \\ -9 & -1 & 0 \\ -6 & -4 & -1 \end{pmatrix}$.

Solution. The characteristic polynomial

$$\det \begin{pmatrix} \lambda-5 & -1 & 0 \\ 9 & \lambda+1 & 0 \\ 6 & 4 & \lambda+1 \end{pmatrix} = (\lambda+1)(\lambda^2-4\lambda+4) = (\lambda+1)(\lambda-2)(\lambda-2)$$

has roots $-1, 2, 2$ with multiplicity. The minimal polynomial must have the roots -1 and 2 and divide the characteristic polynomial so there are only two possibilities: $(\lambda+1)(\lambda-2)$ and $(\lambda+1)(\lambda-2)(\lambda-2)$. Since

$$\left(\begin{pmatrix} 5 & 1 & 0 \\ -9 & -1 & 0 \\ -6 & -4 & -1 \end{pmatrix} + \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right)\left(\begin{pmatrix} 5 & 1 & 0 \\ -9 & -1 & 0 \\ -6 & -4 & -1 \end{pmatrix} + \begin{pmatrix} -2 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -2 \end{pmatrix}\right)$$
$$= \begin{pmatrix} 6 & 1 & 0 \\ -9 & 0 & 0 \\ -6 & -4 & 0 \end{pmatrix}\begin{pmatrix} 3 & 1 & 0 \\ -9 & -3 & 0 \\ -6 & -4 & -3 \end{pmatrix}$$

is not zero, the minimal polynomial is $(\lambda+1)(\lambda-2)(\lambda-2)$. The single invariant factor is then $(\lambda+1)(\lambda-2)(\lambda-2)$ so the elementary divisors are $\lambda+1$ and $(\lambda-2)^2$. Finally, the Jordan normal form is

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}.$$

□

(9) Let M be a finitely generated $\mathbf{Z}$-module and $N \subseteq M$ a submodule.

- Give an example to show that M is not necessarily isomorphic to $N \oplus M/N$.
- Assume that $N \otimes_{\mathbf{Z}} M/N$ is trivial. Show that M is isomorphic to $N \oplus M/N$. (Hint: Use the classification theorem for finitely generated modules.)

Solution.

- If $M = \mathbf{Z}/4\mathbf{Z}$ and N is the unique submodule isomorphic to $\mathbf{Z}/2\mathbf{Z}$, then $N \oplus M/N$ is isomorphic to $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/2\mathbf{Z})$, which is not isomorphic to $\mathbf{Z}/4\mathbf{Z}$.
- Since $\mathbf{Z}$ is a principal ideal domain, the finitely generated modules N and M/N may be written as

  $$\mathrm{Tor}(N) \oplus \mathbf{Z}^{\mathrm{rank}(N)} \qquad \text{and} \qquad \mathrm{Tor}(M/N) \oplus \mathbf{Z}^{\mathrm{rank}(M/N)},$$

  respectively. Then since direct sum commutes with tensor product, $N \oplus M/N$ is isomorphic to

  $$\begin{aligned}(\mathrm{Tor}(N) \otimes_{\mathbf{Z}} \mathbf{Z}^{\mathrm{rank}(M/N)}) \oplus (\mathbf{Z}^{\mathrm{rank}(N)} \otimes_{\mathbf{Z}} \mathrm{Tor}(M/N)) \\ \oplus (\mathrm{Tor}(N) \otimes_{\mathbf{Z}} \mathrm{Tor}(M/N))) \oplus (\mathbf{Z}^{\mathrm{rank}(N)} \otimes_{\mathbf{Z}} \mathbf{Z}^{\mathrm{rank}(M/N)})),\end{aligned}$$

  which in turn is isomorphic to

  $$(\mathrm{Tor}(N) \otimes_{\mathbf{Z}} \mathrm{Tor}(M/N))) \oplus \mathbf{Z}^{\mathrm{rank}(N)\,\mathrm{rank}(M/N)}.$$

  Since $N \otimes_{\mathbf{Z}} M/N$ is trivial by assumption, $\mathrm{Tor}(N) \otimes_{\mathbf{Z}} \mathrm{Tor}(M/N))$ is trivial and either $\mathrm{rank}(N) = 0$ or $\mathrm{rank}(M/N) = 0$.

  Let $e_1 \mid e_2 \mid \cdots \mid e_r$ be the elementary divisors of M and let $f_1 \mid f_2 \mid \cdots \mid f_s$ be the elementary divisors of N. Then

  $$\mathrm{Tor}(N) \otimes_{\mathbf{Z}} \mathrm{Tor}(M/N) \cong \bigoplus (\mathbf{Z}/e_i\mathbf{Z}) \otimes_{\mathbf{Z}} (\mathbf{Z}/f_j\mathbf{Z}) \cong \bigoplus \mathbf{Z}/\gcd(e_i, f_j)\mathbf{Z}$$

  so e_r and f_s are relatively prime. Choose u and v in $\mathbf{Z}$ so that $ue_r + vf_s = 1$. For any m in M, $m = ue_rm + vf_sm$. Assume m in M is torsion. Then $m + N$ is also torsion, in fact f_s torsion, so $f_sm + N = f_s(m + N) = 0 + N$. Thus f_sm is in N and in particular e_r torsion. Therefore $e_rf_sm = 0$. Consequently $m = ue_rm + vf_sm$ decomposes m into the sum of an e_r torsion element vf_sm and an f_s torsion element ue_rm.

  For a an integer, write $\mathrm{Tor}_a(-)$ for the a torsion elements. We have shown that $\mathrm{Tor}(M) = \mathrm{Tor}_{e_r}(M) + \mathrm{Tor}_{f_s}(M)$, but if for some m in $\mathrm{Tor}(M)$ we have $e_rm = 0$ and $f_sm = 0$, then $m = ue_rm + vf_sm = 0$ so in fact $\mathrm{Tor}(M) = \mathrm{Tor}_{e_r}(M) \oplus \mathrm{Tor}_{f_s}(M)$. Then

  $$M \cong \mathrm{Tor}_{e_r}(M) \oplus \mathrm{Tor}_{f_s}(M) \oplus \mathbf{Z}^{\mathrm{rank}(M)}.$$

  The submodule $\mathrm{Tor}(N) \subseteq \mathrm{Tor}(M)$ consists of e_r torsion elements. Conversely, if m is an e_r torsion element of $\mathrm{Tor}(M)$, then $m = ue_rm + vf_sm = vf_sm$ goes to zero under $M \to M/N$, since M/N is f_s torsion, so m is in N. We have therefore proved that $\mathrm{Tor}(N) = \mathrm{Tor}_{e_r}(M)$. Either $\mathrm{rank}(N) = 0$ or $\mathrm{rank}(M/N) = 0$, so $\mathrm{rank}(N) = \mathrm{rank}(M)$, and in either case N is a direct summand of M, that is there exists a projection $M \to M$ onto N (a

linear map whose image is N and whose square is itself) and we may define $p_1 : M \to N$ to be the restriction of this map.

As is the case with any projection map, p_1 must restrict to the identity on its image N since if n is in N, say $n = p_1(n')$, then $p_1(n) = p_1(p_1(n')) = p_1^2(n') = p_1(n') = n$.

Next, define $p_2 : M \to M/N$ as the projection. Then the map $M \to N \oplus M/N$ defined by $m \mapsto (p_1(m), p_2(m))$ is injective since if $p_1(m) = p_2(m) = 0$ then $m + N = 0 + N$ so m is in N and thus $m = p_1(m) = 0$. Also any $(n, m+N)$ in $N \oplus M/N$ is the image of $m - p_1(m) + n$ so $M \to N \oplus M/N$ is an isomorphism. □

(10) Prove that there exists a field of size 16. Prove that any finite field has order p^d, where p is a prime and d is an integer.

Solution. The only quadratic polynomial over $\mathbf{F}_2$ without roots, and hence the only irreducible quadratic polynomial over $\mathbf{F}_2$, is $x^2 + x + 1$. Therefore the only reducible quartic polynomial over $\mathbf{F}_2$ without a root is

$$(x^2 + x + 1)(x^2 + x + 1) = x^4 + x^2 + 1.$$

In particular the quartic polynomial $x^4 + x + 1$ with no roots in $\mathbf{F}_2$ is irreducible. Therefore $\mathbf{F}_2[x]/(x^4 + x + 1)$ is a degree 4 field extension of $\mathbf{F}_2$, and hence a field of order $2^4 = 16$.

Let F be a finite field. Then the unique ring homomorphism $\mathbf{Z} \to F$ is not injective. Since $\mathbf{Z}$ is a principal ideal domain, we may let $n > 0$ be a generator for the kernel. The induced inclusion $\mathbf{Z}/n\mathbf{Z} \to F$ shows that $\mathbf{Z}/n\mathbf{Z}$ is a subring of a field, that is a domain. Therefore $n\mathbf{Z}$ is a prime ideal in $\mathbf{Z}$ and so n is some prime p. Let d be the degree of F over $\mathbf{F}_p$, the image of $\mathbf{Z}$ in F. Then F is of order p^d. □

(11) Let $f = (x^2 + 3)(x^2 - 5)$. Describe a splitting field L for f over $\mathbf{Q}$ and compute its Galois group. Describe all subfields of L and what they correspond to under the Galois correspondence.

Solution. Note that f splits completely in $\mathbf{Q}(\sqrt{5}, \sqrt{-3})$ as

$$f(x) = (x + \sqrt{-3})(x - \sqrt{-3})(x + \sqrt{5})(x - \sqrt{5})$$

so the only subfield of $\mathbf{Q}(\sqrt{5}, \sqrt{-3})$ in which f splits completely is $\mathbf{Q}(\sqrt{5}, \sqrt{-3})$ itself, that is, $L = \mathbf{Q}(\sqrt{5}, \sqrt{-3})$ is a splitting field of f.

There are two extensions of the identity of $\mathbf{Q}$ to an automorphism of $\mathbf{Q}(\sqrt{5})$ since $\sqrt{5}$ may be sent to either root $\sqrt{5}$ or $-\sqrt{5}$ of the minimal

polynomial $x^2 - 5$ for $\sqrt{5}$ over $\mathbf{Q}$:

$$\begin{array}{ccc} \mathbf{Q}(\sqrt{5}) & \dashrightarrow & \mathbf{Q}(\sqrt{5}) \\ \uparrow & & \uparrow \\ \mathbf{Q} & \xrightarrow[\mathbb{1}_{\mathbf{Q}}]{} & \mathbf{Q}. \end{array}$$

For any real number α, $\alpha^2 + 3 \geq 3$ so $x^2 + 3$ has no roots in $\mathbf{R}$ and hence no roots in the subfield $\mathbf{Q}(\sqrt{5})$. Thus $x^2 + 3$ is the minimal polynomial for $\sqrt{-3}$ over $\mathbf{Q}(\sqrt{5})$. Each of the two elements of $\mathrm{Aut}(\mathbf{Q}(\sqrt{5})/\mathbf{Q})$ send $x^2 + 3$ to itself so for any tower of extensions

$$\begin{array}{ccc} \mathbf{Q}(\sqrt{5}, \sqrt{-3}) & \dashrightarrow & \mathbf{Q}(\sqrt{5}, \sqrt{-3}) \\ \uparrow & & \uparrow \\ \mathbf{Q}(\sqrt{5}) & \longrightarrow & \mathbf{Q}(\sqrt{5}) \\ \uparrow & & \uparrow \\ \mathbf{Q} & \xrightarrow[\mathbb{1}_{\mathbf{Q}}]{} & \mathbf{Q} \end{array}$$

the top map can send $\sqrt{-3}$ to either $\sqrt{-3}$ or $-\sqrt{-3}$.[2] Therefore an automorphism of $\mathbf{Q}(\sqrt{5}, \sqrt{-3})$ over $\mathbf{Q}$ can send $\sqrt{5}$ to $\pm\sqrt{5}$ and $\sqrt{-3}$ to $\pm\sqrt{-3}$ independently. The Galois[3] group of $L = \mathbf{Q}(\sqrt{5}, \sqrt{-3})$ over $\mathbf{Q}$ is thus isomorphic to $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$ and is generated by

$$\sigma\colon \begin{cases} \sqrt{5} \mapsto \sqrt{5} \\ \sqrt{-3} \mapsto -\sqrt{-3} \end{cases}$$

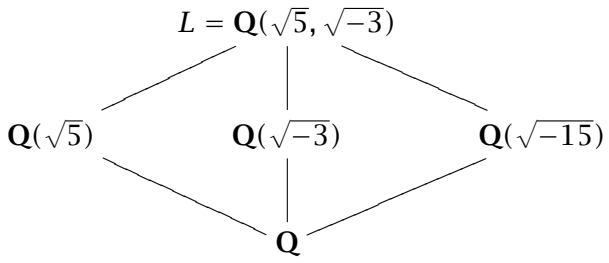
$$\tau\colon \begin{cases} \sqrt{5} \mapsto -\sqrt{5} \\ \sqrt{-3} \mapsto \sqrt{-3}. \end{cases}$$

There are 3 proper subgroups of $\mathrm{Aut}(L/\mathbf{Q})$ (corresponding to the 3 one dimensional subspaces of $\mathbf{F}_2^2$ over $\mathbf{F}_2$), namely the subgroups $\langle\sigma\rangle$, $\langle\tau\rangle$,

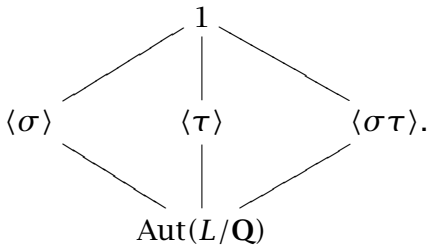
[2] In general, an automorphism of $F(\alpha, \beta)$ over some automorphism of $F(\alpha)$ may send β to an element that is not a root of its minimal polynomial over $F(\alpha)$ because the actual requirement is that β goes to a root of the image of its minimal polynomial under the automorphism of $F(\alpha)$. For example, take $F = \mathbf{Q}$, $\alpha = \sqrt{5}$ and $\beta = \zeta_5 = e^{2\pi i/5}$ (or more generally $\alpha = \sqrt{(-1)^{(p-1)/2}p}$ and $\beta = \zeta_p$ a primitive pth root of unity for p an odd prime). Then $e^{2\pi i/5}$ has minimal polynomial $x^2 + \frac{1-\sqrt{5}}{2}x + 1$ over $\mathbf{Q}(\sqrt{5})$ and so an extension to $\mathbf{Q}(\sqrt{5}, e^{2\pi i/5})$ of the nontrivial automorphism of $\mathbf{Q}(\sqrt{5})$ must send $e^{2\pi i/5}$ to a root of $x^2 + \frac{1+\sqrt{5}}{2}x + 1$ instead of a root of $x^2 + \frac{1-\sqrt{5}}{2}x + 1$.

[3] The extension $L/\mathbf{Q}$ is Galois because a splitting field of a separable (in characteristic 0 every irreducible polynomial is separable) polynomial.

$\langle \sigma\tau \rangle$. Note that $\langle \sigma \rangle$ fixes $\mathbf{Q}(\sqrt{5})$, but $\mathbf{Q}(\sqrt{5})$ has degree 2 over $\mathbf{Q}$, which equals the index of $\langle \sigma \rangle$ in $\mathrm{Aut}(L/\mathbf{Q})$ so $\mathbf{Q}(\sqrt{5})$ is all of the fixed field of $\langle \sigma \rangle$. Similarly the fixed field of $\langle \tau \rangle$ is $\mathbf{Q}(\sqrt{-3})$ and the fixed field of $\langle \sigma \rangle$ is $\mathbf{Q}(\sqrt{-15})$. The fixed field of the trivial subgroup of $\mathrm{Aut}(L/\mathbf{Q})$ is all of L and the fixed field of $\mathrm{Aut}(L/\mathbf{Q})$ is $\mathbf{Q}$. We have describe the 5 subfields of L (containing $\mathbf{Q}$, but every subfield of L contains the prime subfield $\mathbf{Q}$ of L). The lattice of subgroups and corresponding lattice of field extensions are



and



□