Corrections to the Text and Hints and Answers to Problems

July 27, 2012

1 Corrections to the text distributed at the CIMPA School.

These corrections have been made in the posted version.

1. page 3, line 14: \( u(n) = (-1)^n(n - 1) \Rightarrow u(n) = (-1)^n(n - 1)! \)

2. page 4, line -5: varieites \( \Rightarrow \) varieties

3. page 5, line 12: readical \( \Rightarrow \) radical

4. page 7, line -2: continuos \( \Rightarrow \) continuous

5. page 9, line -10: Problem 2.2 should be: Show that any two non-empty \( k \)-open sets have a non-empty intersection

6. page 14, line -9: a finite, solvable subgroup \( \Rightarrow \) a finite subgroup (Note that a subgroup of \( T_n \) is always solvable.)

7. page 24, Proposition 5.6. This contains an incorrect statement and should be replaced by the following (Example 5.7 immediately following the statement of the original Prop. 5.6 gives a counterexample). Here is the correct version

**Proposition 5.6.** Let \( k = C, \sigma = \text{identity or } k = C(x), \sigma(x) = x + 1 \) and let \( R = k[Z, 1/\text{det}(Z)] \) be a PV extension of \( k \) with PV group \( \text{Gal}_\sigma(R/k) = G \). Then

(a) there exists a \( B \in \text{GL}_n(k) \) such that \( BZ \in G(k) \) and the map \( Z \mapsto BZ \) yields an isomorphism of \( R \) onto \( \mathcal{O}_k(G) \), and

(b) \( G/G^0 \) is cyclic and \( R = \bigoplus_{i=0}^{t-1} R_i \) where \( t = \left| G/G^0 \right| \) and \( R_i \simeq \mathcal{O}_k(G^0) \).

8. page 34, line 9: There is a missing “-1”. The ideal should be

\[ I = \langle Y_{1,2} - Y_{2,1}, Y_{2,2} - Y_{1,2}, (Y_{1,1}Y_{2,2} - Y_{1,2}^2)^2 - 1 \rangle. \]
2 Hints and Answers to Problems

2.1 Problems of Chapter 2

2.1 Let $k = \mathbb{Q}$ and for each $i \in \mathbb{Z}$, let $V_i = \{i\}$. Each $V_i$ is $k$-closed, but $\bigcup_{i \in \mathbb{Z}} V_i = \mathbb{Z}$ is not $k$-closed. The reason for this is that if a polynomial $p(x) \in \mathbb{Q}[x]$ vanishes on all $V_i$ then it must be identically 0 and so would vanish everywhere.

2.2 From the definition of $k$-closed, one sees that a set $O \subset \bar{k}^m$ is open if there exists a set of polynomials $\{f_i\}_{i \in I} \subset k[X_1, \ldots, x_m]$ such that $O = \{v \in \bar{k}^m | f_i(v) \neq 0 \text{ for some } i \in I\}$. We say the $\{f_i\}_{i \in I}$ defines $O$. Let $O_1$ be defined by $\{f_i\}_{i \in I}$ and $O_2$ be defined by $\{g_j\}_{j \in J}$. Since they are both nonempty, some $f_i$ and some $g_j$ are not the zero polynomial. Since $\bar{k}$ is infinite, there is an element $v \in \bar{k}^m$ such that $f_i \cdot g_j(v) \neq 0$. This $v$ belongs to $O_1 \cap O_2$.

2.3 Let $V$ be a $k$-variety, so $V = V(I)$ for some ideal $I \subset k[X_1, \ldots, x_m]$. We begin by showing $V \subset V(I_k(V))$. If $v \in V$, then all the elements of $I_k(V)$ vanish at $v$ (by the definition of $I_k(V)$). Therefore $V(I_k(V))$. Now assume that $v \in V(I_k(V))$. Then any polynomial that vanishes on all of $V$ must vanish at $v$. But the elements of $I$ vanish on the elements of $V$ (this is how $V$ is defined), so the elements of $I$ vanish at $v$. So $v \in V(I) = V$.

2.4 (ii) Let $V_1 \supset V_2 \supset \ldots$. We then have $I_k(V_1) \subset I_k(V_2) \subset \ldots$. Therefore by part (i), we have $I_k(V_s) = I_k(V_{s+1}) = \ldots$ for some $s$. From Problem 2.3, we then have that $V_s = V(I_k(V_s)) = V(I_k(V_{s+1})) = \ldots$

(iii) Let $V_1 \in \{V_i\}_{i \in I}$. If $V_1$ is not minimal there is a $V_2 \in \{V_i\}_{i \in I}$ such that $V_1 \supset V_2$. By part (ii) we cannot continue indefinitely so after a finite number of steps we find a $V_j \in \{V_i\}_{i \in I}$ which is minimal.

2.5 (i) This part of Corollary 2.18 follows from Corollary 2.16 in the following way. We have

$$V(I) = V_1 \cup \ldots \cup V_n$$

as in Corollary 2.16. We then have that $I_k(V(I)) = I_k(V_1) \cap \ldots \cap I_k(V_n)$. Since $I$ is already radical, $I_k(V(I)) = I$ by the Hilbert Nullstellensatz. Lemma 2.13 implies that each of the $I_k(V_j)$ are prime. The rest of (i) follows in a similar way.

(ii) Let $R$ be a ring finitely generated over a field $k$. We may write $R = k[x_1, \ldots, x_m]$. Let $k[X_1, \ldots, x_m]$ be the polynomial ring in $m$ variables and $\Phi : k[X_1, \ldots, X_m] \to k[x_1, \ldots, x_m]$ be the homomorphism defined by $\Phi(X_i) = x_i$. If $I$ is a radical ideal of $R$, then $\Phi^{-1}(I)$ is a radical ideal of $k[X_1, \ldots, X_m]$. Apply part (i) to this ideal and write $\Phi^{-1}(I) = P_1 \cap \ldots \cap P_n$. We then have $I = \Phi(P_1) \cap \ldots \cap \Phi(P_n)$.

2.6 As mentioned above, $k$-open sets in $\bar{k}^m$ are of the form $\bigcup_{i \in I} \{v \in \bar{k}^m | p_i(v) \neq 0\}$ where $\{p_i\}_{i \in I}$ is a set of polynomials in $k[X_1, \ldots, X_m]$. There it is enough to show that if
2.2 Problems for Chapter 3

2.7 The coordinate ring of $V$ is $k[X_1, \ldots, X_m]/I_k(V)$. This is an integral domain if and only if $I_k(V)$ is a prime ideal. On the other hand, $I_k(V)$ is a prime ideal if and only if $V$ is $k$-irreducible by Lemma 2.13.

2.2 Problems for Chapter 3

3.1 Let $g \in X$ and assume $e \in X$. The map $x \mapsto gx$ is a homeomorphism of $G$ to $G$ that takes $X$ into $X$. Therefore $gX$ is a closed subset of $X$. Iterating the map, we have $X \supset gX \supset g^2X \supset \ldots$. We cannot have an infinite descending chain of such subsets, so for some $s$, we have $g^sX = g^{s+1}X$. Since $e \in X$, we have $g^s e = g^{s+1}a$ for some $a \in X$. Since $G$ is a group, this implies that $e = ga$, so $X$ is closed under inverse and must be a group.

One can modify this argument when we do not assume $e \in X$. As above one can show $g^sX = g^{s+1}X$ for some $s$. This implies also that $g^sX = g^{s+2}X$, so $g^{s+2} \cdot a = g^s \cdot g$ for some $a \in X$. Therefore $g \cdot a = e$, so $e \in X$ and $X$ contains the inverse of each element of $X$.

3.2 Let $h \in N$. The map $c_h : G \to N$ defined by $g \mapsto gxg^{-1}$ is a continuous map from a connected set to a finite set. Each point of a finite set is closed ($v = (v_1, \ldots, v_m)$ is the unique zero of $\{X_1 - v_1, \ldots, X_m - v_m\}$) so each element of a finite set is one of the components of that set. The image of $G$ under the map $c_h$ is irreducible so must equal on of these points. Since $c_h(e) = e$, we have $c_h(G) = e$. This means $ghg^{-1} = h$ for all $g \in G$ so $h \in Z(G)$.

3.3 This is a long computation. One must show each of these sets is a group, normal in the previous set such that the quotients are abelian. To show the quotients are abelian, one should show that if $g, h$ are in one set then $ghg^{-1}h^{-1}$ is in the next set. Again this is a computation.

3.4 (a) If $A^n = e$ then $A$ satisfies $X^n - 1 = 0$. If 1 is the only eigenvalue, then the minimal polynomial must be of the form $(X - 1)^t$ for some $t$. The minimal polynomial will divide $X^m - 1$ and this can only happen if $m = t = 1$, so $A$ is the identity matrix.

(b) If $g_1, g_2 \in T_n$, the group of upper triangular matrices with nonzero elements on the diagonal, then the diagonal elements of $g_1g_2g_1^{-1}g_2^{-1}$ must all equal 1. If $g_1$ and $g_2$ are furthermore in a finite group then $g_1g_2g_1^{-1}g_2^{-1}$ has finite order. Therefore by (a), we have $g_1$ and $g_2$ commute.

(c) Think of each element of $A_4$ as permuting the basis elements $\{e_1, \ldots, e_4\}$ of a four-dimensional vector space. This gives a representation of $A_4$ as $4 \times 4$ matrices.
The subgroup $H = \{e, (123)(4), (132)(4)\}$ of $A_4$ is abelian and $A_4/H$ has order 4 and so must be abelian as well. Therefore $A_4$ is solvable but nonabelian (check).

3.5 (a) Let $V \in \text{GL}_1(\bar{k}) = \bar{k}^*$ be a $k$-torsor. Since $G$ has two elements, the definition of $k$-torsor implies that $V$ has two elements. It is irreducible and the zero set of polynomials in one variable so we an conclude that $V = V(X^2 + bX + c)$ where $X^2 + bX + C$ is irreducible over $k$. The ring $\mathcal{O}_k(V) = k[X]/\langle X^2 + bX + c \rangle = k(\sqrt{a})$ for some $a$. Since $X^2 + bX + c$ is irreducible over $k$, $a$ is not a square.

(b) If $a = bc^2$, then $b$ is not a square and $k(\sqrt{b}) = k(\sqrt{a})$. Conversely if $k(\sqrt{b}) = k(\sqrt{a})$, then there exist $c,d \in k$ such that $\sqrt{a} = c + d\sqrt{b}$. This implies that $a = c^2 + d^2 + 2cd\sqrt{b}$ and so $cd = 0$. If $d = 0$, then $a$ would be a square, so $c = 0$ and $a = d^2b$.

(c) The torsors $V_1$ and $V_2$ are isomorphic if and only if their coordinate rings are isomorphic (in such a way that the isomorphism commutes with the action of $G$ on these rings). The rest follows from (b).

2.3 Problems for Chapter 4

4.1 One easily checks that $R^\sigma$ is a ring. Assume $R$ is simple and let $c \in R^\sigma, c \neq 0$. One shows that the ideal $\langle c \rangle$ is a $\sigma$-ideal. Since $c \neq 0$, we must have $1 \in \langle c \rangle$ and so there exists an element $b \in R$ such that $bc = 1$. Since $\sigma(b)\sigma(c) = \sigma(b)c = 1 = bc$, we have $\sigma(b) = b$.

4.2 Since $e_0 + \ldots + e_{t-1} = 1$ some $e_i$ has a 1 in the first place. After renumbering, assume this is $e_0$. Let $j$ be the smallest positive integer such that $e_0(j) = 1$ (such an integer exists since $\sigma^j(e_0) = e_0$ so $e_0(t) = 1$). If $j < t$, then $e_j = \sigma^j(e_0)$ has 1 in the $j$th place. This would contradict the fact that $e_0e_j = 0$. Therefore $e_0(0) = 1$ and $e_0(i) = 0$ for $1 < i < t$. Since $e_0 = \sigma^t(e_0)$, we see that $e_0$ satisfies the conclusion of the problem. Since $e_i = \sigma(e_i)$, the other $e_i$ satisfy the conclusion as well.

4.3 Let $R = k[Z, 1/\det(Z)]$. Since $\sigma(Z) = AZ$, we have

$$\sigma^t(Z) = BZ$$

where $B = A\sigma(A)\cdots\sigma^{t-1}(Z)$.

We have $R_i = k[e_iZ, 1/\det(e_iZ)]$ and $\sigma^t(e_iZ) = B(e_iZ)$.

2.4 Problems for Chapter 5

5.1 Let $R = R_0 \oplus \ldots \oplus R_{t-1}$ where $R_i = e_iR$ is an integral domain. For any $r \in R$ we can write $r = (r_0, \ldots, r_{t-1}), r_i \in R_i$. Note that if $r$ satisfies $r^2 = r$, then each $r_i$ must be either 0 or 1 in $R_i$, since these rings are domains. Let $f_i = \phi(r_i)$. We therefore have the only entries of $f_i$ are 0 or 1.

For $r \in R$, define $\text{supp}(r) = \{i \mid r_i \neq 0\}$. Note that $\text{supp}e_i = \{i\}$. We have the following observations
5.4 Let \( r \neq 0 \) then \( \text{supp}(r) \neq \emptyset \).

(i) If \( r, s \in R \) and \( rs = 0 \) then \( \text{supp}(r) \cap \text{supp}(s) = \emptyset \).

Note that since each \( e_i e_j = 0 \), we have \( f_i f_j = 0 \). Therefore \( \{\text{supp}(f_i)\}_{i=0}^{t-1} \) is a partition of \( \{0, \ldots, t-1\} \) into \( n \) disjoint nonempty sets. This implies that each \( \text{supp}(f_i) \) is a singleton. We have already seen that the nonzero entry must be 1 so the \( f_i \) are just a permutation of the \( e_i \).

5.2 Let \( u_i = \sigma^i(u), i = 0, \ldots, s - 1 \). The set \( \{u_i\}_{i=0}^{s-1} \) is stable under the action of \( \sigma \). Therefore any symmetric function of these elements is left fixed by \( \sigma \). This means that the coefficients of

\[
p(X) = \prod_{i=0}^{s-1} (X - u_i) = X^s - (u_0 + \ldots + u_{s-1})X^{s-1} + \ldots + (-1)^s(\prod u_i)
\]

are left fixed by \( \sigma \) and so lie in \( k^\sigma \). Therefore \( u \) is algebraic over \( k^\sigma \).

5.3 (i) Note that \( (r, s)(u, v) = (ru, sv) = (0, 1) \) if and only if \( ru = 0 \). Therefore, if \( (r, s) \) is a non-zerodivisor if and only if \( r \) is a non-zerodivisor. This implies that if \( (r, s) \) is not a zerodivisor, then \( (s, r) \in Q(R) \).

(ii) It is enough to show that if \( (r, 1) \sim (0, 1) \) then \( r = 0 \). This follows from \( r\cdot 1 - 1\cdot 0 = 0 \).

5.4 Let \( (r, s) \in Q(R) \) and assume that \( \sigma((r, s)) = (r, s) \). Let \( I = \{u \in R \mid (u, 1)(r, s) \in R\} \) where we identify \( R \) as in 5.3(ii). One sees that \( I \) is a difference ideal containing \( s \) so must be all of \( R \). Therefore \( 1 \in I \) and this implies that \( (r, s) \sim (u, 1) \in R \).

5.5 Note that since each \( R_i \) is a domain, \( Q(R_i) \) is the usual quotient field. An element \( s = (s_0, \ldots, s_t - 1) \in R \) is a non-zerodivisor if and only if all the \( r_i \) are nonzero. Therefore we may make the following identification:

\[
Q(R) = \{(r, s) \mid r = (r_0, \ldots, r_{t-1}), s = (s_0, \ldots, s_{t-1}), \text{ all the } s_i \neq 0\}
\]

\[=
\{(r_0, s_0), \ldots, (r_{t-1}, s_{t-1}) \mid \text{ all the } s_i \neq 0\}
\]

\[= \oplus_{i=0}^{t-1} Q(R_i)
\]

5.6 (i) Note that \( \mathcal{O}_k(\text{GL}_1) = k[Y, 1/Y] \simeq R \), where \( Y \) is an indeterminate, so \( Q(R) = k(Y) \).

(ii) The action of \( \text{GL}_1 \) on \( Q(R) \) is given by \( Y \mapsto Yc = cY \) for \( (c) \in \text{GL}_1(C) \). The subgroups of \( \text{GL}_1(C) \) are the whole group and the cyclic groups \( G_n = \{c \in C \mid c^n = 1\} \). The Galois theory says that the subring of \( K(Y) \) corresponding to the whole group is \( k \). The subring (in fact subfield) corresponding to \( G_n \) is \( k(Y^n) \).